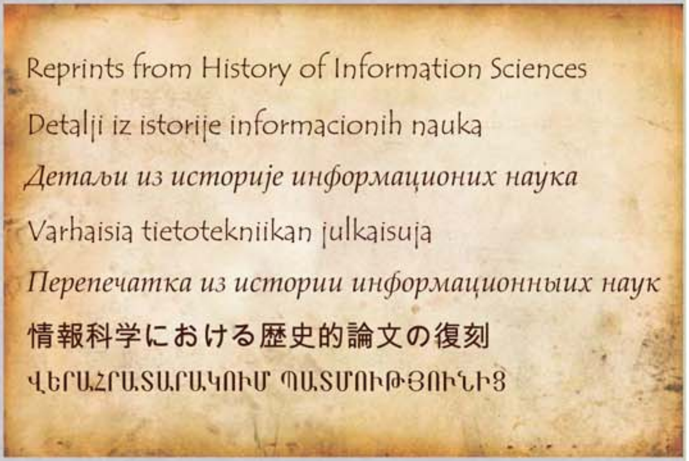
TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

Tampere International Center for Signal Processing

Reprints from the Early Days of Information Sciences

On the Contributions of Arto Salomaa to Multiple-Valued Logic



Reprints from History of Information Sciences

Detalji iz istorije informacionih nauka

Детаљи из историје информационих наука

Varhaisia tietotekniikan julkaisuja

Перепечатка из истории информационныих наук

情報科学における歴史的論文の復刻

ՎԵՐԱՀՐԱՏԱՐԱԿՈՒՄ ՊԱՏՄՈՒԹՅՈՒՆԻՑ

Tampere International Center for Signal Processing
Tampere 2009

Tampere International Center for Signal Processing.
TICSP series # 50

Radomir S. Stanković & Jaakko T. Astola (Eds.)

Reprints from the Early Days of Information Sciences

On the Contributions of Arto Salomaa to Multiple-Valued Logic

Tampere International Center for Signal Processing
Tampere 2009

ISBN 978-952-15-2290-1
ISSN 1456-2774

Reprints from the Early Days of Information Sciences

TICSP Series

On the Contributions

of

Arto Salomaa

to

Multiple-Valued Logic

2009

Reprints from the Early Days of Information Sciences

TICSP Series

On the Contributions

of

Arto Salomaa

to

Multiple-Valued Logic

2009

Editors' Notice

Sincere thanks are due to Editors of the journals that provided copyright permissions for reprinted papers and reviews

Richard A. Shore, *Journal of Symbolic Logic*
Kelly Thomas, *SIAM Review*
Sami Pihlström, *Ajatus*
Ilkka Niiniluoto, *Acta Philosophica Fennica*
Olli Martio, *Annales Academiae Scientiarum Fennicae*
Maarit Järvenpää, *Arkhimedes*.

This publication has been written and edited by
Radomir S. Stanković and Jaakko T. Astola.

Contents

Reprints from The Early Days of Information Sciences

Historical studies about a scientific discipline is a sign of its maturity. When properly understood and carried out, this kind of studies are more than enumeration of facts or giving credit to particular important researchers. It is more discovering and tracing the way of thinking that have lead to important discoveries. In this respect, it is interesting and also important to recall publications where for the first time some important concepts, theories, methods, and algorithms have been introduced.

In every branch of science there are some important results published in national or local journals or other publications that have not been widely distributed for different reasons, due to which they often remain unknown to the research community and therefore are rarely referenced. Sometimes the importance of such discoveries is overlooked or underestimated even by the inventors themselves. Such inventions are often re-discovered long after, but their initial sources may remain almost forgotten, and mostly remain sporadically recalled and mentioned within quite limited circles of experts. This is especially often the case with publications in other languages than the English language which is presently the most common language in the scientific world.

This series of publications is aimed at reprinting and, when appropriate, also translating some less known or almost forgotten, but important publications, where some concepts, methods or algorithms have been discussed for the first time or introduced independently on other related works.

Another aim of Reprints is to collect and present at the same place publications on certain particular subject of an important scholar whose scientific work is signified by contributions to different areas of sciences.

R.S. Stanković, J.T. Astola

On the Contributions

of

Arto Salomaa

to

Multiple-Valued Logic

Acknowledgments

The Editors are grateful to Mrs. Marju Taavetti, the Librarian of the Library of Tempere University of Technology, and Mrs. Pirkko Ruotsalainen, the Development Manager of the Department of Signal Processing, Tampere University of Technology, for the help in collecting the related literature.

On the Contributions of Arto Salomaa to Multiple-Valued Logic

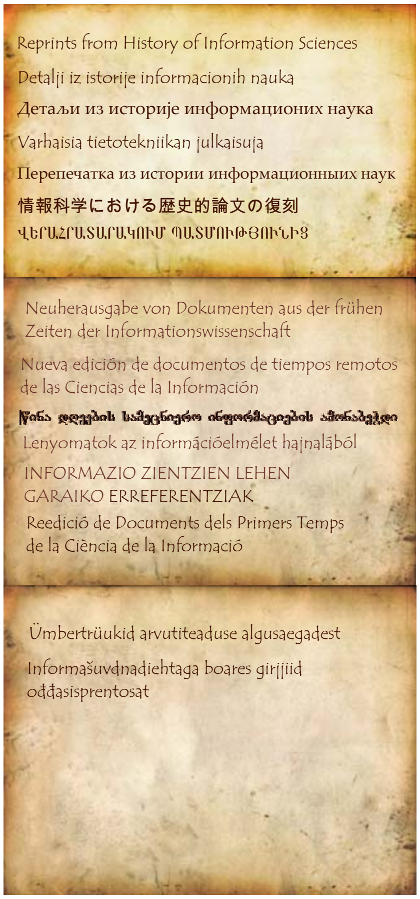
Abstract

The present issue of Reprints from the Early Days of Information Sciences discusses research work of Arto Salomaa on Multiple-Valued Logic. It presents 14 papers by Arto Salomaa, and highlights the impact of this work to the research at the time in this area. Included are also 8 *reviews about his work in multiple-valued logic, and* 12 *reviews written by Arto Salomaa on the work of other authors in this area. The publication includes an article by Arto Salomaa "What computer scientists should know about sauna", and an interview with Arto Salomaa given to the editors on March 17, 2009.*

Notice

This book contains several reprints of pages from books by Arto Salomaa or books devoted to him. They contain interesting historical information about Arto Salomaa and the research community in general. We did not want to rephrase or rewrite the original statements, since we believe that the way they were presented originally has a particular value for the reader.

We kindly ask for these reprints to not be considered simply as graphic illustrations from previous publications, but to be read as a part of the presentation in this book.



Reprints from History of Information Sciences

Detalji iz istorije informacionih nauka

Детаљи из историје информационих наука

Varhaisia tietotekniikan julkaisuja

Перепечатка из истории информационныих наук

情報科学における歴史的論文の復刻

ՎԵՐԱՀՐԱՏԱՐԱԿՈՒՄ ՊԱՏՄՈՒԹՅՈՒՆԻՑ

Neuherausgabe von Dokumenten aus der frühen
Zeiten der Informationswissenschaft

Nueva edición de documentos de tiempos remotos
de las Ciencias de la Información

წინა დღეების სამეცნიერო ინფორმაციების ამონაბეჭდი

Lenyomatok az információelmélet hajnalából

INFORMAZIO ZIENTZIEN LEHEN
GARAIKO ERREFERENTZIAK

Reedició de Documents dels Primers Temps
de la Ciència de la Informació

Ümbertrüukid arvutiteaduse algusaegadest

Informašuvdnadiehtaga boares girjjiid
ođđasisprentosat

English, Serbian Latin, Serbian Cyrillic, Finnish, Russian, Japanese, Armenian, German, Castilian, Georgian, Hungarian, Bask, Estonian, Sami

1 Multiple-Valued Logic

Multiple-valued logic (MVL) emerged as a generalization and extension of binary logic aiming at representation and study of discrete p-valued ($p > 2$) systems, including at the final extent systems in terms of discrete variables with an infinite number of values.

When related to concrete particular applications, MVL systems can be viewed either as non-binary logic circuits, or particular algebraic structures, or symbolic logic constructions.

Since variables are discrete, MVL systems can be viewed as subsets of discrete systems. When p is of a limited value, and cardinalities of the sets of function values are also limited, they are a subsets of digital systems [1], [6], [11]. Therefore, MVL systems can be included in the study of digital signals and systems. In this context, MVL appears to be an important tool in the areas of electronic design and automation - computer aided design (EDA-CAD), and circuit design. MVL circuits offer advantages as reducing the power, improving speed, increasing packaging density, reducing complexity of interconnections due to greater information content per line, etc., [5]. In this context, due to ever increasing complexity of systems in everyday practice, the importance of MVL is supposed to increase in future. Another area of applications of MVL is study of quantum logic circuits and algorithm development. Due to recent developments in these areas, there is a renewed interest in multiple-valued logic.

Mathematical foundations of MVL, after Aristotle and Boole, have been set by many logicians and mathematicians. Already Aristotle has had some doubts about exclusivity of binary logic, in particular the Law of excluding middle (*Tertium non Datur*), as it can be seen in the so-called Aristotle's paradox of the sea battle, discussing the question whether every proposition about future must be either true or false (*De Interpretatione*, Chapter 9).

Contributions to the theory have been done by logicians and mathematicians in the beginning of 20th century. For instance, in 1920 Jan Łukasiewicz introduced a third value *possible* to deal with Aristotle's paradox of the sea battle [4]. In 1921, Emil L. Post introduced the formulation of additional truth degrees with $p > 2$, where p are the truth values [7]. Jan Łukasiewicz and Alfred Tarski considered later a logic on p truth values where $p \geq 2$. In 1932, Hans Reichenbach elaborated a logic of many truth values where $p \to \infty$, see [8], [9], [10]. In 1932, Kurt Gödel showed that *intuitionistic logic* is not a finitely-many valued logic, and the Gödel logic - is called the *intermediate logics*.

In particular, different interpretations of the third value as possible, undefined, undetermined, senseless, paradoxical, etc., lead to formulation of different ternary logics. Some of multiple-valued algebras were implementation oriented [2], [13].

Besides importance in theoretical computer science, ternary logic as a part of MVL can be viewed as an engineering discipline. For instance, a ternary computer has been realized in 1958 as a project leaded by Sergei Sobolev and Nikolay Brusentsov in Moscow, USSR. Further, ternary and quaternary memory chips are a reality already from eighties in the last century.

A closely related subject is *fuzzy logic* that was initiated in the work by Lotfi Zadeh in middle seventies.

The study of MVL as an engineering discipline is supported by IEEE, through the IEEE Computer System Technical Committee on Multiple-Valued Logic, IEICE though the Japan Research Group on MVL, and the activities are regularly summarized at yearly international symposia on the subject (ISMVL). The journal *Multiple Valued Logic and Soft Computing* is dedicated to problems in this area.

References

[1] Aizenberg I.N., Aizenberg N.N., Vandewalle J. *Multi-Valued and Universal Binary Neurons - Theory, Learning, Applications*, Kluwer Academic Publishers, Boston, Dordrecht, London, 2000.

[2] Allen, C.M., Givone, D.P., ”The Allen-Givone implementation algebra”, in Rine, D.C., (ed.), *Computer Science and Multiple-Valued Logic*, North Holland, 1977, second edition 1984.

[3] Gödel, K., ”Zum intuitionistischen Aussagenkalkül”, *Anzeiger Akademie der Wissenschaften Wien*, Vol. 69, 1932, 6566.

[4] Łukasiewicz, J., ”O logice tròjwartos̀ciowej” (On three-valued logic), *Ruch Filozoficzny*, Vol. 5, 1920, 169171.

[5] Miller, M.D., Thornton, M.A., *Multiple Valued Logic - Concepts and Representations*, Morgan & Claypool Publishers, 2008.

[6] Muzio, J.C., Wesselkamper, T.C., *Multiple-Valued Switching Theory*, Adam Hilger, Bristol, 1986.

[7] Post, E.L., "Introduction to a general theory of elementary propositions", *Amer. J. Math.*, Vol. 43, 1921, 163 - 185.

[8] Reichenbach, H., *Elements of Symbolic Logic*, Macmillan Co., New York, 1947.

[9] Reichenbach, H., "Über die erkenntnistheoretische Problemlage und den Gebrauch einer dreiwertigen Logik in der Quantenmechanik", 1951.

[10] Reichenbach, H., "Les fondements logiques de la théorie des quanta, Utilisation d'une logique à trois valeurs", 1954.

[11] Rine, D.C., (ed.), *Computer Science and Multiple-Valued Logic Theory and Applications*, North-Holland Publishing Company, 1977.

[12] Rescher, N., *Many-Valued Logic*, McGraw-Hill Education, 1969.

[13] Vranesic, Z.G., Lee, E.S., Smith, K.C., "A many-valued algebra for switching systems", *IEEE Trans. Computers*, Vol. C-19, No. 10, 1970, 964-971.

2 Arto Salomaa's Work on Multiple-Valued Logic

Arto Kustaa Salomaa formally started his scientific research work by a paper in *Ajatus* in 1959 and continued with his PhD Thesis in the area of multiple-valued logic defended at the University of Turku, Turku, Finland, in 1960. The Thesis was entitled *On the Composition of Functions of Several Variables Ranging Over a Finite Set*, and has been supervised by Professor Kustaa Inkeri.

Several publications that have followed were also devoted to various subjects in MVL and will be reprinted in this issue of Reprints (Section 5) together with reviews of some of these publications (Section 6).

Academician Prof. Salomaa serves as the Editor or several journals devoted to the topics in MVL, and in particular, he has served as the Editor of the *Journal of Symbolic Logic* in the period 1968-1984. In this journal, Prof. Salomaa reviewed a number of publications by different authors (see Section 7).

The most recent publication of Prof. Salomaa in the area of MVL appeared in the book *Grigore Moisil and His Followers*, Romanian Academy of Sciences, 2006, devoted to the memory of Grigore Moisil, the Romanian mathematician working in this area, and recognized among other things, by the axiomatization of ternary logic.

Table 1: Journals where A. Salomaa has published about MVL.

Journal	Year of publication
Ajatus	1959
Journal of Symbolic Logic	1960
Ann. Univ. Turku	1960, 1962 (2), 1963 (2), 1964
Ann. Acad. Scient. Fenicae	1963 (2), 1965
Acta Philos. Fenica	1965
Archimedes	1968

The number in parentheses shows the number of papers published in the particular year.

Publications by A. Salomaa on Multiple-Valued Logic

”On many-valued systems of logic”, *Ajatus*, No. 22, 1959, 115-159.

”On the composition of functions of several variables ranging over a finite set”, *Ann. Univ. Turku*, Ser. A I, No. 41, 1960, 48 pages.

”A theorem concerning the composition of functions of several variables ranging over a finite set”, *Journal of Symbolic Logic*, 1960, 25, 203-208.

”On the number of simple bases of the set of functions over a finite domain”, *Ann. Univ. Turku*, Ser. A I, N. 52, 1962, 4 pages.

”Some completeness criteria for sets of functions over a finite domain, I”, *Ann. Univ. Turku*, Ser. A I, No. 53, 1962, 10 pages.

”Some completeness criteria for sets of functions over a finite domain, II”, *Ann. Univ. Turku*, Ser. A I, No. 63, 1963, 19 pages, (Russian translations of two previous papers in *Kibernetitseskii sbornik*, No. 8, 1964, 8-32.)

”On sequences of functions over an arbitrary domain”, *Ann. Univ. Turku.*, Ser. A I, No. 62, 1963, 5 pages.

”Some analogues of Sheffer functions in infinite-valued logics”, *Proc. Colloq. Modal and Many-valued Logics in Helsinki 1962*, Published in 1963, 227-235.

”On basic groups for the set of functions over a finite domain”, *Ann. Acad. Scient. Fennicae*, Ser. A I, No. 338, 1963, 15 pages.

”On essential variables of functions, especially in the algebra of logic”, *Ann. Acad. Scient. Fennicae*, Ser. A I, No. 339, 1963, 11 pages.

”On infinitely generated sets of operations in finite algebras”, *Ann. Univ. Turku*, Ser. A I, No. 74, 1964, 13 pages.

”On the heights of closed sets of operations in finite algebras”, *Ann. Acad. Scient. Fennicae*, Ser. A I, No. 363, 1965, 12 pages.

”On some algebraic notions in the theory of truth-functions”, *Acta Philos. Fennica*, No. 18, 1965, 193-202.

”Matematiikka ja tietokone”, *Arkhimedes*, 1968, 5-10.

”Sata vuotta matemaattista logiikkaa: paattelysaannoista tietokoneohjelmointiin”, In: *Muuttuvat ajat*, WSOY, Porvoo, Finland, 1979, 116-130.

3 One of the Twelve

The biography of Arto Salomaa has been published many times at different occasions, as for instance, when he was accepted as a member of one of four Academia, some round birthdays, etc. Therefore, instead of writing yet another formal one, we will provide several photos and excerpts from books written by Prof. Salomaa or devoted to him. These photos should illustrate the main principles accepted and appreciated by Prof. Salomaa in his life and work. Photos were taken while talking with Prof. Salomaa about his numerous books (Section 4). They were taken without any pretensions except to be some simple reminders of particular details he presented, however, later we realized that they can tell much more than that.

For details in biography of Prof. Salomaa and concrete data, we refer to

Juhani Karhumäki, ”A short biography of Arto Salomaa”, *Information and Computation*, Vol. 151, 1999, 2-4,

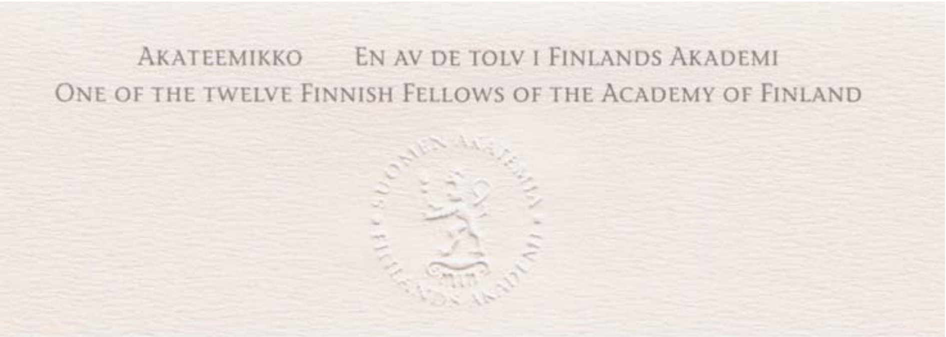
and to the web site of Prof. Salomaa

http://vanha.math.utu.fi/staff/asalomaa/

To simply explain who is Arto Salomaa it is sufficient to say

One of the Twelve

as stated in the memorandum of letters used by members of the Finnish Academy



AKATEEMIKKO EN AV DE TOLV I FINLANDS AKADEMI
ONE OF THE TWELVE FINNISH FELLOWS OF THE ACADEMY OF FINLAND

SUOMEN AKATEMIA • FINLANDS AKADEMI •

4 Interview with Arto Salomaa

The interview was conducted by Radomir S. Stanković in the office of Arto Salomaa, B-6035, Turku Centre for Computer Science (TUCS) Joukahaisenkatu 3-5 B, 20520 Turku, Finland.

Interview

We would like to ask about your work in Multiple-Valued Logic, since this would be the main subject of this issue of Reprints devoted to a part of your work.

Recently I have not really done anything on that subject except, there is one thing, I don't know if you know about this, this is a recent book, it appeared last year or 2006, here I wrote an article about Moisil and Many-Valued Logic and it has some of my recollections. This is the only thing I've really published about this after what I've said in 1964/65.

We would like to reprint your paper in Ajatus, the first paper from 1959 and maybe we also have to take a look in this.

This was actually my first publication.

This is why it is so interesting.

Then my PhD thesis was about Sheffer functions and the main theorem appeared also in the *Journal of Symbolic Logic* in 1960.

You were very active as a reviewer for Journal of Symbolic Logic.

That is true, however, only in early days, but not anymore.

Let me maybe first start with a classical question. Everyone knows who you are in science, but it is very interesting to see how you view yourself in this perspective, because you have so many different interests, including sauna, on your web pages there are photos of your family, and so on. What you *would say now about, what is your main?*

It is very difficult to say what the main is, because there are so different things in many years, but I have really always liked the things I'm doing at the moment, and I have written many books. In another interview, not so long ago, Christian Calude asked me what I liked, and I would say I like my first book, "Theory of Automata" the most, and it was quite long, seven years after my PhD, but it was the first book. The publisher was very bad, this Pergamon Press, there were all kind of scandals, they screwed up things enormously, but I still like the book. And I think that things that are in the book still nothing much has changed from these days, it is very mathematical, so it stays the same.

Exactly as you say in one title: "Theory is Forever".

Yes, this was one book that was published for my birthday, so that was not my invention, the title.

May I ask you about your name - Arto Kustaa Salomaa. Who gave you the name, maybe your father?

Yes, so in the first place my last name, of course, comes from my father and his original name was Grönholm, which is a Swedish name and means Green Island. When he was very young, something like 15, in that time there was a movement in Finland to translate names into Finnish, and Salomaa is quite common name in Finland. There are many Salomaas and they are not related to me. Then Arto, it is very easy to say, is the Finnish form of German Arthur or English Arthur. Arthur Schopenhauer was my father's favorite philosopher and he wanted me to have this name. And Kustaa is from Gustav Swedish name, and there are kings in Sweden with this name Gustav and I got name Kustaa just because in Finland we have The Name Days, and today (March 17) is the day of Kerttu, that is the women's name, and I was born on June 6, which is Kustaa's Day, so this is the explanation of the name.

Can you tell us something about the place where you were born, and early days, how it looked in the primary school at that time, maybe you remember your teachers or friends?

Yes, I was born in Turku, and basically spent whole my life here, I've been 10 years abroad. I was born here and my childhood was here, and of course childhood was at the time of the war, and these were very rough times. I was pretty much alone, because my brother was in the front and my father was also involved in war activities, and my mother and sister were also engaged. My sister was actually 15 years older than me, so she was with me, but she had to work until late in the evening, so I was just hanging around with boys and this was my first contact with cryptography, because the boys gangs were using this coding and I was very good in breaking codes and doing things like this. I was also interested in mathematical problems at that time.

For instance, one problem is when there are leagues of football teams, for example, n teams, and how many games teams plays against each other. Of course I didn't know anything about Pascal's triangle or binomial coefficients, but I was able to invent the rule for this and the boys did not believe this rule and they came up with the counter example, and they took, actually fourteen existing Finnish teams and they took actual games. There were 90 games and my formula gave 91, 7 times 13. But when we carefully looked through the list, one game was missing. They had 2 Turku teams and the game between them was missing, so my formula was correct. And then, of course, the elementary school of that time was for one or two hours per day, and there was bombing going on in Turku. Sometimes, some of the activities were taking place in Naantali, the place not far from Turku and the danger of bombing was not so high. After elementary school, I went to classical lyceum, and five years after the end of war nothing much was available. People usually say that people were much satisfied in that time when there was nothing available. Of course I had some good teachers, for example my math teacher in classical lyceum was very good, and also I liked Latin very much, and now when I have time I still read some Latin and so forth. In fact, it was by kind of accident that I haven't studied Latin, so I started the mathematic studies and I was the first years in Turku and I found my research field, Formal Languages and the Automata Theory, when I was in Berkeley.

What was the profession of your father?

He was a Professor of Philosophy in Turku.

What was the problem with books and text books of that time, because it was *post-war era, no media available, how you got literature to study?*

I would say that the math curricula of that time was very classical, it was basically analysis, and a bit of algebra, and these books existed in Finnish. But the modern books, I knew them only when I went to Berkeley.

How have you selected Berkeley?

This was more accidentally, there was a system of scholarships and grants. Finland was the only state that paid its debts to United States after the First World war and at some stage, around 1950, it was decided that from that point on, all the further payments will be used for cultural exchange. So scholars came to Finland and there were grants for Finnish students to study in United States and this was graduate studies, so I have already had my master degree when I applied this. And I really think it was kind of accident, I knew the name of Tarski, who was in Berkeley, and I had listed three universities, and the Committee chose Berkeley, so I went there. So the Tarski's name was my choice why I've put Berkeley.

Then you said you have met John Myhill.

Yes, John Myhill was one of the founding fathers of *Automata Theory* and I attended his seminar. On that seminar there was a new book called "Automata Studies" and we went through this book. My own work on this seminar was about self-reproducing machines and in that time it was not much known in biology or anything. For instance, it was a controversial thing whether machines could at all reproduce themselves, because there were all kind of arguments in articles that if you self-reproduce yourself, you have to be more than what a machine can be. Von Neumann was the great name and my work was more or less to do in detail what Von Neumann's paper was. My work there was never published, this was kind of very detailed constructions of instructions for the machine. Parts for the machine were randomly provided in plane and the machine was moving around and collecting the parts. It was like Theory of Turing Machines.

Maybe in that time there were thoughts - can machines think?

Yes, the artificial intelligence was also forming, there were all kinds of questions what is possible for machines and what is not. If I compare the situation then and now, the differences are that in late fifties early sixties, people were very optimistic with machines translations, that it is a very easy thing to translate from one language to another, but this was very difficult. And people were thinking that machines could never play good chess, now it turns to be the entirely opposite.

So, there have been some different opinions then and now? How do you predict the future of machines nowadays, they will put us into slavery?

I don't think so; I'm not into science fiction. Of course this is more political question, like some search engines as Google, if they get too much power or one gets information only from them, it is not so good. But, I think, once you use your own judgment, it is a very good source to find information.

Do you think they have changed the way of learning or thinking of people, because now we can find data and information everywhere?

Well, I think the learning is certainly totally different now, and this is of course a problem for teachers, because if you have to write an essay, it is so easy to copy from internet and it is very difficult for teachers to find this. But, I think, in general this is a great asset, these new things.

You said that in your childhood there were your sister and your friends, but now kids are growing near electronic media and after some years they start reading, does it also influence their way of learning?

It certainly does, because some of my friends think that reading becomes obsolete at some stage. But still, books are nicer to read than from the machines.

What do you think after writing so many books, do you think it would be possible to change something in the way of writing, to approach maybe classical books to electronic media presentations?

I think it is going very much towards electronic media. I have been involved in one entirely electronic journal called the *Journal on Universal Computer Science*. It brings also printed volumes, but these volumes are going mainly to libraries. The publishing in general and the editing job now is much easier than before. It is the same this peer reviewing, but earlier I had to make many copies and mail an article and ask the person if he wants to review and ask to send it back, but now I can just email the file, otherwise I would have to make copies, etc. Also now I can just send the file and if he does want to review, he will act as a referee and if disagrees, then I can ask someone else in the same way just by forwarding the message. But how would be the publishing in general, I think the journals will still exist, because people want to see the paper, not only at the screen. Maybe the more finalized version can be printed, and in these electronic journals one can still change the contents.

What do you think about the quality printing? Would you like to see your books printed in a good quality or maybe cheaper that would be easier accessible?

I think this electronic means have certainly improved the quality, now it is much easier to write papers than before. For example, the LaTex is a very good tool and so on. I like when book appears in good quality and usually the publishers do that, and then they can charge. I am an Editor of this series of books, and these are nice books, and for one such book the publisher can charge 100 euro.

How do you remember your colleagues and Professors from Berkeley, especially John Myhill as a person I mean?

John Myhill was a very difficult person, he had several nervous breakdowns and sometimes he had to spend months in sanatorium and so forth, and I was never so close with him. But, his lectures were very impressive, because he was full of new ideas, but he was kind of out of this world. I have told many times this story, it is a true story. We were waiting for him to come to a lecture, and when he didn't come we went to search him around and he was in another room and he had already written the blackboard half full without noticing that there was no audience. Tarski was, of course, entirely different, he was very socializing, and was kind of a Man of the World, always dressed very elegantly and so forth. I took some courses from him. There were many other people, like Roger Lyndon and Robert McNaughton were there at that time, later they became very well known in this field.

In this book on the occasion of your 70th birthday, it is written that you are one of the most influential researchers in the Theoretical Computer Science. Of course, there are many directions, but which one would you maybe want *to select, where you went deeper?*

Certainly Automata and Formal Languages, these two subjects. Sometimes you speak separately on Lindenmayer systems, because it is kind of biological, but it's much more Formal Language theory. I have also written two books about Formal Power Series, and it is also kind of another extension of Formal Languages because it's not power series in the sense of classical mathematics but in non-commuting variables, it is like words where letters do not commute. The other field I have been working or teaching much is Cryptography, and I have written a book about cryptography, but I'm not saying that I made any significant contribution to it, except maybe I was the first one to teach cryptography in Finland and so many of these practical people, in Nokia for instance, they are my students.

You actually started teaching cryptography when playing with kids.

It is true, but there was a time gap, this was in mid forties, then I came back to cryptography only in late seventies, when there was this idea of Public-Key Cryptography, very nice mathematically, very challenging and interesting mathematically. I gave here in Turku first lectures, I think in 1982.

And then the book appeared in 1990.

Yes, the book appeared in 1990.

Here in your book could be found that William Stanley Jevons actually provided first idea about this one way function in cryptography. Do you have any comment about this, maybe like this problem of factoring product of two large numbers?

This is the key issue in this, but I'm not aware of any significant progress in this. Of course, if some fast algorithm will be invented, this would mean that RSA will become very vulnerable and a lot of these security things, computers, are using RSA in some form.

It appeared this Shor algorithm related to the quantum computing. Is this a problem for this area or still not?

Not yet as far as I know, because the quantum computers are still developing, so I don't think they still do some real big stuff.

You started speaking about your Professorship in mathematics in Turku, you taught also cryptography and some other courses?

I can say that I have been teaching here in Turku, since I came back from Berkeley, in 1957. And I have been teaching any kinds of courses, from differential equations, calculus, number theory, algebra. Now I've just noticed that also I gave course in game theory in 1965, and I've noticed that I still have my lectures from this course and I've talked about this "Nash Equilibrium", you know this now Nash became very famous, he won Nobel Prize and there is this movie "Beautiful Mind" which is about him. It was a pretty new thing in 1965 this "Nash Equilibrium", so I talked a bit about this in my lectures.

Does it mean that you like teaching or how do you feel teaching compared to research?

Especially when I was younger I surely liked teaching. I also like very much to guide PhD students. I have really wonderful PhD students, much better than myself. They are all different and you need to have different approach to every of them. Like, some students work entirely alone, and some you have to see once or twice a week. So it very much depends on the person.

In one period, you also studied in Helsinki?

I have never studied in Helsinki University, but it was kind of formal reason that I took one exam or degree. I have master degree here in Turku, and then doctor degree in Turku, but it was kind of formal requirement that I have this intermediate degree, licentiate degree as called in Finland, so I had this in Helsinki. I never actually studied there; I only took this degree there.

Then you went to Western Ontario in Canada?

I was two years there where, and I wrote this book "Theory of Automata" and it was a very nice period, it was an developing University and very nice colleagues.

How did you get contact to go to Western Ontario?

Actually, they have approached me, because Robert McNuaghton, whom I've mentioned earlier, we were together in Berkeley, he had given lectures in a summer school in London, Ontario, and he had mentioned about my work on Axiom System for Regular Expressions and that is how they knew me. So, they contacted me, actually by phone, it sounded like a nice opportunity and I went there.

Kai Salomaa?

Kai Salomaa, yes he is my son.

And he is there?

He is not actually there, but he is in Canada. He is in Queens University, Kingston. He was, of course, a small boy when I was visiting there, but actually I get regular contact with London and I have visited it almost every year, including last fall. Now, of course I have additional motivation, because my son is in Canada, and I want to visit him. But always when I visit Canada, I spent couple of weeks in London, because still there are actually many professors, my former PhD students, there are two who came from here, Turku Center for Computer Science, Lucian Ilie and Lila Kari, they are both there professors now.

Then you went to Aarhus, Denmark?

Yes, in between I was five years in Finland, and then I was a Visiting Professor in Aarhus for two years. There I had also very nice time, that was kind of beginning time of Lindenmayer systems, this biological thing. I had some students in Aarhus, so we did some work there.

Then you also published this Mathematical Theory of L-Systems?

This was a bit later; it was actually written in late seventies, when I came back to Finland. I was together with Grzegorz Rozenberg, who is, really I can say, my best friend and we keep in daily contact, even now we phone each other every day.

Then in 1999, in a conference in Prague, you had a joint invited talk?

Yes, we actually started to talk and we practiced very much, saying the same things together and we both gave some parts of the talk after that.

That's really impressive, that you have so many co-authors, somewhere I have found over 50. And also all these students, associates, you said very close friends, for example Derick Wood or Hermann Maurer.

We all work in the so called MSW group and we work together.

How this group started?

It started, so that Hermann Maurer invited me to Graz, he had also earlier worked with Derick Wood, and we started writing papers together and it was a very nice collaboration. It was always starting in the following way, that two of us start together and wrote the paper and the third one checked it, so this happened in all places. Derick Wood was in Canada, and Hermann was originally in Karlsruhe, Germany, but both came to Graz, Austria, and I was here.

This huge group of your associates are from Romania, and they actually came here.

Yes, actually Moisil I knew a little bit, we have talked few times in the early sixties. I met him in a big math congress that is held every four years, and it was in 1962 in Stockholm. After that he came to Helsinki and I met him there. He had done work on mathematic logic, but then there was practically nothing in between, but only after the revolution in Romania. So first Lila Kari came here and then after that I had very close cooperation with Gheorghe Paun and Alexandru Mateescu, who died unfortunately few years ago. So these are the closest Rumanians. And then of course, I had Romanian PhD students here, Valeria Mihalache and Lucian Ilie here in Turku. Lucian Ilie is now a Professor in London, Ontario.

And with Professor Mateescu you wrote a chapter in a handbook about languages something that is very interesting for me to ask. There is a table of languages, how they develop, and in one place you are mentioning Serbo-Croatian language, Bulgarian language, but not the Macedonian language.

Is it just because it belongs to the same family of Indo-European languages?

I think this refers to this table; this is more or less the table that appeared in some linguistic thing, it was in *Scientific American* or something similar. This is basically where we did not do any more details, this is just kind of introduction from language point of view, and this is more or less also from *Scientific American*.

Was it so that it was one prototype language, proto-language, and that all other languages developed from it?

This is how it is viewed in Indo-European languages, so our original contribution here in this chapter starts from this *Formal Language Theory*, it is more this telegraphic survey.

Your book on Formal Languages, published in 1973, was referred in 1991 among the 100 most cited texts, and it is really impressive and after that appeared this Handbook on Formal Languages.

Yes, but this is entirely different thing. Like we say here, in some parts of introduction, in that time, in 1973, one could really write about formal languages in a single volume and still bring the topic to the area of recent topics. But now, in nineties when this book was compiled, this book has 51 authors. It was impossible to conceive such one book, and that's why we wanted to make this Handbook. I think that I have written some articles, like two articles with Mateescu and couple of others, and also one with Lila Kari and Rozenberg about Lindenmayer systems.

Then about the origins of the Formal Language Theory, you wrote pretty much about this story of origins in combinatorics, computability theory, etc. What is you opinion now about these origins?

My opinion about origins has not changed. I have been mostly interested in these aspects that are kind of mathematical aspects, dealing with Automata Theory and combinatorics of words rather than these linguistic origins. For the linguistic origins, for instance, the linguistic people, they kind of emphasize different things, which, of course, have also led to very interesting mathematical formal problems. But, as regards the origins in general, I still think that formal languages came from many sources.

Emil Post, Axel Thue, Alan Turing, including Chomsky?

Chomsky is a bit different than the other three, from Post and Turing they are more of this my type of origins.

But it is also interesting that Emil Post had just one paper about multiple-valued logic, he started the same as you, and you also had several papers. Is it the normal way of development, starting from multi-valued logic?

No, it is very accidental.

But beside these Formal languages you are also interested in the Turku dialect?

Well, to some extent, yes, surely. But I have not done anything formal about this or anything in writing about this, but in translations of my cryptography book, I have mentioned some examples of this Turku dialect. This is the Chinese translation of Cryptography Book, I think here my point is that if your language is Chinese, you don't need any cryptography because this is already a cryptography, and then I say that I ask whether the Chinese people could read these phrases in Finnish. Jaakko Astola would surely understand that. This last sentence is very good, you really have to know Turku language to understand this.

Another interesting question is, since you have so many associates, so many students, and you work with them in a different manner, maybe sauna was the place to meet them?

Yes, some of them yes, but the point is that some people don't want to come to sauna. Some Finns make this mistake, they kind of force people to come and my usual attitude is that, ok if you don't want to come to paradise that's up to you. I have never forced anybody to come to sauna, but certainly I've met some of them, like MSW group, we spoke about three-sauna-problems. Because, I have an idea that the veins in your brain open when you are in sauna. And then, if a problem is difficult, like Sherlock Holmes spoke of three-pipe-problems, we spoke of three-sauna-problems and that you have to go three times to sauna to solve this problem.

Salosauna is?

Salosauna is my sauna, I had it since 1975, it's about 50 km from Turku, it's very old building so we bought this, Salosauna was already built around 1870, so it's an old wooden building.

There is a song about it by Herman Maurer?

There is a song, but it's about people who came on the conference, it's not actually about Salosauna. Oh, he has also written about Salosauna, so you are right, it's actually in this book that I have. So this is Hermann Maurer's poem, he has written several things about Salousauna, both in English and German.

And your paper "What computer scientists should know about sauna"?

Yes, this appears in this Bulletin, actually several times. It is also available in the net, and it's also in German translation, somebody translated into English and German.

Have you ever met any Serbian Professor?

I have certainly met, like there was this Oberwolfach Conference in earlier times. I remember especially there was one Serbian, who was very good in drawing, but I don't remember his name. He drew a picture of me that was very good.

And you became a Doctor Honoris Causa of six Universities?

Yes, actually of seven. It was six, but I think Graz was the latest.

What is your cooperation with those Universities? Do you have some cooperation in teaching or giving lectures?

The first one was the Swedish University in Turku, Åbo Akademia and of course I had some colleagues there, then University of Oulu also in Finland, my former student is a Professor of Math there and I have been there. In all of these Universities I have some contact and in Bucharest in Romania, Szged in Hungary, then Magdeburg in Germany, there I also knew people.

I have visited University of Latvia in Riga. I think in all of them there has been some cooperation, more or less. Like, just yesterday I got an invitation to State University of Latvia, they have some celebration, they could be 90 or 100 years old and they invited me, but I'm not planning to go, because I don't travel so much these days anymore.

Then you became a Member of four Academia; it is Finnish Academy, Swedish Academy in Finland, Hungarian Academy, then Academia Europaea?

Actually two in Finland, they are Swedish speaking Academy in Finland, then Academy of Sciences in Finland.

You are active there?

I am not really very active; I very seldom go to these meetings. Like, these two Academies in Finland, they meet in Helsinki and I usually don't go there, very seldom.

And about this European Association for Theoretical Computer Science, you have been there a president and chairing it, etc. What you can tell us more about this Association?

This was kind of small at the beginning and I was somehow involved in it from really early stages. And then it started to develop and it became almost equally big as the corresponding association in America. It used to have these main activities, so it has this Bulletin which they publish; I had my Formal Languages column there for decades and it publishes other things, like reports from the conferences, announcements of the conferences and this *Theoretical Computer Science* journal used to be also the journal of this Association. But I don't really know what exact relations are now, maybe it is not advertised that much anymore, this Association. Then also we had this book series which were initiated by this Academy.

You have been very active in the Nevanlinna Institute and also in the jury for the Gödel Prize. What are your memories about this?

I was a member when it started, about 10 years, but it seem very long time ago now, now it's something like that my job finished there in early nineties. But it was first kind of Institute common to all Universities in Finland;

it was in Mathematics and Computer Science. Its activities included, for instance, and this is still true, they give prize for the best Doctoral dissertation in Mathematics in Finland each year. Some of my students have also got this prize from the Nevanlinna Institute. The Gödel Prize is kind of common between this EATCS and corresponding American organization. I was there and there are some rules how many years you serve there. I have served there many years as the rules say and at least once, one year I was Chairman in this. It selects what is called Gödel Prize for the best article in Theoretical Computer Science within the last five years also.

You said Mathematics and Computer Science; are they different or maybe they are combined areas? How do you feel about this?

They are certainly combined areas; it is very difficult to say what about Automata Theory and Mathematics, it is very close to Semirings Theory and it is very mathematical and this Formal Power Series is of course very mathematical. This of course concerns Theoretical Computer Science and Computer Science in general.

You have selected very interesting titles for your books, one was "Theory of Automata", then "Computation and Automata" and then it was this "Jewels of Formal Language Theory". It is a very interesting title.

This Jewels was kind of, actually the other two you have mentioned they were kind of general research, but this Jewels was intended to present mathematically beautiful things in Formal Languages. The model for this book was this Russian Khinchin's book "Three Pearls of Number Theory" so I had this as a starting point for this Jewels book.

You have mentioned Russian authors and it's mainly Soviet time. Was there any influence of Soviet time to Finland, especially science in Finland? Where they completely independent?

Yes, certainly. In my case there was no, but this can vary from field to field, like there was some definite cooperation in certain technical areas. Of course, I had some Russian colleagues who visited me here and so forth. My main contacts were not in Russia.

How about the way of studying or life of a student here in Finland and maybe

States? Was it so different?

Maybe not anymore now so different. But in my time it was very different, because in that time students were really on their own, there was very little guidance and Professors were very big bosses and you couldn't see them much. It was very different from when I went from here to Berkeley, to see that famous persons, like Tarski, were available for ordinary student like me.

How could you see Finland and science in Finland now in the world perspective, because we all know Finland is one of the highest tech countries?

Well, it is very difficult to say in general for Science, but I think in my area, Theoretical Computer Science, Finland is very good and there are my students and there are also a lot of other people. And if you relate this to the number of people in the country, I would say that only Israel is maybe equally good in Theoretical Computer Science as Finland. Otherwise, Finland is superior if you take the number of people in the population in the country.

How do you feel, how it happened that Finland is so highly developed after so terrible time, World War in Europe? After Second World War, you had very hard time, is it mentality of people?

I think one reason was, that there were few instances in history where a small country like Finland, was able to defend itself from a vastly superior power like when Finland was in the Winter War and in the Second World War Finland was never occupied by foreign troops, and this makes Finns kind of proud and maybe people didn't want to leave the country. This is of course one explanation. The other explanation would be that in sauna veins open, but this is very difficult to say.

Turku was a former capital in some period. And is it Turku capital in science and how are the relations between Turku and Helsinki, Turku and Tampere?

I think they are good, of course I can say that Helsinki now has a bigger Institute and definitely much more people, it is also capital in science, there is no question about it, but I think relations are good, and also with Tampere relations are very good. I personally have very good relations with both Technical Universities and former Rector Timo Lepistö, who is now late, he died unfortunately early, we were very close personal friends and I have visited Tampere quite often. Even now I have good contacts there with both schools, Technical University and University of Tampere. But these are smaller places, but if you ask for capital, then you have to say it is Helsinki.

I would like to ask you more about this Many-Valued Logic, because it is my field of interest. Once you have written that the interpretation of the values could be very important for practical application. But how to think about it, what could be the interpretation, do you have your own opinion?

Well I have not been thinking about this so much lately. Of course, the interpretation could be different kind of probabilities, but I think that basically some meta language level things start to be two valued after all. My work in many-valued logic and my own contributions were not in these interpretations, but this could be considered as purely combinatorial topic that is this Composition Theory of Functions over finite sets, truth-values are from finite sets and using this compositions, you can get any function. This can be stated as strictly mathematical topic without any reference to many-valued truth values. But I was also involved, this was a second part of my thesis, I wrote something about axiomatization of logic, but it was never published. Of course, later, there were many works done on this.

Since you analyze the history of many-valued logic and origins, do you see the perspective of this area, maybe from engineering point of view, concrete applications?

I know there are many people working in this area and many things have been done since I was interested in this. Certainly, there are applications, but I am not so much aware of them, so it is difficult to say, but certainly the engineers have been working on this.

And about this DNA computing?

DNA computing is entirely different thing, so that was the field I've got interested, because it is very nice from the Formal Language point of view, because it brought entirely new problem areas. It is also very nice in these steps that it could bring something entirely new, because you have this massive parallelism, once you make this DNA soup, then you can encode all possibilities, and then all these complementarities and the combinations form, you get kind of computation really in this sense. This really could lead to something, but it is also difficult to compare which one is more promising, the quantum computing or DNA, but really no striking applications have been shown yet. It is kind of, how should I say, I do not believe either one would ever substitute normal computers. In some problem areas, I can visualize they can be very useful, especially Quantum computing could be very useful in cryptography. And DNA computing also if one can really take care of this massive parallelism in laboratory.

About these regularities that are described by using the L-systems, you also mentioned the Sierpinski triangle, are they really appearing in nature, so are they so natural that should be mapped into mathematics or they are more mathematical and then we suddenly discover something in nature that matches them?

Well, it's both ways, so one speaks much about this general term Natural computing, so it is computing model by nature, like genetic algorithms to one can look as algorithms that started in nature. We look what happen in nature, and then perhaps we can bring this to our own computing devices. So, this is a really very very promising approach.

And about these regularities and automata - do you think that automata are very good models to describe a lot of different phenomena or how would you say? Automata, they are more mathematical models for many phenomena?

They have been used really, like this text editing and many things like this. Now there is very much advanced theoretical work done on this complexity of basic automata operations, these regular operations. For instance, if you search certain texts, certain subtext, then really automata are very helpful, but it is certainly not everywhere, so you have to look what kind of problems come up and then decide.

What would be the vision for the development of Formal languages in the future?

There is of course this, that I would like to call the French School, that are very much in this combinatorics on words and this kind of mathematical aspects of words. Then, there are these various linguistic approaches that are good topics for natural languages. Now there are all kinds of families that are bigger than context-free languages, like one that we studied that are good for natural languages. There are recent things like these biological things like this slicing that we have done in DNA computing, and there are many areas, so I cannot say which one will be most important in future. The only thing I can say for sure is that this French School, this mathematical topic are important, because mathematics will always be there, but how important are other things will depend on whether they really bring something significant to this.

Do you think that you, somehow, always support this mathematical approach to Formal Languages? Does it mean that mathematics is essential thing in this area?

Yes, certainly, of course.

And there is this binary Logic, Multi-valued logic, Fuzzy Logic? What do you think about this Fuzzy Logic, because it is close to computing with words?

Yes, yes, there are all kinds of claims that Japanese have made all kinds of equipment using Fuzzy Logic. I don't know so much about this, but there was one doctoral student here in Turku, who moved latter to Lappeenranta, working in this area and then I had to know a little bit of this. I think it certainly one can not ignore this topic, it is very promising approach, because I think that life is not this black and white, but there are this different shades of gray and similar things in all kinds of situations, for instance if is it cold or not in this room, etc. For all kinds of regulating devices, you need this Fuzzy Logic for sure.

Would you like to visit East Europe one day, maybe Serbia, I would like to invite you.

I would like certainly, however, as I said, I travel very little these days. My health is otherwise ok, but I have very bad knees, so I'm using stick when I walk outside. The only trip I like to go is that I usually go once a year to Canada, and occasionally something else. But, very few trips abroad these days.

There is another interesting question. Your son is working in your field.

How does it feel to cooperate with your own son in the same field? Is it easy?

It is, of course, very easy, but we have not cooperated very much, but we had some joint publications. But mainly, in all of these publications, there is not a single publication where are just two of us, there is always somebody else. My Chinese friend Sheng Yu is in many of these.

You have visited China?

I have not visited China, but also I have contact, because my son is married to a Chinese.

And about translations of your books, they have been translated in many languages. How do you feel, is translation always very close to the original or not so similar?

Except for German I cannot tell, for example for Chinese and Japanese I cannot tell at all, then I think also Romanian and Vietnamese, they have been really translated into languages that are not familiar to me. And there is this German translation of Formal Languages that is very good. And there is also a French translation of one of my books that is also ok. Then Russian translations, I know and I can read a little bit of Russian, but I cannot really tell is it good or not. There is this DNA computing in Russian translation, and it is probably very good, because these are very good people who translate.

You probably receive many letters from your former students all around the world?

Yes, especially now e-mails.

How is to work with someone and became a friend at the same time? Is it simplifies the scientific work or when you are friends you cannot fight that much and argue on some topics or it just helps?

It certainly helps, so I would say that my best friends are really people with whom I have worked very much. So it certainly helps, and I would say that good cooperation is something where you don't count how much work each of you does, but everybody tries its best. This was always the case for this

MSW group, we never counted we should do equally, and everybody tries to do as much as possible. There are also different types of people, like some people do not like to write things up, so I like to write things up. It is very often, when we have certain results, then I write the paper up, and I produce the final results.

How about mathematical proofs? Do you like to prove your theories or you just came up with some theorem, and you know that it's correct and you don't like to write a complete proof or you prefer to do that?

Of course, if you publish it, you should write a proof and you should write it in reasonable big details. When I write a proof, I usually do so, this is my style of writing. I also provide some intuitive application. There are also other styles, that are strictly formal, that say this is this, and this is this, and it can go several pages, and one doesn't really know what is happening. Some people think this is not good, but I think it is good that I always like explanations, like now we do this because we try to get this at the end, and so forth.

And about examples in writing?

Examples I like really much. I liked very much, with this Romanian, my very good friend, Alexandru Mateescu, who died three years ago. We were different in this sense, I always provided an example when we came up to a new thing, and then he started to generalize it to get algebraic generalizations, and I wanted to have specific examples to see where it leads to.

What is the topic that you maybe would like to say, and that I would ask, and I didn't ask about? Maybe some things considering work with students, after so many years of experience?

There are of course many things, well one thing I would like to say is a personal thing, I like classical music very much. I usually say that if you have a very beautiful mathematical results, this is something like Beethoven quartetto or something like this. Mathematics can be really very beautiful and this is what I also like to say, that mathematics is a great fun. If you really have some problem and you are really making some progress and prove it, then there is no other thing that I would like to do more. Like I want to watch football and my favorite example is that there was a World

Cup Final in football, it was between Germany and Argentine in 1990, and at the same time I had a really a very nice thing to write. Then finally I watched the final, but immediately I came to this that was interesting.

Are you playing some instrument?

I'm not playing myself. This is also when I compare music and mathematics, it is that you can really enjoy in music without being professional, but I doubt whether you could really enjoy mathematical beauty without being, at least to some extent, professional.

5 Reprints

1. Paper 1
   ”On many-valued systems of logic”, *Ajatus*, Vol. 22, 1959, 115-159.

2. Paper 2
   ”On the composition of functions of several variables over a finite set”, *Annales Universitatis Turkuensis,* Ser. A I, Vol. 41, 1960, 1-48.

3. Paper 3
   ”A theorem concerning the composition of functions of several variables ranging over a finite set”, *Journal of Symbolic Logic*, Vol. 25, No. 3, 203-208.

4. Paper 4
   ”On the number of simple bases of the set of functions over a finite domain”, *Ann. Univ. Turku*, Ser. A I, 52, 1962, 1-4.

5. Paper 5
   ”Some completeness criteria for sets of functions over a finite domain, I, *Ann. Univ. Turku*, Ser. A I, Vol. 53, 1962, 1-10.

6. Paper 6
   ”Some completeness criteria for sets of functions over a finite domain, II, *Ann. Univ. Turku*, Ser. A I, Vol. 63, 1963, 1-19,
   Russian translations of two previous papers in Kibernetitseskii sbornik 8 (1964), 8-32.

7. Paper 7
   ”On sequences of functions over an arbitrary domain”, *Ann. Univ. Turku.*, Ser. A I, Vol. 62, 1963, 1-5.

8. Paper 8
   ”Some analogues of Sheffer functions in infinite-valued logics”, *Proc. Colloq. Modal and Many-Valued Logics*, Helsinki 1962, 227-235.

9. Paper 9
   ”On basic groups for the set of functions over a finite domain”, *Ann. Acad. Scient. Fennicae*, Ser. A I, Vol. 338, 1963, 1-15.

10. Paper 10
    ”On infinitely generated sets of operations in finite algebras”, *Ann. Univ. Turku*, Ser. A I, Vol. 74, 1964, 1-13.

11. Paper 11
    ”On the heights of closed sets of operations in finite algebras”, *Ann. Acad. Scient. Fennicae*, Ser. A I, Vol. 363, 1965, 1-12.

12. Paper 12
    ”On some algebraic notions in the theory of truth-functions”, *Acta Philos. Fennica*, Vol. 18, 1965, 193-202.

13. Paper 13
    ”On essential variables of functions especially in the algebra of logic”, *Ann. Acad. Sci. Fennicae*, Ser. A I, Mathematica, No. 339, Helsinki, 1963, 1-11.

14. Paper 14
    ”Matematiikka ja tietokone”, *Arkhimedes*, No. 2, 1968, 5-9.

On Many-valued Systems of Logic

BY

ARTO SALOMAA

1. HISTORICAL AND PHILOSOPHICAL REMARKS

1.1. The present paper is divided into two parts. In the first part we outline the historical development of many-valued logical systems and discuss philosophical problems concerning many-valued logics in general. A certain problem of many-valued propositional calculus is investigated in the second part. The author is indebted to Professor Georg Henrik von Wright for many valuable suggestions, especially in the first part of the paper.

In a many-valued system of logic the principle »Every proposition is either true or false» is not valid. Instead of two truth-values, »truth» and »falsity», there are three or more truth-values. The principle mentioned is replaced by another such as »Every proposition is true or false or tertium». From a philosophical point of view, the difficulty with the many-valued systems consists in finding an interpretation of the truth-values involved in the system. Without an interpretation assigning a meaning to the truth-values the given many-valued logic remains an abstract structure. The originators of many-valued logics have had various interpretations in mind, as will be seen in the following brief historical remarks.

The first forerunners[1] of many-valued logics were MacColl and

[1] The history of the law of the excluded middle lies beyond the scope of this work. We refer to some works among the vast literature on this subject. Lukasiewicz is of the opinion that while Aristotle was

PEIRCE. The former refers to his logic as a »logic of three dimensions», opposite to the logic of Schröder and that of Venn which have only two dimensions. [Cf. MacColl, p. 182.] MacColl divides all propositions into three classes:
propositions which are certain, i.e. always and necessarily true; propositions which are impossible, i.e. always and necessarily false; and propositions which are variable, i.e. which can be true or false. As examples of these classes, respectively, he mentions the following propositions: »$2 + 3 = 5$», »$\sim (2 + 3 = 5)$» and »$x = 2$». [Cf. Lovett, pp. 166—68 and MacColl, p. 157.] The logic of MacColl is developed in the form of an algebra where the law of the excluded fourth holds, i.e. every proposition belongs to one of the three classes.

familiar with this law he did not accept it without reservations because it is not applicable to propositions which refer to future contingent events. The actual inventor of this law was Chrysippus, a founder of the Stoic school. Therefore, we should rather speak of »non-Chrysippian» than of »non-Aristotelian» logics. [Cf. Lukasiewicz 2, pp. 63—64 and 75—76; and Lukasiewicz 3. The Stoic insistence that every proposition must be either true or false is pointed out also in Bochenski, p. 91.] Opposite views have been stated especially in a discussion concerning the matter during recent years. [Cf. eg. Anscombe. Most of the papers belonging to this discussion have appeared in the »Philosophical Review». The view that Aristotle did not want to introduce a third truth-value has been expressed earlier in Becker. Cf. also Prior 2 where strong evidence is given to the opinion that if Aristotle had a three-valued logic then his disjunction was not truth-functional.]

There is an extensive study by Michalski concerning the history of the law of the excluded middle during the Middle Ages. [Cf. Michalski, especially pp. 285—331.] It is emphasized that both Duns Scotus and Occam considered it necessary to introduce a third truth-value. Their argument was based, following Aristotle, on propositions which refer to future contingent events. On p. 301 of Michalski's work we read:

> »... dans l'argumentation d'Ockham l'idée d'une troisième valeur dans la logique n'est pas le résultat d'une discussion théologique, mais en est un instrument tiré du traité d'Aristote De Interpretatione. Jean Duns Scot puisait sans nul doute aussi à ce même traité, quand il expliquait l'essence des propositions qui ne sont ni vraies ni erronées, complexa neutra.»

[Cf. Lovett, pp. 166–68.] MacColl applies his logic especially to the calculus of probabilities. In fact, he is to be considered as a forerunner of the view which interprets truth-values as probabilities.

Peirce has expressed his ideas in a rather fragmentary form, mostly in an unpublished paper »Minute Logic», dated 1902. He speaks of a »trichotomic mathematics» which could be interpreted as mathematics with three truth-values. However, he thinks that a trichotomic mathematics entirely free from any dichotomic element is impossible. [Cf. Peirce 4.308.] Peirce failed to develop his trichotomic system to any considerable degree.

The work of VASILIEV which was published about ten years later but has remained fairly unknown comes closer to the modern conception of a many-valued logic. Vasiliev has in his logic three »forms of the judgment»: simple affirmation »S is P»; simple negation »S is non-P»; and combination of the affirmation and of the negation (indifferent judgment) »S is simultaneously P and non-P». [Vasiliev, p. 108.] The law of the excluded fourth is valid. Vasiliev constructs a consistent system on the basis of these suppositions. In essential, Vasiliev's theory was directed against conceiving the principle of contradiction in too general a fashion.

We quote finally a statement by GUTHRIE from 1916 where some main ideas leading to a many-valued logic are very clearly expressed. [Guthrie, pp. 157 and 336.] Guthrie did not develop his ideas any further.

> »Not only can logic include more than the logic of Aristotle, as the modern logistic does, there might have been non-Aristotelian logics with principles different from the familiar laws of contradiction and excluded middle. What final authority would judge between the ultimate 'correctness' of Aristotle's logic which offers two contradictories, obeying the laws: $x \cdot x' = 0$, $x + x' = 1$, $(x')' = x$, and a logic which would provide three contradictories, obeying the laws: $x \cdot x' \cdot x'' = 0$, $x + x' + x'' = 1$, $(x')' = x''$, $(x'')' = x$? It is true that we can only discuss other logics in terms of one logic, but this is no more a proof that they are therefore unreal than is the fact that an Englishman in discussing German must use English, a proof that English is the a priori condition of communication, valid for all times and all places.»

1.2. The actual discovery of many-valued logics was made independently by LUKASIEWICZ and POST about 1920.

Lukasiewicz published a three-valued logic in 1920 which he generalized two years later into a logic with any denumerable number of truth-values. [Cf. Lukasiewicz 1 and Tarski, p. 47.] The l'idée-force leading Lukasiewicz to the discovery of many-valued systems of logic is his conviction that two-valuedness is not adequate for modal logic. He chooses three principles to be the basis for modal logic. Of these we mention the third: for some *p*, it is possible that *p* and it is possible that not-*p*. This principle is the result of a study concerning propositions about future contingent events. Using this principle and the hypothesis that the modal operator M (»it is possible that») is a two-valued functor, Lukasiewicz easily deduces some contradictions from well-known tautologies of the two-valued propositional calculus. [Cf. Lukasiewicz 2, pp. 53—62. The principle mentioned above is the main source of contradictions. The other two principles only make modal concepts unnecessary by reducing M*p* to *p*.] These difficulties are overcome by the introduction of a third truth-value. And Lukasiewicz concludes [Lukasiewicz 2, p. 71]:

> »... alle für modale Aussagen überlieferten Sätze sind im dreiwertigen Aussagenkalkül widerspruchsfrei erwiesen. Dieses Resultat scheint mir im hohen Grade bemerkenswert zu sein. Es hat nämlich den Anschein, als ob unsere, mit den Begriffen der Möglichkeit und Notwendigkeit verbundenen Intuitionen auf ein logisches System hinweisen würden, dass von der gewöhnlichen, auf dem Zweiwertigkeitssatz gegründeten Logik grundsätzlich verschieden ist.»

Although the value of Lukasiewicz's discovery is not to be underestimated, the argument which led him to this discovery seems to be rather vague. The problems of modal logic and those of truth-logic are on different levels, and solutions are not found by simply introducing an intermediate truth-value »possible». Lukasiewicz's whole argument rests on the hypothesis that modal operators are truth-functional. This leaves only four choices for each (one-place) modal operator, eg. M, and none of them corresponds to our intuitive ideas of M. On the other hand, Lukasiewicz takes these intuitive ideas to be the basis for modal logic. Therefore it is no wonder that contradictions arise. Lukasiewicz's hypothesis is to be rejected because it has been generally accepted that modal operators are not truth-functional but more like quantifiers. [Cf. Prior 1 and Prior 2, p. 324.] Of course, these remarks have no bearing on the formal results of Lukasiewicz.[1] They merely make it questionable whether his three-valued system possesses an intuitively acceptable interpretation. [This is claimed in Lukasiewicz 2, p. 74.]

We mention finally an interesting problem formulated by Lukasiewicz: what is the difference between an m- and n-valued logic $(m > 2, n > 2)$, especially from a philosophical point of view? [Cf. Lukasiewicz 2, p. 73.] Lukasiewicz was earlier of the opinion that only three-valued and infinite-valued logics have philosophical importance, and n-valued logic is essentially the same as three-valued logic, for any finite n. [Lukasiewicz 2, p. 73.] Later on, while studying a new system of modal logic, he changed his opinion. [Lukasiewicz 4, p. 129.] The whole problem is still far from a satisfactory solution. It is closely related to the problem which will be discussed in section 1.6. In the solution especially some formal results have to be taken into consideration. [Cf. Kalicki, p. 177.]

Post discovered many-valued logics independently of Lukasiewicz and published his results in 1921. [Post, pp. 180—85.] He never published anything concerning the matter since then and thus his contributions to the theory of many-valued logics fill only six pages. Unlike Lukasiewicz who begins with a three-valued system and generalizes it afterwards, Post presents his ideas at once in their full generality. He even considers an arbitrary number of designated truth-values while Lukasiewicz has only one designated truth-value. [For the notion of a designated truth-value, cf. Rosser-Turquette, p. 12.] On the other hand, Post does not generalize his systems to contain an infinite number of truth-values. He does not try to find an intuitively acceptable interpretation for his systems.

[1] It is customary in the literature to refer to these results as the »Lukasiewicz-Tarski calculi». It is to be emphasized that only the definition of the modal operator M in terms of implication C and negation N is due to Tarski. [Cf. Lukasiewicz 2, p. 66; and Tarski, p. 38.]

His many-valued logics are a direct generalization of the truth-table technique invented by him.

1.3. In the following four sections we shall discuss some of the major philosophical problems concerning many-valued logics in general. The interpretation of the truth-values is one of them. Lukasiewicz had in mind three modal concepts »necessity», »contingency» and »impossibility» for his three-valued logic. As seen above, there are several difficulties involved in this kind of interpretation of the truth-values. It seems more plausible to interpret the truth-values through epistemic concepts such as »known», »unknown» and »undetermined», or »verified», »falsified» and »undecided». If this is done then the set consisting of »true» and »false» is replaced by a set consisting of three epistemic concepts. This does not necessarily mean rejection of the law of the excluded middle but only indicates that the latter set is more useful than the former. The same thing is expressed by Baylis as follows [Baylis, pp. 164—65]:

> »Of course it may be that some who deny that every proposition is either true or false do so not because they confuse truth and verifiability but because they wish to use the word 'truth' to signify what is ordinarily signified by the word 'verifiability'. With such persons there seems little need to dispute, for what they propose is only a terminological change and they could not object logically to the use of some other word for what is now signified by the word 'truth' . . . Much more important than such terminological considerations are such questions as the following. Are there sets of concepts, other than the truth-falsity set, such that every proposition exemplifies at least one member of the set and that the concepts of the set together exhaust the relevant possibilities? If there are such sets, are they more useful than the truth-falsity set? . . . For any such exhaustive classification of propositions into *n* classes the work of Lukasiewicz and Tarski has provided us with an *n*-valued matrix calculus for the precise statement of certain relations between members of these various classes.

When the number of truth-values grows larger then the interpretation becomes still more difficult. Some have tried to identify the truth-value of a proposition with probability. However, this is futile because of the following reason noticed first by Mazurkiewicz. [Cf. Zawirski 1, pp. 516—17.] In all existing systems of many-valued logic disjunction is truth-functional, i.e. the truth-value of a disjunction is known when the truth-values of both components are known. The same does not hold true with respect to the probability of a disjunction. There are some attempts in the literature to overcome this difficulty by letting the truth-value of a disjunction depend on the truth-values of both components and, in addition, on a third independent parameter. [Cf. Reichenbach 1 where this parameter is called »Kopplungsgrad». The question has been studied more thoroughly by Zawirski. The remarks above apply to both disjunction and conjunction. Cf. Zawirski 2.] According to the theory of Zawirski, in an n-valued logic there are n-1 possibilities for the truth-value of a disjunction after the truth-values of both components have been fixed. This is not plausible and, therefore, this solution of the problem is not satisfactory. [Cf. Zawirski 2, especially p. 440.] So no advantage for many-valued logic is derived from this interpretation. On the other hand, the calculus of probabilities can be developed within the framework of two-valued logic and, thus, there is no use of combining these two things.

To sum up, we see that the problem of finding an interpretation for the truth-values is still far from a satisfactory solution, at least in the general n-valued case. This need not deter us. The abstract nature of truth-values has been indicated already by Peirce. [Cf. Peirce 3.366.] And in the formal development of many-valued logic the semantical meaning of truth-values is quite unessential. As a matter of fact, it is an advantage from the formal point of view that we have no prejudices regarding the possible interpretations.

The precise formal development of many-valued logic has so far not been carried beyond the level of the first order predicate calculus. It seems probable that when one has constructed many-valued logics which are at least rich enough to include a theory of numbers then it is also easier to find a plausible interpretation for the truth-values. [Cf. also Rosser-Turquette, p. 2.]

1.4. A variety of problems arises from the fact that, as it is claimed, in the development of a many-valued logic the meta-language is two-valued. This was pointed out already by Post [Post, p. 185.] as follows:

> »We must however take into account the fact that our development has been given in the language of ${}_1T_2$ and for that very reason every other kind of system appears distorted. This suggests that if we translate the entire development into the language of any one ${}_\mu T_m$ by means of its interpretation, then it would be the formal system most in harmony with regard to the two developments.»

Since then, the alleged two-valuedness of the meta-language has been the chief argument used by the opponents of many-valued logic. [Cf. eg. Linke who refers to many-valued logics as only »logoide Formalismen».] To meet this objection, one can state that n-valued logic is not meant to be the only existing logic. It is used for those purposes for which it suits better than two-valued logic. [This is also the point of Rosser and Turquette. Cf. Rosser-Turquette, p. 1.] It is not even necessary to go so far because the whole question about the two-valuedness of the meta-language is unclear. The two-valuedness of the meta-language is doubtful, if not untrue, and at least cannot be precisely stated without a formalization of the meta-language.

As regards the critisisms directed against many-valued logics, a couple of other points are to be mentioned. Leblanc points out that if the number of designated truth-values in an n-valued logic is greater than one then the epistemological significance of n-valued tautologies is obscure. [Leblanc, p. 45.] In our estimation, it will then be more difficult to find a satisfactory interpretation for the designated truth-values than for the undesignated ones.

The following fact noticed by Frey might be very fruitful for further study. We cannot define a many-valued logic by using only the axiomatic method. An ordinary axiomatization does not involve many-valuedness. The latter is obtained by introducing truth-tables. [Cf. Rosser-Turquette where the difference between a »truth-value stipulation» and an »axiomatic stipulation» is pointed out.] In order to obtain a many-valued logic through the axiomatic method, we should introduce a separate axiom system for each of the truth-values. In the following quotation [Frey, p. 58] Frey refers to three-valued logic.

> »Eine mehrwertige Logik ist vom axiomatischen Standpunkt aus erst dann mehrwertig, wenn für alle Grundbereiche ein eigenes Axiomensystem angegeben werden kann. Es muss aber klar sein, dass die drei verschiedenen Axiomensysteme als solche ohne jeden inneren Zusammenhang sind. Dieser Zusammenhang ist nicht axiomatischer, sondern wieder rein funktionaler Natur. Es bleibt also die vorhin ausgesprochene Tatsache bestehen, dass die Mehrwertigkeit einer Logik nur vom funktionalen Standpunkt aus sinnvoll ist, während eine Logik vom axiomatischen Standpunkt aus immer aristotelisch, d.h. zweiwertig ist.»

1.5. Many-valued logic is often compared with non-Euclidean geometry. Euclidean and non-Euclidean geometry cannot be given preference over one another on purely formal grounds, and the same holds true with respect to two-valued and many-valued logic. [Cf. eg. Ushenko. Cf. also Post, pp. 182—85, where the following interesting difference between point spaces and »truth spaces» is studied: we are able to intuite a three-dimensional point space but only a two-dimensional truth space.] This analogy has been carried even farther. Just like only one geometry is true of the actual world, some authors claim that only one logic is »right», i.e. only one logic can be accepted as actual logic. [Cf. Ushenko, p. 612.] Lukasiewicz is of the opinion that the choice between a two-valued and a many-valued logic is not arbitrary. Experience will decide which of these logics is right. [Cf. Kokoszyńska.] Lukasiewicz does not, however, indicate how this decision is made and which logic experience is based upon.

This analogy does not seem well-established. There are no fixed laws of logic which could be found out in the same way as the laws of the universe. At this point, we share the view of Lewis [Lewis, pp. 483—84.]:

> »There are no 'laws of logic' which can be attributed to the universe or to human reason in the traditional fashion. What are ordinarily called 'laws of logic' are nothing but explicative or analytic statements of the meaning of certain concepts, such as truth and falsity,

> negation, 'either-or', implication, consistency, etc., which are taken as basis.
>
> A 'system of logic' is nothing more than a convenient collection of such concepts, together with the principles to which they give rise by analysis of their meaning.
>
> There are an unlimited number of possible systems of logic, each such that every one of its laws is true and is applicable to deduction. These systems are alternatives in the sense that concepts and principles belonging to one cannot generally be introduced into another — because of fundamental differences in category.
>
> . . .
>
> Sufficiency for the guidance and testing of our usual deductions, systematic simplicity and convenience, accord with our psychological limitations and our mental habits, and so on, operate as criteria in our conscious or unconscious choice of 'good logic'. Any current or accepted canon of inference must be pragmatically determined. That one such system should be thus accepted does not imply that the alternative systems are false: it does imply that they are — or would be thought to be — relatively poorer instruments for the conduct and testing of our ordinary inferences.»

1.6. Many-valued logical systems have purely theoretical interest as formal systems of a certain kind. From a pragmatic point of view, however, it is natural to ask whether these systems have useful applications. More precise formulations of this question would be: what problems can be solved by means of many-valued logics which cannot be solved by the ordinary two-valued logic, or what are the problems whose solution is simplified by the use of a many-valued logic? [Cf. also Rosser-Turquette, pp. 110—11.] This question is closely related to the one discussed in section 1.3 and, therefore, it is natural that very little has been found out so far.

Many-valued logics seem to lead the way out of certain well-known paradoxes. Bochvar has developed a three-valued system of logic without a theory of types and shown that Russell's paradox cannot arise in this system. [Cf. Szmielew.] Recently, Skolem has obtained a more general result. Suppose a definition of a set is built of statements of the form »*u* belongs to *v*» by using only sentential connectives. Then, according to Skolem's result, no contradiction can arise from this definition, provided that the connectives involved are interpreted as in Lukasiewicz's infinite-valued propositional calculus. [Cf. Skolem, pp. 1—6.]

. The idea that many-valued logics may have applications in physics was suggested by certain results which, according to some physicists, called for a new type of reasoning. Thus in Zwicky we read:

> »From a deeper scrutiny of the foundations of scientific truth it follows that every scientific statement referring to observations should possess a certain minimum degree of flexibility. In other words, no set of two-valued truths can be established with the expectation that this set ultimately will stand the test of experience. Formulations of scientific truth intrinsically must be many-valued.»

Many authors have taken it for granted that the logic of modern science is at least three-valued. [Cf. eg. Reichenbach 2, pp. 144—48 and 160—66.] In more recent years one has become more cautious concerning the necessity of the use of a many-valued logic in physics. [Cf. Margenau and Rosser-Turquette, p. 2. Cf. also Birkhoff—von Neumann where it is clearly pointed out that from the point of view of quantum mechanics distributive identities are the weakest link in logic and so there is no special need for many-valuedness.] It has been emphasized that new systems of logic are highly interesting and useful in their own right but their establishment need not be justified by the allegation that they are implied by scientific procedures. It has also been pointed out that one cannot use three-valued logic and, at the same time, some parts of mathematics which are based on two-valued logic. [This is done, for instance, in Reichenbach 2. Cf. Margenau, p. 87.] Thus the possibilities of the use of many-valued logics in modern science are still unclear and the proposals made so far are to be considered premature.[1]

2. GENERALIZED CONNECTIVES

2.1. In what follows we shall study generalizations of the familiar connectives in two-valued propositional calculus: implication,

[1] We consider as premature also some recent more or less informal attempts to apply many-valued logics in ethics. [Cf. Cohen.]

equivalence, negation, conjunction and disjunction. This is one of the problems in many-valued propositional calculus.[1] It is not clear how, for instance, implication is most suitably characterized in an n-valued propositional calculus. Therefore, it is natural to ask how one can define connectives for n-valued propositional calculus which are analogous to those in two-valued calculus.

After a few historical remarks we discuss various conditions which may be imposed upon the generalizations in question. Furthermore, we choose some sets of these conditions and investigate problems concerning consistency and independence. (Sections 2.2—2.5.) Then we establish interconnections between Sheffer functions and generalized connectives (section 2.6), investigate methods of deciding whether a given function satisfies a certain condition (section 2.7), as well as methods of calculating the number of functions satisfying a certain condition (sections 2.8—2.9). Finally, we obtain results concerning the validity of some tautologies of two-valued propositional calculus when the connectives involved are replaced by some generalized ones and the calculus is considered to be n-valued (section 2.10).

The first generalized implication was introduced by LUKASIEWICZ. [Cf. Lukasiewicz 1 and Lukasiewicz 2, p. 72.] Its truth-function c (x, y) is defined as follows:

[1] We use the word in the sense of Rosser and Turquette. [Cf. Rosser-Turquette, pp. 10—12.] We also apply, without further explanations, some customary terminology such as »well-formed formula» or »wff», »designated truth-value», »truth-function» or shortly »function», and »Sheffer function». [Cf. Rosser-Turquette, pp. 10—12 and 25.] We shall always use the numbers $1, 2, \ldots, n$ to denote truth-values and the numbers $1, \ldots, d$ to denote designated truth-values ($d < n$). d and n are used instead of S and M in Rosser-Turquette. So the number of truth-values is considered to be finite. We refer to 1 as the »greatest» truth-value and to n as the »least» truth-value. Thus, by the expression »a greater truth-value» is to be understood »a numerically less truth-value». All operations, eg. addition, are carried out modulo n. We finally mention that for our purposes it is not necessary to introduce in the meta-language new names for the variables and connectives. Thus, we simply let every variable, connective and wff serve as its own name.

$$c(x, y) = \max(1, 1-x+y).$$

Lukasiewicz does not motivate the choice of this particular function. However, his function satisfies most of the requirements for a generalized implication, as will be seen in section 2.2. This is the case only when the number of designated truth-values is one.

According to Lewis and Langford, implication is any connective whose truth-function c (x, y) satisfies the following condition: if i is designated and j undesignated then c (i, j) is undesignated. [Lewis-Langford, p. 233.] This condition guarantees the validity of modus ponens. In our estimation, however, it is too weak to be an adequate characterization of an implication function. As a matter of fact, in two-valued propositional calculus there are eight functions satisfying it.

A much stronger characterization for an implication function is given by Webb. According to him, c (i, j) has a designated value if and only if $i \geqq j$. [Cf. Webb, pp. 162—64. As a matter of fact, Webb deals with calculi with only one designated value but we have »translated» the condition for the general case. This remark applies also to the reference to Lewis-Langford given above.] In the two-valued case only one function, namely material implication, satisfies this condition. The same condition with the exception that the case $i = j$ is left open is given by Swift. He introduces also the condition that implication should be transitive, as well as a condition whose generalization is condition 12) in section 2.2. [Cf. Swift, p. 615. For the latter, cf. also Dienes.]

For other generalized connectives, very few characterizations are given in the literature. Negation, conjunction and disjunction are usually taken to be the connectives whose truth-functions are, respectively: ne $(x) = n + 1 - x$, k $(x, y) = \max(x, y)$ and a $(x, y) = \min(x, y)$. They originate from Lukasiewicz. [Cf. Lukasiewicz 1 and Lukasiewicz 2, p. 72.] Hempel speaks of a system of generalized negations [cf. Hempel] but, in our estimation, there is no reason for calling his one-place functions negations. The same holds true for the so-called cyclical negation ne $(x) = x + 1$. [Cf. Post, p. 180 and Reichenbach 2, pp. 150—60.] More general conditions for conjunction and disjunction are given by Dienes. [Cf. Dienes.] They are essentially the same as conditions 1), 1′), 7) and 7′) in section 2.5 below. Dienes gives also a list of tautologies of two-valued propositional calculus which are supposed to remain valid when the connectives involved are replaced by the generalized ones and, thus, obtains some further characteristics of the generalized connectives.

Finally, we mention the very strong conditions imposed upon generalized connectives by ROSSER and TURQUETTE. According to them, implication satisfies »standard conditions» if its truth-function c (x, y) assumes an undesignated value if and only if x is designated and y is undesignated. Conjunction satisfies standard conditions if its truth-function k (x, y) assumes a designated value if and only if x and y are both designated. Standard conditions for other connectives are defined analogously. [Rosser-Turquette, pp. 25—26.] Thus, by the definition of generalized connectives, every tautology of two-valued propositional calculus remains valid in n-valued propositional calculus. [Cf. section 2.2.]

2.2. We use capital letters C, E, N, K and A to denote implication, equivalence, negation, conjunction and disjunction, respectively. The corresponding truth-functions will be denoted by small letters: c (x, y), e (x, y), ne (x), k (x, y) and a (x, y). (The function corresponding to negation is denoted by »ne» to avoid confusions with the number of truth-values n.) In this section we discuss the following conditions which may be imposed upon implication. Only such conditions are taken into consideration which can be stated without defining any other generalized connective.

1). For every $i \leqq d$ and $j > d$, c $(i, j) > d$.
2). For some i and j, c $(i, j) \leqq d$ and c $(j, i) > d$.
3). For some $j > d$, c $(i, j) \leqq d$.
4). For some $i \leqq d$ and $j \leqq d$, c $(i, j) \leqq d$.
5). For every i, c $(i, i) \leqq d$.
6′). For all i and j, if $i > j$ then c $(i, j) \leqq d$.
6). For all i and j, if $i \geqq j$ then c $(i, j) \leqq d$.
7). For all i and j, if $i < j$ then c $(i, j) > d$.
8). For all i, j and h, if $i > j$ then c $(h, i) \geqq$ c (h, j).

9). For all i, j and h, if $i > j$ then $c(i, h) \leqq c(j, h)$.

10). Always when $c(h, i) \leqq d$ and $c(i, j) \leqq d$ then also $c(h, j) \leqq d$.

11). $c(i, j) > d$ if and only if both $i \leqq d$ and $j > d$.

12). $c(1, n) = n$ and $c(n, 1) = c(1,1) = c(n, n) = 1$.

In syntactical terms, these conditions read as follows:

1). Modus ponens is a valid rule of inference for implication C.

2). Implication is not commutative (symmetrical). As a matter of fact, this condition defines non-symmetry in a strong sense. Weaker condition would be: for some i and j, $c(i, j) \neq c(j, i)$.

3). $p\mathrm{C}q$ does not require q, i.e. in modus ponens the minor premise is not superfluous.

4). $p\mathrm{C}q$ does not exclude q, i.e. modus ponens is not empty.

5). $p\mathrm{C}p$ is always assertable.

6'). $p\mathrm{C}q$ is assertable when p has a smaller truth-value than q.

6). $p\mathrm{C}q$ is assertable when p has a smaller truth-value than q or a truth-value which is equal to that of q.

7). $p\mathrm{C}q$ is not assertable when p has a greater truth-value than q. (6) and 7) together imply that $p\mathrm{C}q$ is assertable if and only if the truth-value of p is less than or equal to that of q.)

8). Suppose the truth-value of p is less than that of q. Then the inference from any r to p cannot have a greater truth-value than the inference from r to q.

9). Let p, q and r be as in 8). Then the inference from p to r cannot have a smaller truth-value than the inference from q to r.

10). Implication is transitive in the following sense. If $p\mathrm{C}q$ and $q\mathrm{C}r$ are both assertable then also $p\mathrm{C}r$ is assertable.

11). $p\mathrm{C}q$ is assertable if and only if p is not assertable or q is assertable (inclusive »or»).

12). Implication reduces to the standard two-valued one if the »intermediate» truth-values are left out.

At least these conditions (and perhaps some others) have to be taken into consideration when one wants to study the question which among the functions in n-valued propositional calculus might plausibly be considered to be implication functions.

We begin with some obvious remarks concerning conditions

1)—12). Condition 5) implies both 3) and 4), 6) implies 6′), and 6) and 7) together imply conditions 1)—5) and 10). 6′) and 7) together imply 1), 2) and 10), and also 3) and 4) in case $1 < d < n-1$. Condition 11) alone implies 1)—6) and 10). However, 11) is not consistent with 7). There are, namely, $^1/_2\,(n^2-n) - d\,(n-d)$ pairs (i, j) for which c (i, j) has a value $\leqq d$ according to 11) but a value $> d$ according to 7).

After these preliminary remarks we denote certain sets of conditions 1)—12) as follows:

(C_1) is the set consisting of 1), 2), 3) and 4).
(C_2) —»— 1), 2) and 5).
(C_3) —»— 1), 2), 5) and 10).
(C_4) —»— 6) and 7).
(C_5) —»— 6), 7), 8) and 9).
(C_6) —»— 11) alone.
(C_7) —»— 11), 8) and 9).

Definition 2.2.1. A two-place function c (x, y) is an *implication function satisfying* (C_i) if c (x, y) satisfies each condition in the set (C_i) where $i = 1, \ldots, 7$.

It is easily verified that each of the sets (C_i) is strong enough to determine implication uniquely when $n = 2$ and $d = 1$. (If we want to study implications C for which pCp is not always assertable we can replace 6) by 6′) in (C_4) and (C_5). Then the uniqueness in the two-valued case is no more valid. However, theorem 2.2.1 remains valid.)

Furthermore, (C_1) — (C_5) form a sequence of sets of conditions in which each set contains stronger conditions than the preceding set, i.e. if a function satisfies (C_i) then it satisfies also (C_{i-1}) where $i = 2, 3, 4, 5$. The same holds true with respect to (C_1), (C_2), (C_3), (C_6) and (C_7). The sets (C_1) — (C_7), thus, give a pretty good view of conditions of various strengths which may be imposed upon implication, as well as of the contradictoriness of conditions 7) and 11). Any function satisfying (C_5) or (C_7) satisfies ten of our conditions 1)—12). We have entirely omitted condition 12) from the sets (C_i) because, although it is mentioned by some authors [cf. section 2.1], we do not consider it plausible, at least not for all values of n and d. However, one may add it to some or all of the sets (C_i). Theorem 2.2.1 remains valid also in this case, with a couple of exceptions. [Cf. the end of the proof.]

Obviously, the sets (C_i) are *consistent*, i.e. if you choose any one of the sets (C_i) there is a function satisfying all conditions in this set. This is true for any n and d. The following functions $c_1(x, y)$ and $c_2(x, y)$, for instance, suffice to show the consistency of the sets (C_i):

$c_1(x, y) = 1$ for $x \geqq y$, $c_1(x, y) = n$ for $x < y$.
$c_2(x, y) = n$ if both $x \leqq d$ and $y > d$, $c_2(x, y) = 1$ otherwise.

On the other hand, each of the sets (C_i) consists of independent conditions, i.e. no condition in a set (C_i) can be deduced from the other conditions in the same set. Here we have to distinguish between two kinds of independence. Suppose that conditions A and B are consistent, i.e. for any n and d there is a function which satisfies both A and B. We say that A and B are *strongly independent* if, for any n and d where $n \geqq 3$, there is a function which satisfies A but does not satisfy B and a function which satisfies B but does not satisfy A. (The requirement $n \geqq 3$ is made to omit some trivial cases in the following proofs.) A and B are *weakly independent* if, for some n and d, there is a function which satisfies A but does not satisfy B and a function which satisfies B but does not satisfy A.

Theorem 2.2.1. Each of the sets $(C_1) - (C_6)$ consists of strongly independent conditions and the set (C_7) of weakly independent conditions.

Proof. To prove the theorem for the set (C_1) it suffices to show that, for any choice of n and d where $n \geqq 3$, there is a function $f(x, y)$ such that $f(x, y)$ satisfies all conditions 1)–4) except i). Here i) is successively 1), 2), 3) and 4). The following functions have the required properties. We write in front of each function the condition not satisfied by it.

1). $f(x, y) = 1$ if $x \neq n$ or $y \neq 1$ (inclusive »or»), $f(n, 1) = n$.
2). $f(x, y) = 1$ for $x = y$, $f(x, y) = n$ for $x \neq y$.

3). $f(x, y) = 1$ for $y = 1$, $f(x, y) = n$ for $y \neq 1$.

4). $f(x, y) = 1$ for $x = n$, $f(x, y) = n$ for $x \neq n$.

For the proof of the theorem for (C_2), choose the first three functions above. The proof for (C_3) is as follows:

1). $f(x, y) = 1$ for $x = y$, $f(1, n) = 1$, $f(x, y) = n$ otherwise.

2). $f(x, y) = 1$ for $x = y$, $f(x, y) = n$ for $x \neq y$.

5). $f(x, y) = n$ if $x \neq n$ or $y \neq 1$ (inclusive »or»), $f(n, 1) = 1$.

10). If $d = 1$ choose: $f(1, y) = n$ for $y \neq 1$, $f(2, 1) = n$, $f(x, y) = 1$ otherwise.

If $d > 1$ choose: $f(x, y) = n$ if both $x \leqq d$ and $y > d$, $f(n, 2) = n$, $f(x, y) = 1$ otherwise.

The proof for (C_4) and (C_6) is obvious. For (C_5) we have:

6). $f(x, y) = n$ for all x and y.

7). $f(x, y) = 1$ for all x and y.

8). $d = 1$. $f(x, y) = 1$ for $x \geqq y$. For $x < y$, $f(x, y) = n - 1$ if $y = n$ and $f(x, y) = n$ if $y \neq n$.

$d > 1$. $f(x, y) = n$ for $x < y$. For $x \geqq y$, $f(x, y) = 2$ if $y = 2$ and $f(x, y) = 1$ if $y \neq 2$.

9). $d = 1$. $f(x, y) = 1$ for $x \geqq y$. For $x < y$, $f(x, y) = n - 1$ if $x = 1$ and $f(x, y) = n$ if $x \neq 1$.

$d > 1$. $f(x, y) = n$ for $x < y$, $f(1, 1) = 1$, $f(x, y) = 2$ otherwise.

Consider, finally, the set (C_7) and suppose $d > 1$. The following functions show the independence of the conditions in (C_7):

11). $f(x, y) = n$ for all x and y.

8). $f(x, y) = n$ if both $x \leqq d$ and $y > d$, $f(x, 1) = 2$ for any x, $f(x, y) = 1$ otherwise.

9). $f(x, y) = n$ if both $x \leqq d$ and $y > d$, $f(1, 1) = 1$, $f(x, y) = 2$ otherwise.

Obviously, if $d = 1$ then 9) follows from 11). We, thus, have only weak independence for the conditions in the set (C_7). The proof of theorem 2.2.1 has been completed. With some slight changes the proof is modified to remain valid if condition 12) is added to the sets (C_i). However, in this case one obtains only weak independence for (C_5). Both 8) and 9) follow, namely, from the remaining conditions in (C_5) when $n = 3$ and $d = 1$.

No one of the sets (C_i) determines a unique function when $n > 2$, i.e. there are several implication functions satisfying (C_i) for $i = 1, \ldots, 7$. We get a set of conditions which uniquely determines a function if, instead of 8) and 9), we take the following conditions:

8′). For all i, j and h, if $i > j \geqq h$ then $c(h, i) > c(h, j)$.

9′). For all i, j and h, if $h \geqq i > j$ then $c(i, h) < c(j, h)$.

Conditions 8′) and 9′) do not limit the choice of values for $c(x, y)$ when $x > y$, i.e. below the main diagonal of the matrix of $c(x, y)$. But for $x \leqq y$, we have in 8′) and 9′) strict inequalities corresponding to the inequalities in 8) and 9). Let (C_8) be the set consisting of 8), 8′) and 9′). Clearly, (C_8) determines a unique function when $n = 2$. In the following theorem it is seen that this is always the case.

Theorem 2.2.2. (C_8) consists of strongly independent conditions and determines a unique function $c_8(x, y)$. $c_8(x, y)$ satisfies conditions 1)—10) and 12) in case $d = 1$.

Proof. Independence is shown as follows:

8). $f(x, y) = n$ for $x > y$, $f(x, y) = y - x + 1$ for $x \leqq y$.

8′). $f(x, y) = 1$ for $x > y$, $f(x, y) = n - x + 1$ for $x \leqq y$.

9′). $f(x, y) = 1$ for $x > y$, $f(x, y) = y$ for $x \leqq y$.

Consider any function $c(x, y)$ satisfying (C_8). Because of 8′), $c(1, n) > c(1, n-1) > \ldots > c(1, 1)$. This is possible only if $c(1, y) = y$, for any y. Using 9′) we conclude in a similar manner that $c(x, n) = n - x + 1$, for any x. By an obvious inductive argument we obtain the result

$$c(x, y) = y - x + 1 \qquad \text{for } x \leqq y.$$

This shows that $c(i, i) = 1$, for any i. From this it follows by 8) that

$$c(x, y) = 1 \qquad \text{for } x > y.$$

Hence (C_8) determines a unique function $c(x, y)$ which we denote by $c_8(x, y)$. Clearly, $c_8(x, y)$ is the Lukasiewicz implication. [Cf. section 2.1.]

It is readily checked that $c_8(x, y)$ satisfies conditions 1)—10) and 12) if $d = 1$. 11) is never satisfied by $c_8(x, y)$. On the other hand, if $d > 1$ then $c_8(x, y)$ satisfies none of the conditions 1), 7) or 10). Thus, in this case, it cannot plausibly be considered as an implication function.

We have already pointed out the contradictoriness of conditions 7) and 11). Consider the »strongest» sets (C_i) which contain 7) and 11), namely, (C_5) and (C_7). No function satisfies both (C_5) and (C_7) when $n > 2$. The question arises: are the tautologies of two-valued propositional calculus valid when implication is replaced by a generalized connective whose truth-function satisfies (C_5) or (C_7)? Consider, for instance, the following tautologies:

T_1. $pC{:}pCq.Cq$

T_2. $qC.pCq$

T_3. $pCq.C{:}qCr.C.pCr$

T_4. $qCr.C{:}pCq.C.pCr$

T_5. $pC.qCr{:}C{:}qC.pCr$

(We use ordinary punctuation instead of the parenthesis-free notation of Lukasiewicz.)

It is easily seen that any tautology involving only implication is valid if C is a connective whose truth-function satisfies (C_7). In this case, namely, ordinary truth-table technique can be applied. This is illustrated by the following proof of T_5 where »des» stands for a designated value and »und» for an undesignated value.

p	q	r	qCr	$pC.qCr$	pCr	$qC.pCr$	T_5
des	des	des	des	des	des	des	des
des	des	und	und	und	und	und	des
des	und	des	des	des	des	des	des
des	und	und	des	des	und	des	des
und	des	des	des	des	des	des	des
und	des	und	und	des	des	des	des
und	und	des	des	des	des	des	des
und	und	und	des	des	des	des	des

The same does not hold true with respect to (C_5). As a matter of fact, for any n and d where $n > 2$, there is an implication function satisfying (C_5) such that $T_1 - T_5$ are not valid. If $d = 1$ such a function is:

$$c(x, y) = 1 \text{ for } x \geqq y, \ c(x, y) = n - x + 1 \text{ for } x < y.$$

If we now assign for both p and q the truth-value $n - 1$, T_1 will get the undesignated value 2. The assignments $p = 1$, $q = 2$; $p = n - 1$, $q = r = n$; $p = q = n - 1$, $r = n$; and $p = n - 1$, $q = 1$, $r = n$ give the undesignated value $n - 1$ for T_2, T_3, T_4 and T_5, respectively. If $d > 1$ we choose the following function satisfying (C_5):

$c(x, y) = 1$ for $x > y$, $c(x, y) = d$ for $x = y$, $c(x, y) = n$ for $x < y$.

The assignments $p = 1$, $q = n$; $p = q = 1$; $p = n - 1$, $q = n - 2$, $r = n$; $p = n$, $q = n - 1$, $r = 1$; and $p = n$, $q = r = 1$, give the undesignated value n for T_1, T_2, T_3, T_4 and T_5, respectively.

These have been preliminary remarks concerning the validity of tautologies of two-valued propositional calculus when the connectives are replaced by the generalized ones. In section 2.10 we obtain general results concerning this problem. It will be seen, for instance, that there are implication functions satisfying (C_5) such that $T_1 - T_5$ are valid. For T_1, T_3, T_4 and T_5 it is always possible to find such a function but for T_2 only when $d = 1$.

2.3. In the following three sections we shall discuss other connectives: in 2.3 equivalence, in 2.4 negation, and in 2.5 conjunction and disjunction.

Conditions for equivalence function $e(x, y)$:

1). For every i, $e(i, i) \leqq d$. ($p\mathrm{E}p$ is always assertable.)

2). For all i and j, $e(i, j) = e(j, i)$. (Equivalence is symmetrical, i.e. $p\mathrm{E}q$ has the same truth-value as $q\mathrm{E}p$.)

3). If both $e(h, i) \leqq d$ and $e(i, j) \leqq d$ then also $e(h, j) \leqq d$. (Equivalence is transitive with respect to assertability.)

4). $e(i, j) \leqq d$ if and only if both $c(i, j) \leqq d$ and $c(j, i) \leqq d$. (pEq is assertable if and only if both pCq and qCp are assertable. So here we assume that we have defined implication before defining equivalence.)

5). If $i \geqq j \geqq h$ then $e(i, j) \leqq e(i, h)$ and $e(j, h) \leqq e(i, h)$. (This is a condition corresponding to conditions 8) and 9) in section 2.2. I.e. if the truth-value of q is »closer» than that of r to the truth-value of p then pEq cannot have a smaller truth-value than pEr. And if the truth-value of q is closer than that of p to the truth-value of r then qEr cannot have a smaller truth-value than pEr.)

6). $e(i, j) \leqq d$ if and only if either $i \leqq d$ and $j \leqq d$, or $i > d$ and $j > d$. (A condition corresponding to 11) in section 2.2.)

7). $e(1, 1) = e(n, n) = 1$ and $e(1, n) = e(n, 1) = n$. (A condition corresponding to 12) in section 2.2.)

In order to study functions satisfying these conditions we have to specify the implication function $c(x, y)$ mentioned in 4) above. We assume that $c(x, y)$ is an implication function satisfying (C_7). Let (E_1) be the set consisting of conditions 2), 4) and 5) above.

Definition 2.3.1. A two-place function $e(x, y)$ is an *equivalence function satisfying* (E_1) if $e(x, y)$ satisfies each condition in the set (E_1).

Clearly, the conditions in the set (E_1) are consistent, for any n and d. The following function, for instance, satisfies all of them:

$e(x, y) = 1$ if both $x \leqq d$ and $y \leqq d$, $e(x, y) = 1$ if both $x > d$ and $y > d$, $e(x, y) = n$ otherwise.

Theorem 2.3.1. The set (E_1) consists of strongly independent conditions. Furthermore, any function satisfying (E_1) satisfies also conditions 1), 3) and 6).

Proof. Independence is shown as follows:

2). $d < n - 1$. $f(x, y) = 1$ if $x, y \leqq d$ or $x, y > d$. Otherwise, $f(x, y) = n - 1$ for $y = d + 1$, $f(x, y) = n$ for $y \neq d + 1$.

$d = n - 1$. $f(x, y) = n$ if $x = n$ or $y = n$ (exclusive »or»). Otherwise, $f(x, y) = 2$ for $y = 2$, $f(x, y) = 1$ for $y \neq 2$.

4). $f(x, y) = 1$, for all x and y.

5). $d < n - 1$. $f(x, y) = 1$ if $x, y \leqq d$ or $x, y > d$. $f(n, 1) = f(1, n) = n - 1$. Otherwise, $f(x, y) = n$.

$d = n - 1$. $\mathrm{f}(x, y) = n$ if $x = n$ or $y = n$ (exclusive »or»). $\mathrm{f}(1, 1) = 2$. Otherwise, $\mathrm{f}(x, y) = 1$.

Since $\mathrm{c}(x, y)$ was supposed to satisfy (C_7), $\mathrm{c}(i, i) \leqq d$ and, furthermore, $\mathrm{c}(i, j) > d$ if and only if both $i \leqq d$ and $j > d$. Therefore, it is clear that 1) and 6) are satisfied by any function satisfying 4) and, hence, by any function satisfying (E_1). Finally, suppose that $\mathrm{e}(x, y)$ satisfies (E_1) and that $\mathrm{e}(h, i) \leqq d$ and $\mathrm{e}(i, j) \leqq d$. Then also, by 4), $\mathrm{c}(h, i) \leqq d$, $\mathrm{c}(i, h) \leqq d$, $\mathrm{c}(i, j) \leqq d$ and $\mathrm{c}(j, i) \leqq d$. From this it follows that $\mathrm{c}(h, j) \leqq d$ and $\mathrm{c}(j, h) \leqq d$. Therefore, $\mathrm{e}(h, j) \leqq d$ and, thus, condition 3) is satisfied by any function satisfying (E_1). The proof of theorem 2.3.1 has been completed.

If we do not assume that $\mathrm{c}(x, y)$ satisfies (C_7), theorem 2.3.1 does not, in general, hold. For instance, if we assume that $\mathrm{c}(x, y)$ is an implication function satisfying (C_5) then conditions 4) and 6) will always be contradictory and, furthermore, 2) will follow from 4) when $d = n - 1$.

The set (E_1) does not determine a unique function (except when $n = 2$). Uniqueness is obtained by strengthening condition 5) as follows:

5'). If $i \geqq j > h$ then $\mathrm{e}(i, j) < \mathrm{e}(i, h)$.

5''). If $i > j \geqq h$ then $\mathrm{e}(j, h) < \mathrm{e}(i, h)$.

Let (E_2) be the set consisting of 2), 5') and 5''). For the following theorem, let $\mathrm{c}(x, y)$ be an implication function satisfying (C_i) where i is some of the numbers $2, \ldots, 7$.

Theorem 2.3.2. (E_2) consists of strongly independent conditions and determines a unique function $\mathrm{e}_2(x, y)$. $\mathrm{e}_2(x, y)$ satisfies conditions 1), 3), 4) and 7) if $d = 1$.

Proof. Independence is shown as follows:

2). $\mathrm{f}(x, y) = 1$ for $x \leqq y$, $\mathrm{f}(x, y) = x - y + 1$ for $x > y$.

5'). $\mathrm{f}(x, y) = 1$ for $x = y$, $\mathrm{f}(x, y) = x$ for $x > y$, $\mathrm{f}(x, y) = y$ for $x < y$.

5''). $\mathrm{f}(x, y) = 1$ for $x = y$, $\mathrm{f}(x, y) = n - y + 1$ for $x > y$, $\mathrm{f}(x, y) = n - x + 1$ for $x < y$.

Uniqueness is shown in the same way as in the proof of theorem 2.2.2. The function $\mathrm{e}_2(x, y)$ will be:

$$e_2(x, y) = |x - y| + 1.$$

It is readily checked that this function satisfies 1), 3), 4) and 7) when $d = 1$. This completes the proof.

6) is never satisfied by $e_2(x, y)$, and if $d > 1$ neither 3) nor 4) is satisfied by it. So $e_2(x, y)$ cannot plausibly be regarded as an equivalence function when $d > 1$.

2.4. Conditions for negation:

1). For every $i \leqq d$, $\mathrm{ne}(i) > d$. (Always when p is assertable, Np is not assertable. 1') is a weaker formulation of 1).)

1'). For some $i \leqq d$, $\mathrm{ne}(i) > d$.

2). For every $i > d$, $\mathrm{ne}(i) \leqq d$. (Always when p is not assertable, Np is assertable. 1) and 2) together express that negation converts assertable statements into non-assertable, and vice versa. 2') is a weaker formulation of 2).)

2'). For some $i > d$, $\mathrm{ne}(i) \leqq d$.

3). For all i and j, if $i > j$ then $\mathrm{ne}(i) \leqq \mathrm{ne}(j)$. (If p has a greater truth-value than q then Np cannot have a greater truth-value than Nq.)

4). $\mathrm{ne}(1) = n$ and $\mathrm{ne}(n) = 1$. (A condition corresponding to 12) in section 2.2 and 7) in section 2.3.)[1]

Let (N_1) be the set consisting of 1), 2') and 3); (N_2) the set consisting of 1'), 2) and 3); and (N_3) the set consisting of 1), 2) and 3). The conditions in each of the sets (N_i) are, clearly, consistent. Furthermore, each of the sets (N_i) is »strong» enough to determine negation uniquely in the two-valued case.

Definition 2.4.1. A one-place function ne (x) is a *negation function*

[1] We do not consider the following condition given by Hempel [cf. Hempel, p. 28] as a characteristic of negation:

$$\text{for some } i,\ \mathrm{ne}(x) \leqq d \text{ if } x = i \text{ and } \mathrm{ne}(x) > d \text{ if } x \neq i.$$

That it holds true in the two-valued case is due merely to the fact that in this case it expresses the same thing as conditions 1) and 2) above. [Cf. also Rosser-Turquette, p. 26. Here negation is given separately from the functions satisfying Hempel's condition.]

satisfying (N_i) if $\mathrm{ne}(x)$ satisfies each condition in the set (N_i) where $i = 1, 2, 3$.

Theorem 2.4.1. Each of the sets $(\mathrm{N}_1)-(\mathrm{N}_3)$ consists of weakly independent conditions.

The proof is straightforward. That we obtain only weak independence is due to the fact that 3) follows from 1) when $d = n - 1$, and from 2) when $d = 1$.

A unique negation is obtained if we strengthen condition 3) as follows:

3′). For all i and j, if $i > j$ then $\mathrm{ne}(i) < \mathrm{ne}(j)$.

If we denote, in analogy with the preceding sections, the set consisting of 3′) alone by (N_4) we get the obvious

Theorem 2.4.2. (N_4) determines a unique function $\mathrm{ne}_4\,(x)$ which satisfies conditions 1)—4) in case n is even and $d = \frac{n}{2}$.

$\mathrm{ne}_4\,(x)$ is the negation of Lukasiewicz:

$$\mathrm{ne}_4\,(x) = n - x + 1.$$

It does not satisfy 1) if $d > \frac{n}{2}$, and does not satisfy 2) if $d < \frac{n}{2}$.

So $\mathrm{ne}_4\,(x)$ satisfies one of $(\mathrm{N}_1) - (\mathrm{N}_3)$, for any n and d.

2.5. Conditions for conjunction:

1). For all i and j, $\mathrm{k}\,(i, j) = \mathrm{k}\,(j, i)$. (Symmetry.)

2) For every i, $\mathrm{k}\,(i, i) = i$. ($p\mathrm{K}p$ has the same truth-value as p.)

3) For all i, j and h, $\mathrm{k}\,(i, \mathrm{k}\,(j, h)) = \mathrm{k}\,(\mathrm{k}\,(i, j), h)$. (Conjunction is associative.)

4). For all i, j and h, if $i > j$ then $\mathrm{k}\,(i, h) \geqq \mathrm{k}\,(j, h)$. (Conditions 1)—4) are common characteristics of both conjunction and disjunction. The following ones characterize conjunction alone.)

5). If $i > j \geqq h$ then $\mathrm{k}\,(i, h) > \mathrm{k}\,(j, h)$.

6). $\mathrm{k}\,(i, j) \leqq d$ if and only if both $i \leqq d$ and $j \leqq d$.

7). $\mathrm{k}\,(1, 1) = 1$, $\mathrm{k}\,(1, n) = \mathrm{k}\,(n, 1) = \mathrm{k}\,(n, n) = n$. (6) corresponds to 11) in 2.2, 6) in 2.3 and 1)—2) in 2.4. 7) corresponds to 12) in 2.2, 7) in 2.3 and 4) in 2.4.)

Let (K_1) be the set consisting of 1), 2) and 5).

Definition 2.5.1. A two-place function $k(x, y)$ is a *conjunction function satisfying* (K_1) if $k(x, y)$ satisfies each condition in the set (K_1).

Theorem 2.5.1. (K_1) consists of strongly independent conditions and determines a unique function $k_1(x, y)$. Furthermore, $k_1(x, y)$ satisfies conditions 3), 4), 6) and 7).

Proof. Independence is shown as follows:

1). $f(x, y) = \max(x, y)$ for $x \geqq y$, $f(x, y) = 1$ for $x < y$.

2). $f(x, y) = \max(x, y)$ for $x \neq y$, $f(x, y) = 1$ for $x = y$.

5). $f(x, y) = 1$ for $x \neq y$, $f(x, y) = x$ for $x = y$.

Uniqueness follows easily from the fact that condition 2) determines all values of $k_1(x, y)$ where $x = y$, condition 5) determines all values of $k_1(x, y)$ where $x > y$, and condition 1) determines the remaining values of $k_1(x, y)$. It is seen that

$$k_1(x, y) = \max(x, y).$$

It is clear that $k_1(x, y)$ satisfies conditions 4), 6) and 7). The satisfaction of condition 3) follows because, for any i, j and h,

$$\max(i, \max(j, h)) = \max(\max(i, j), h).$$

Hence the theorem.

Let us mark the conditions for disjunction with primes. Then 1')—4') will be the same as 1)—4) above, with $k(x, y)$ replaced by $a(x, y)$. The remaining conditions will be:

5'). If $h \geqq i > j$ then $a(i, h) > a(j, h)$.

6'). $a(i, j) > d$ if and only if both $i > d$ and $j > d$.

7'). $a(1, 1) = a(1, n) = a(n, 1) = 1$ and $a(n, n) = n$.

8'). For all i, j and h, $k(i, a(j, h)) = a(k(i, j), k(i, h))$ and $a(i, k(j, h)) = k(a(i, j), a(i, h))$. (These are two distributive laws. Here we suppose that we have defined conjunction before defining disjunction.)

Let (A_1) be the set consisting of 1'), 2') and 5').

Definition 2.5.2. A two-place function $a(x, y)$ is a *disjunction* *function satisfying* (A_1) if a (x, y) satisfies each condition in the set (A_1).

In the following theorem, we suppose that the function k (x, y) mentioned in condition 8′) is $k_1 (x, y)$.

Theorem 2.5.2. (A_1) consists of strongly independent conditions and determines a unique function $a_1 (x, y)$ which satisfies conditions 3′), 4′), 6′), 7′) and 8′).

The proof is similar to that of theorem 2.5.1. It is seen that

$$a_1 (x, y) = \min (x, y).$$

$a_1 (x, y)$ and $k_1 (x, y)$ satisfy condition 8′) because, for all i, j and h,

$$\max (i, \min (j, h)) = \min (\max (i, j), \max (i, h)) \qquad \text{and}$$
$$\min (i, \max (j, h)) = \max (\min (i, j), \min (i, h)).$$

2.6. In this section we make a few remarks concerning the question whether it is possible that the truth-function corresponding to a generalized connective is a Sheffer function. In this case, namely, a functionally complete n-valued propositional logic can be based upon a single primitive connective which has the properties of, say, implication. It turns out that very few truth-functions corresponding to our generalized connectives are Sheffer functions.

Clearly, no negation function is a Sheffer function since no one-place function is a Sheffer function. No conjunction or disjunction function is a Sheffer function. This is obvious because any Sheffer function f (x, y) has the property that f $(i, i) \neq i$, for any i. Consider, then, any implication function c (x, y) satisfying (C_6) or (C_7). c (x, y) $\leqq d$ when $x \leqq d$ and $y \leqq d$. Hence c (x, y) is not a Sheffer function. The same holds true with respect to any equivalence function satisfying (E_1).

It is not possible to find, for all n and d, an implication function c (x, y) satisfying (C_5) such that c (x, y) is a Sheffer function. For always when $d = 1$, c $(1, 1) = 1$ and, hence, c (x, y) is not a Sheffer function. For some values of n and d, however, it is possible to find such a c (x, y). When $n = 3$ and $d = 2$, for instance, the following two functions satisfy (C_5) and are Sheffer functions:

$$\begin{matrix} 2 & 3 & 3 \\ 1 & 1 & 3 \\ 1 & 1 & 1 \end{matrix} \qquad \text{and} \qquad \begin{matrix} 2 & 3 & 3 \\ 1 & 1 & 3 \\ 1 & 1 & 2 \end{matrix}$$

2.7. In sections 2.2—2.5 we have given a number of conditions which certain functions have to satisfy. Now the question arises: given a matrix which defines a function f (x) or f (x, y), how can we decide as easily as possible whether the function in question satisfies these conditions? It is fairly easy to see that a mechanical decision procedure exists for each condition presented in sections 2.2—2.5.

For most of the conditions, such as 1)—7), 11) and 12) in 2.2, we have only to check that there is a given number or a number within given limits in certain entries of the matrix. For some other conditions, we have to find out whether the rows or columns in the matrix form a monotonous sequence of numbers. Thus, condition 8) in 2.2 requires that each row in the matrix forms a monotonously increasing sequence of numbers, whereas in condition 9) it is required that each column forms a monotonously decreasing sequence of numbers. According to condition 8′) in 2.2, that part of each row which is above the main diagonal of the matrix forms a monotonously increasing sequence with strict inequalities. (I.e. a number is always greater than its predecessor.) A corresponding fact with respect to columns is required in 9′) of 2.2.

Consider, then, conditions 10) in 2.2 and 3) in 2.3 which require transitivity with respect to assertability. A procedure to decide whether a matrix satisfies these conditions is the following: Find all numbers $x \leqq d$ in the matrix. Suppose such a number x is in the $(i, j)^{\text{th}}$ entry of the matrix. Find out whether in the i^{th} row there is a number $\leqq d$ in every entry such that in the opposite entry in the j^{th} row there is a number $\leqq d$. If this is the case, and the same thing happens for all $x \leqq d$ then the conditions considered are satisfied, otherwise they are not.

A similar »straightforward» decision method can be given for conditions 3) and 3′) in section 2.5. The criterion presented in the following theorem is more useful. Theorem 2.7.1 gives a necessary condition for a function f (x, y) defined by a given matrix to be associative. We say that the number h in the $(i, j)^{\text{th}}$ entry of a given matrix has the *inclusion property* if every number in the h^{th} row appears in the i^{th} row and every number in the h^{th} column appears in the j^{th} column, i.e. the set of numbers in the h^{th} row is included in the set of numbers in the i^{th} row and the set of numbers in the h^{th} column is included in the set of numbers in the j^{th} column.

Theorem 2.7.1. In a matrix which defines an associative function every number has the inclusion property.

Proof. Let f (x, y) be an associative function defined by a given matrix. Suppose the number h in the $(i, j)^{\text{th}}$ entry has not the inclusion property. Then either there is a number u in the h^{th} row which does not appear in the i^{th} row or there is a number v in the h^{th} column which does not appear in the j^{th} column. In the first case, suppose u is in the $(h, j')^{\text{th}}$ entry. Then

$$\mathrm{f}\,(\mathrm{f}\,(i, j), j') = \mathrm{f}\,(h, j') = u.$$

But

$$\mathrm{f}\,(i, \mathrm{f}\,(j, j')) \neq u$$

since u does not appear in the i^{th} row. Thus f (x, y) is not associative, contrary to the hypothesis. The argument is similar in the second case, and this completes the proof.

The converse of theorem 2.7.1 does not hold in general, as seen by the following counter-example:

$$\begin{matrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & 1 & 3 \end{matrix}$$

In this matrix, namely, every number has the inclusion property and the function defined by it is not associative. However, in the two-valued case the converse of theorem 2.7.1 holds. This is shown by checking through all the 16 matrices in question.

2.8. As we have pointed out, the sets of conditions discussed in sections 2.2—2.5 do not determine a unique function except when

$n = 2$. There are, for instance, several implication functions satisfying (C_2). It is of some interest to calculate the number of functions satisfying some condition or some set of conditions. In general, if two conditions A and B are strongly independent then, for any n and d, the number of functions satisfying both A and B is less than the number of functions satisfying A and also less than the number of functions satisfying B. If A and B are weakly independent this is true only for some n and d. Nothing general can be said about how great the decrease will be.

We do not perform any calculations in detail but give only the final figures. We have not been able to solve the problem for all sets of conditions discussed in 2.2—2.5, in particular, when a condition of transitivity is involved. In the second column of the following table is given the number of functions which satisfy the condition or conditions mentioned in the opposite place in the first column.

1) in 2.2.	$n^{n^2-(n-d)\,d} \cdot (n-d)^{nd-d^2}$
6′) and 7) in 2.2.	$(d\,(n-d))^{\frac{1}{2}(n^2-n)} \cdot n^n$
(C_4) in 2.2.	$d^{\frac{1}{2}(n^2+n)} \cdot (n-d)^{\frac{1}{2}(n^2-n)}$
(C_6) in 2.2.	$d^{n^2-(n-d)\,d} \cdot (n-d)^{nd-d^2}$
(C_2) in 2.2.	$d^n \cdot (n-d)^{dn-d^2} \cdot n^{n^2-n-(nd-d^2)}$ $-d^n \cdot (n-d)^{2\,(nd-d^2)} \cdot \sum_{i=0}^{u} \binom{u}{i} d^{2u-2i} \cdot (n-d)^{2i}$ where $u = \frac{1}{2}\,(n^2-n-2\,(nd-d^2))$ and $\binom{u}{i}$ is a binomial coefficient. (Eg. for $n = 3$, $d = 1$, the no. of impl. functions sat. (C_2) is 244, and for $n = 3$, $d = 2$ it is 608.)
1) and 2) in 2.4.	$(n-d)^d \cdot d^{n-d}$
1) and 2′) in 2.4.	$(n-d)^d \cdot (n^{n-d} - (n--d)^{n-d})$
1′) and 2) in 2.4.	$d^{n-d} \cdot (n^d - d^d)$

3) in 2.4. $\sum_{h=1}^{n} \varphi_n(h)$ where the φ's are calculated recursively as follows: $\varphi_1(h) = 1$, for any h,

$$\varphi_{l+1}(h) = \sum_{i=1}^{h} \varphi_l(h).$$

(N_3) in 2.4. $\left(\sum_{h=1}^{n-d} \varphi_d(h)\right) \cdot \left(\sum_{h=1}^{d} \varphi_{n-d}(h)\right)$ where the φ's are calculated as above. (Eg. for $n = 3$, $d = 1, 2$, the of no. neg. functions sat. (N_3) is 2.)

2.9. There is a more general method which can be applied for the solving of the problem discussed in the preceding section. In some cases, namely, an arbitrary function can be represented as a polynomial of its variables in the field of residue classes modulo n. This is possible at least when n is a prime number. [Cf. Bernstein.] Conditions imposed upon a function are expressed as equations for the coefficients of this polynomial. Therefore, the whole problem reduces to the solving of some equations.

We illustrate this method by the following example. We want to determine all functions $\mathrm{k}(x, y)$ in three-valued propositional calculus which satisfy the following conditions:

1) $\mathrm{k}(0, 0) = 0$ and $\mathrm{k}(0,2) = \mathrm{k}(2,0) = \mathrm{k}(2, 2) = 2$.

2). For any x, $\mathrm{k}(x, x) = x$.

3). For any x and y, $\mathrm{k}(x, y) = \mathrm{k}(y, x)$.

4). For any x, y and z, $\mathrm{k}(\mathrm{k}(x, y), z) = \mathrm{k}(x, \mathrm{k}(y, z))$.

In this example we use numbers 0, 1 and 2 instead of 1, 2 and 3, respectively, because of their arithmetical properties. All operations are carried out modulo 3. It is seen that the functions $\mathrm{k}(x, y)$ defined by the preceding conditions are more general conjunction functions than $\mathrm{k}_1(x, y)$ in theorem 2.5.1.

A general two-place function $\mathrm{k}(x, y)$ in three values is expressed as follows:

$$\mathrm{k}(x,y) = a_1x^2y^2 + a_2x^2y + a_3xy^2 + a_4x^2 + a_5y^2 + a_6xy + a_7x + a_8y + a_9.$$

Using conditions 1)—3) we get the following equations if we put $a_1 = a$ and $a_8 = h$:

$$\begin{cases} a_1 = a \\ a_2 = 2 + 2h \\ a_3 = 2 + 2h \\ a_4 = 2 + h \\ a_5 = 2 + h \\ a_6 = 2a + h + 2 \\ a_7 = h \\ a_8 = h \\ a_9 = 0 \end{cases}$$

From condition 4) we obtain by substituting and comparing coefficients the following equations for the parameters a and h:

$$\begin{cases} h^2 + 2ah + 2h + a = 0 \\ 2ah^2 + h^2 + 2ah + 2h + 2a = 0 \\ ah^2 + a^2h + 2a^2 + ah + a = 0 \\ 2a^2h + a^2 + a + 2ah = 0 \\ h^2 + 2ah + a^2h + h + a = 0 \end{cases}$$

These equations have four solutions:

$$\begin{cases} h = 0 \\ a = 0 \end{cases} \qquad \begin{cases} h = 1 \\ a = 1 \end{cases} \qquad \begin{cases} h = 1 \\ a = 2 \end{cases} \qquad \begin{cases} h = 2 \\ a = 2 \end{cases}$$

So there are four functions k (x, y) satisfying our conditions 1)—4). They are defined by the subsequent matrices:

$$\begin{matrix} 0 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 2 \end{matrix} \qquad \begin{matrix} 0 & 1 & 2 \\ 1 & 1 & 2 \\ 2 & 2 & 2 \end{matrix} \qquad \begin{matrix} 0 & 1 & 2 \\ 1 & 1 & 1 \\ 2 & 1 & 2 \end{matrix} \qquad \begin{matrix} 0 & 0 & 2 \\ 0 & 1 & 2 \\ 2 & 2 & 2 \end{matrix}$$

2.10. In this section we discuss the validity of certain wffs, which are known to be tautologies in two-valued propositional calculus, when all connectives are replaced by some generalized ones and the calculus is considered to be n-valued. For this purpose, we have chosen the following tautologies of two-valued propositional calculus. The list includes all propositions considered as most important in divisions 2—5 of Principia Mathematica plus a few others. [Cf. Whitehead-Russell, pp. 99, 100, 104, 105, 110—12, 116, 120, 123, 124.] We have changed the notation to suit our own but left the numbers of the propositions unchanged.

2.02 *q*C. *p*C*q*
2.03 *p*C. N*q*: C: *q*C. N*p*
2.15 N*p*. C*q*: C: N*q*. C*p*
2.16 *p*C*q*. C: N*q*. C. N*p*
2.17 N*q*. C. N*p*: C. *p*C*q*
2.04 *p*C.*q*C*r*: C: *q*C. *p*C*r*
2.05 *q*C*r*. C: *p*C*q*. C. *p*C*r*
2.06 *p*C*q*. C: *q*C*r*. C. *p*C*r*
2.08 *p*C*p*
2.21 N*p*. C. *p*C*q*
3.2 *p*C: *q*C. *p*K*q*
3.26 *p*K*q*. C*p*
3.27 *p*K*q*. C*q*
3.3 *p*K*q*. C*r*: C: *p*C. *q*C*r*
3.31 *p*C. *q*C*r*: C: *p*K*q*. C*r*
3.35 *p*K. *p*C*q*: C*q*
3.43 *p*C*q*. K. *p*C*r*: C: *p*C. *q*K*r*
4.73 *q*C: *p*E. *p*K*q*
5.1 *p*K*q*. C. *p*E*q*
5.32 *p*C. *q*E*r*: E: *p*K*q*. E. *p*K*r*
5.6 *p*K. N*q*: C*r*.: E: *p*C. *q*A*r*

2.01 *p*C. N*p*: C. N*p*

3.45 *p*C*q*. C: *p*K*r*. C. *q*K*r*
3.47 *p*C*r*. K. *q*C*s*: C: *p*K*q*. C. *r*K*s*
4.1 *p*C*q*. E: N*q*. C. N*p*
4.11 *p*E*q*. E: N*p*. E. N*q*
4.13 *p*E: N. N*p*
4.2 *p*E*p*
4.21 *p*E*q*. E. *q*E*p*
4.22 *p*E*q*. K. *q*E*r*: C. *p*E*r*
4.24 *p*E. *p*K*p*
4.25 *p*E. *p*A*p*
4.3 *p*K*q*. E. *q*K*p*
4.31 *p*A*q*. E. *q*A*p*
4.32 *p*K*q*. K*r*: E: *p*K.*q*K*r*
4.33 *p*A*q*. A*r*: E: *p*A. *q*A*r*
4.4 *p*K. *q*A*r*: E: *p*K*q*. A. *p*K*r*
4.41 *p*A. *q*K*r*: E: *p*A*q*. K. *p*A*r*
4.71 *p*C*q*. E: *p*E. *p*K*q*
2.27 *p*C: *p*C*q*. C*q*
2.36 *q*C*r*. C: *p*A*q*. C. *r*A*p*
3.33 *p*C*q*. K. *q*C*r*: C. *p*C*r*
4.5 *p*K*q*. E:. N: N*p*. A. N*q*
4.57 N: N*p*. K. N*q*.: E. *p*A*q*
5.19 N: *p*E. N*p*

In the subsequent discussion we are concerned with those generalized connectives whose truth-functions are implication functions satisfying (C$_2$), (C$_5$) or (C$_7$); negation functions satisfying (N$_3$) or (N$_4$); conjunction functions satisfying (K$_1$) and disjunction functions satisfying (A$_1$). So we shall consider both of the »strong» sets of conditions for implication — (C$_5$) and (C$_7$) — as well as one »weak» set, namely, (C$_2$). The unique negation, conjunction and disjunction presented in theorems 2.4.2, 2.5.1 and 2.5.2 will be discussed and, furthermore, the strongest of the sets $(N_1)-(N_3)$ given in section 2.4. Equivalence will always be defined as follows:

$$pEq = pCq.\ K.\ qCp$$ [1]

So we investigate, in succession, subsequent systems of conditions: $[(C_2), (N_3), (K_1), (A_1)]$, $[(C_2), (N_4), (K_1), (A_1)]$, $[(C_5), (N_3), (K_1), (A_1)]$, $[(C_5), (N_4), (K_1), (A_1)]$, $[(C_7), (N_3), (K_1), (A_1)]$ and $[(C_7), (N_4), (K_1), (A_1)]$.

We have, for instance, the following problem while considering the third among these systems. If in wff 5.6 above C, N, K and A are connectives whose truth-functions satisfy (C_5), (N_3), (K_1) and (A_1), respectively, and E is defined as above in terms of C and K, what can we say about the assertability of 5.6? Will 5.6 be always assertable, for any *n* and *d*, no matter how we choose C and N from the sets in question? (K and A are unique after *n* and *d* have been fixed.) Or will it never be assertable? Or will it, for some values of *n* and *d*, be assertable independently of the choice of C and N, and for some other values not assertable? And so on. In general, suppose T (C, N, K, A, E) is a wff involving connectives C, N, K, A and E (not necessarily all of them). Suppose $S_{n,d}$ (c, ne, k, a, e) is a system of conditions for the truth-functions of these connectives which determines, for any *n* and *d*, a certain set of quintuples (C, N, K, A, E). Let us denote this set by »Q (*n*, *d*)». Then the following seven cases may occur. We denote the different cases by capital letters as indicated.

V). Given any *n* and *d*, all members of Q (*n*, *d*) make T assertable. I.e. in this case T is always a consequence of the conditions in S.

W). Given any *n* and *d*, all members of Q (*n*, *d*) make T non-

[1] So equivalence function is always uniquely determined after the choice of implication function. It satisfies conditions 1, 2) and 4) in section 2.3 if the implication function satisfies (C_2) and, in addition, 3) and 5) if the implication function satisfies (C_5). Finally, it satisfies conditions 1)—6) of 2.3 if the implication function satisfies (C_7).

assertable. This means that T is always contradictory to the conditions in S.

U). Given any n and d, some members of Q (n, d) make T assertable and some members of Q (n, d) make T non-assertable. I.e. T is always independent of the conditions in S.

These are the three »pure» cases, i.e. independent of the choice of n and d. We have the following four »mixed» cases.

VW). For some values of n and d, all members of Q (n, d) make T assertable. For all other values of n and d, all members of Q (n, d) make T non-assertable. In other words, T is both a consequence of and contradictory to S, depending on the choice of n and d.

WU). For some values of n and d, all members of Q (n, d) make T non-assertable. For all other values of n and d, there is a member of Q (n, d) which makes T assertable and a member of Q (n, d) which makes T non-assertable. I.e. T is both contradictory to and independent of S, depending on the choice of n and d.

VU). For some values of n and d, all members of Q (n, d) make T assertable. For all other values of n and d, there is a member of Q (n, d) which makes T assertable and a member of Q (n, d) which makes T non-assertable. I.e. T is both a consequence of and independent of S, depending on the choice of n and d.

VWU). For some n and d, all members of Q (n, d) make T assertable. For some n and d, all members of Q (n, d) make T non-assertable. For some n and d, there is a member of Q (n, d) which makes T assertable and a member of Q (n, d) which makes T non-assertable. So T is both a consequence of, contradictory to and independent of the conditions in S, depending on the choice of n and d.

Obviously these seven cases are mutually exclusive. One important remark has to be added. The range of quantification for n consists of values $n \geqq 3$. When $n = 2$ each of the six systems of conditions discussed determines a unique quintuple of connectives, namely, the ordinary two-valued implication, negation, conjunction, disjunction and equivalence. So if we would extend the range of quantification to consist of values $n \geqq 2$ we would exclude the three cases W), U) and WU). And this we do not want to happen.

In the subsequent table of results it is seen which of the seven possibilities occurs when T is one of the wffs listed above and S is one of the six systems of conditions. Thus, in the table we find U opposite 5.6 and under [(C$_2$), (N$_3$), (K$_1$), (A$_1$)]. That means: for every n and d, there is a quintuple of connectives (C, N, K, A, E) satisfying [(C$_2$), (N$_3$), (K$_1$), (A$_1$)] such that it makes 5.6 assertable, and a quintuple of connectives (C, N, K, A, E) satisfying [(C$_2$), (N$_3$), (K$_1$), (A$_1$)] such that it makes 5.6 non-assertable. The rest of the table reads in the same manner. In the footnotes following the table we give, furthermore, the corresponding values of n and d for all »mixed» cases appearing in the table. The two last columns of the table remain unaltered if we take (C$_6$) instead of (C$_7$). We hope to return in another connection for a closer examination of the results. (It is also of some interest to study the converse problem: given a set of wffs, eg. a subset of those listed above, how is the choice of the connectives limited if it is required that all of the wffs in this set have to be assertable? Results similar to the one presented in [Gödel] are obtained.)

	[(C$_2$), (N$_3$); (K$_1$), (A$_1$)]	[(C$_2$), (N$_4$); (K$_1$), (A$_1$)]	[(C$_5$), (N$_3$); (K$_1$), (A$_1$)]	[(C$_5$), (N$_4$); (K$_1$), (A$_1$)]	[(C$_7$), (N$_3$); (K$_1$), (A$_1$)]	[(C$_7$), (N$_4$); (K$_1$), (A$_1$)]
2.02	U	U	WU[1]	WU[1]	V	V
2.03	U	U	U	U	V	VW[2]
2.15	U	U	U	U	V	VW[2]
2.16	U	U	U	U	V	VW[2]
2.17	U	U	WU[3]	U	V	VW[2]
2.04	U	U	U	U	V	V
2.05	U	U	U	U	V	V
2.06	U	U	U	U	V	V
2.08	V	V	V	V	V	V
2.21	U	WU[4]	WU[5]	WU[1]	VW[2]	V
3.2	U	U	WU[1]	WU[1]	V	V
3.26	U	U	V	V	V	V
3.27	U	U	V	V	V	V

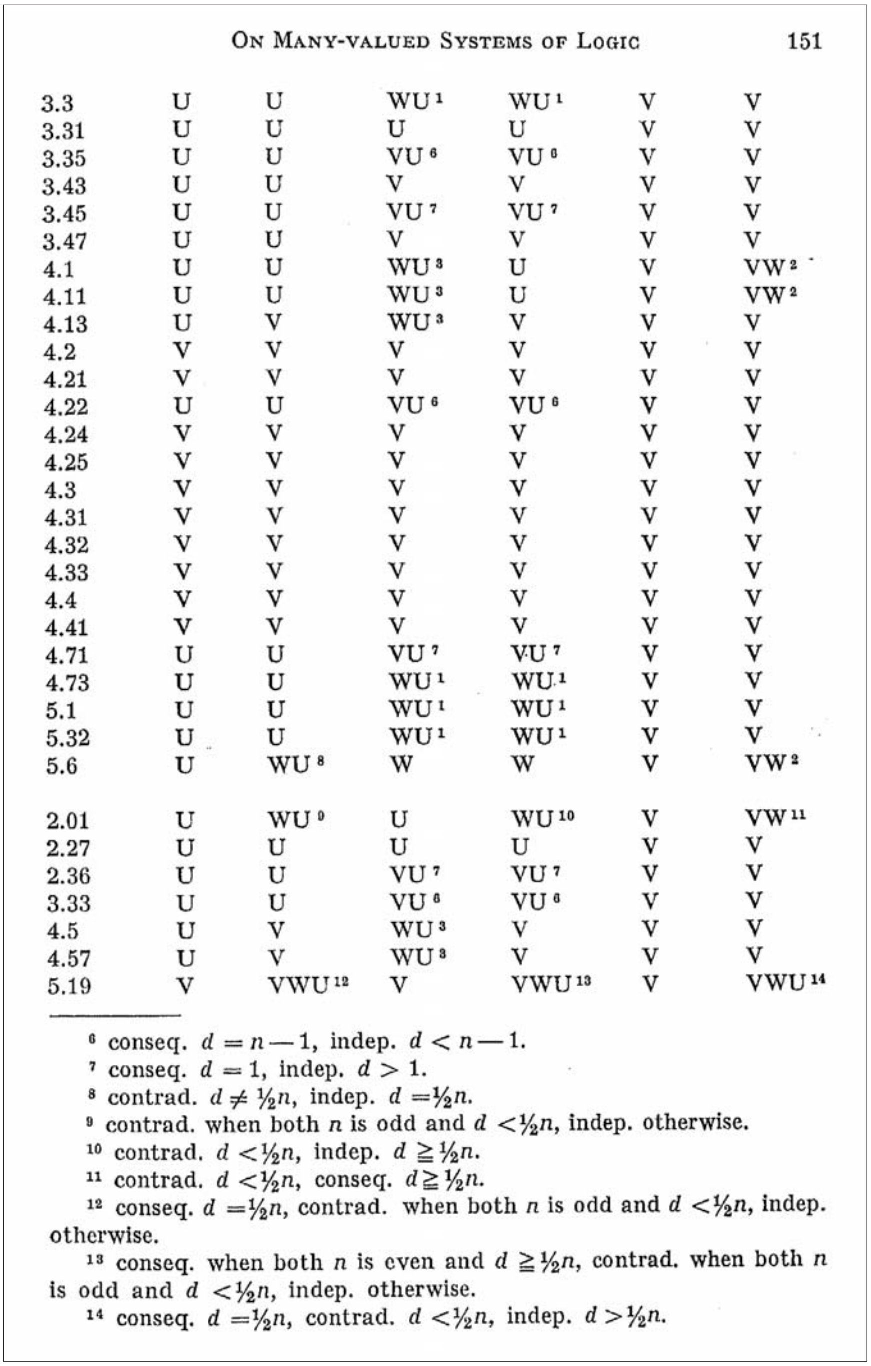
[1] contradictory when $d > 1$, independent when $d = 1$.

[2] consequence when $d = \frac{1}{2}n$, contrad. when $d \neq \frac{1}{2}n$. ($d = \frac{1}{2}n$ requires, naturally, that n is even.)

[3] contrad. $d \neq \frac{1}{2}n$, indep. $d = \frac{1}{2}n$.

[4] contrad. $d > \frac{1}{2}n$, indep. $d \leqq \frac{1}{2}n$.

[5] conrad. $d < n - 1$, indep. $d = n - 1$.



3.3	U	U	WU[1]	WU[1]	V	V
3.31	U	U	U	U	V	V
3.35	U	U	VU[6]	VU[6]	V	V
3.43	U	U	V	V	V	V
3.45	U	U	VU[7]	VU[7]	V	V
3.47	U	U	V	V	V	V
4.1	U	U	WU[3]	U	V	VW[2]
4.11	U	U	WU[3]	U	V	VW[2]
4.13	U	V	WU[3]	V	V	V
4.2	V	V	V	V	V	V
4.21	V	V	V	V	V	V
4.22	U	U	VU[6]	VU[6]	V	V
4.24	V	V	V	V	V	V
4.25	V	V	V	V	V	V
4.3	V	V	V	V	V	V
4.31	V	V	V	V	V	V
4.32	V	V	V	V	V	V
4.33	V	V	V	V	V	V
4.4	V	V	V	V	V	V
4.41	V	V	V	V	V	V
4.71	U	U	VU[7]	VU[7]	V	V
4.73	U	U	WU[1]	WU[1]	V	V
5.1	U	U	WU[1]	WU[1]	V	V
5.32	U	U	WU[1]	WU[1]	V	V
5.6	U	WU[8]	W	W	V	VW[2]
2.01	U	WU[9]	U	WU[10]	V	VW[11]
2.27	U	U	U	U	V	V
2.36	U	U	VU[7]	VU[7]	V	V
3.33	U	U	VU[6]	VU[6]	V	V
4.5	U	V	WU[3]	V	V	V
4.57	U	V	WU[3]	V	V	V
5.19	V	VWU[12]	V	VWU[13]	V	VWU[14]

[6] conseq. $d = n - 1$, indep. $d < n - 1$.

[7] conseq. $d = 1$, indep. $d > 1$.

[8] contrad. $d \neq \frac{1}{2}n$, indep. $d = \frac{1}{2}n$.

[9] contrad. when both n is odd and $d < \frac{1}{2}n$, indep. otherwise.

[10] contrad. $d < \frac{1}{2}n$, indep. $d \geqq \frac{1}{2}n$.

[11] contrad. $d < \frac{1}{2}n$, conseq. $d \geqq \frac{1}{2}n$.

[12] conseq. $d = \frac{1}{2}n$, contrad. when both n is odd and $d < \frac{1}{2}n$, indep. otherwise.

[13] conseq. when both n is even and $d \geqq \frac{1}{2}n$, contrad. when both n is odd and $d < \frac{1}{2}n$, indep. otherwise.

[14] conseq. $d = \frac{1}{2}n$, contrad. $d < \frac{1}{2}n$, indep. $d > \frac{1}{2}n$.

We omit the proofs of these results to save space. To illustrate methods used in the proofs, we give a proof of the fact that the »commutative principle» 2.04 is, for any n and d, independent of (C_5), i.e. that *U appears opposite 2.04 in the third and fourth columns of the table.* (Since N does not occur in 2.04, the third and fourth columns of the table must have the same letter opposite 2.04.)

Proof. Consider the following implication function $c_w(x, y)$ which satisfies (C_5), for any n and d:

$$c_w(x, y) = 1 \text{ for } x \geqq y, \; c_w(x, y) = n \text{ for } x < y.$$

If we let C in 2.04 be the connective corresponding to $c_w(x, y)$ and assign for p, q and r the values 1, 2 and 2, respectively, then 2.04 will get the undesignated value n. Hence, given any n and d, $c_w(x, y)$ makes 2.04 non-assertable. So we know that we are dealing with one of the cases W), U) or WU). (In the two-valued case, of course, $c_w(x, y)$ makes 2.04 assertable. But the convention has been made that we consider only cases where $n \geqq 3$.)

Suppose $d = 1$. Then we claim that the Lukasiewicz implication, i.e. the connective whose truth-function is $c_8(x, y)$ makes 2.04 assertable. ($c_8(x, y)$ satisfies (C_5), as was seen in section 2.2.) Let us denote, for the moment, the truth-values of p, q and r by $\bar{p}$, $\bar{q}$ and $\bar{r}$, respectively. Consider the following truth-table where inequalities refer to numerical values.

	pCr	$qC.\,pCr$	qCr	$pC.\,qCr$	2.04
$\bar{p} \geqq \bar{r}$	1	1			1
$\bar{p} < \bar{r}$, $\bar{q} < \bar{r}$ and $\bar{q} \geqq \bar{r} - \bar{p} + 1$	$\bar{r} - \bar{p} + 1$	1	$\bar{r} - \bar{q} + 1$	1	1
$\bar{p} < \bar{r}$, $\bar{q} < \bar{r}$ and $\bar{q} < \bar{r} - \bar{p} + 1$	$\bar{r} - \bar{p} + 1$	$\bar{r} - \bar{p} - \bar{q} + 2$	$\bar{r} - \bar{q} + 1$	$\bar{r} - \bar{q} - \bar{p} + 2$	1
$\bar{p} < \bar{r} \leqq \bar{q}$	$\bar{r} - \bar{p} + 1$	1	1	1	1

Since the cases given on the left exhaust all of the possibilities for $\bar{p}$, $\bar{q}$ and $\bar{r}$ we have shown that 2.04 gets always the truth-value 1. Hence the Lukasiewicz implication makes 2.04 assertable when $d = 1$, and we conclude that the case W) is excluded.

Now we know that we are dealing with the case U) or the case

WU). It will be more difficult to prove that the first alternative is the correct one. For this purpose, we assume $d > 1$ and consider a function $\mathrm{c}\,(x, y)$ defined as follows.

$$\begin{array}{ll} \mathrm{c}\,(n, i) = \mathrm{c}\,(i, 1) = 1, & \text{for any } i, \\ \mathrm{c}\,(1, i) = n & \text{for } i > 1, \\ \mathrm{c}\,(i, n) = n & \text{for } i < n. \end{array}$$

If both x and y differ from 1 and n then

$$\begin{array}{ll} \mathrm{c}\,(x, y) = \min\,(n, d + \max\,(|x\text{-}d|, |y\text{-}d|)) & \text{for } x < y, \\ \mathrm{c}\,(x, y) = \max\,(2, d - \max\,(|x\text{-}d|, |y\text{-}d|)) & \text{for } x \geqq y. \end{array}$$

Since the definition of $\mathrm{c}\,(x, y)$ is somewhat complicated we give, as an example, the matrix of $\mathrm{c}\,(x, y)$ when $n = 7$ and $d = 2$, 3, 4, 5 and 6, successively.

$$\begin{array}{ccccccc} 1&7&7&7&7&7&7\\ 1&2&3&4&5&6&7\\ 1&2&2&4&5&6&7\\ 1&2&2&2&5&6&7\\ 1&2&2&2&2&6&7\\ 1&2&2&2&2&2&7\\ 1&1&1&1&1&1&1 \end{array} \qquad \begin{array}{ccccccc} 1&7&7&7&7&7&7\\ 1&2&4&4&5&6&7\\ 1&2&3&4&5&6&7\\ 1&2&2&2&5&6&7\\ 1&2&2&2&2&6&7\\ 1&2&2&2&2&2&7\\ 1&1&1&1&1&1&1 \end{array} \qquad \begin{array}{ccccccc} 1&7&7&7&7&7&7\\ 1&2&6&6&6&6&7\\ 1&2&3&5&5&6&7\\ 1&2&3&4&5&6&7\\ 1&2&3&3&3&6&7\\ 1&2&2&2&2&2&7\\ 1&1&1&1&1&1&1 \end{array}$$

$$\begin{array}{ccccccc} 1&7&7&7&7&7&7\\ 1&2&7&7&7&7&7\\ 1&2&3&7&7&7&7\\ 1&2&3&4&6&6&7\\ 1&2&3&4&5&6&7\\ 1&2&3&4&4&4&7\\ 1&1&1&1&1&1&1 \end{array} \qquad \begin{array}{ccccccc} 1&7&7&7&7&7&7\\ 1&2&7&7&7&7&7\\ 1&2&3&7&7&7&7\\ 1&2&3&4&7&7&7\\ 1&2&3&4&5&7&7\\ 1&2&3&4&5&6&7\\ 1&1&1&1&1&1&1 \end{array}$$

Clearly, $\mathrm{c}\,(x, y)$ satisfies (C_5). We want to show that the connective corresponding to $\mathrm{c}\,(x, y)$ makes 2.04 assertable. We do this in two steps.

I. At least one of p, q and r has the truth-value 1 or the truth-value n. Consider the following truth-table where $1 < e < n$.

$p\ q\ r$	pCr	$qC.pCr$	qCr	$pC.qCr$	2.04
$1\ 1\ 1$	1	1	1	1	1
$1\ 1\ n$	n	n	n	n	1
$1\ 1\ e$	n	n	n	n	1
$1\ n\ 1$	1	1	1	1	1
$1\ n\ n$	n	1	1	1	1
$1\ n\ e$	n	1	1	1	1
$1\ e\ 1$	1	1	1	1	1
$1\ e\ n$	n	n	n	n	1
$1\ e\ e$	n	n	e, n	n	1
$n\ 1\ 1$	1	1	1	1	1
$n\ 1\ n$	1	1	n	1	1
$n\ 1\ e$	1	1	n	1	1
$n\ n\ 1$	1	1	1	1	1
$n\ n\ n$	1	1	1	1	1
$n\ n\ e$	1	1	1	1	1
$n\ e\ 1$	1	1	1	1	1
$n\ e\ n$	1	1	n	1	1
$n\ e\ e$	1	1	e, n	1	1
$e\ 1\ 1$	1	1	1	1	1
$e\ 1\ n$	n	n	n	n	1
$e\ 1\ e$	e, n	n	n	n	1
$e\ n\ 1$	1	1	1	1	1
$e\ n\ n$	n	1	1	1	1
$e\ n\ e$	e, n	1	1	1	1
$e\ e\ 1$	1	1	1	1	1
$e\ e\ n$	n	n	n	n	1

Actually, this is a system of truth-tables. e is not to be considered as a fixed number. It simply indicates that in its place any number from the open interval $(1, n)$ may occur. We see that in this case 2.04 gets always the designated value 1.

II. p, q and r have each a truth-value different from 1 and n. In this case we proceed by induction. First, if p, q and r have all the truth-value d then also 2.04 gets the value d. We make the subsequent inductive hypothesis: 2.04 gets a designated value always when the values of p, q and r belong to the intersection of the two closed intervals $(d-i,\ d+i)$ and $(2,\ n-1)$. To complete the induction, we have to show that 2.04 gets a designated value always when the values of p, q and r belong to the intersection of the two closed intervals $(d-i-1,\ d+i+1)$ and $(2, n-1)$. We separate four subcases:

1). $d-i-1 > 1$ and $d+i+1 < n$.
2). $d-i-1 > 1$ and $d+i+1 \geqq n$.
3). $d-i-1 \leqq 1$ and $d+i+1 < n$.
4). $d-i-1 \leqq 1$ and $d+i+1 \geqq n$.

In subcase 1) the truth-table looks as follows:

p	q	r	pCr	$qC.\,pCr$	qCr	$pC.\,qCr$	2.04
$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d-i-1$	$d-i-1$	e	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d-i-1$
$d-i-1$	$d-i-1$	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d-i-1$
$d-i-1$	e	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d-i-1$	e	e	$d+i+1$	$d+i+1$	e	$d+i+1$	$d-i-1$
$d-i-1$	e	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d-i-1$
$d-i-1$	$d+i+1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d-i-1$	$d+i+1$	e	$d+i+1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d-i-1$	$d+i+1$	$d+i+1$	$d+i+1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
e	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
e	$d-i-1$	e	e	$d+i+1$	$d+i+1$	$d+i+1$	$d-i-1$
e	$d-i-1$	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d-i-1$
e	e	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
e	e	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d-i-1$
e	$d+i+1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
e	$d+i+1$	e	e	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
e	$d+i+1$	$d+i+1$	$d+i+1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d+i+1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d+i+1$	$d-i-1$	e	$d-i-1$	$d-i-1$	$d+i+1$	$d-i-1$	$d-i-1$
$d+i+1$	$d-i-1$	$d+i+1$	$d-i-1$	$d-i-1$	$d+i+1$	$d-i-1$	$d-i-1$
$d+i+1$	e	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d+i+1$	e	e	$d-i-1$	$d-i-1$	e	$d-i-1$	$d-i-1$
$d+i+1$	e	$d+i+1$	$d-i-1$	$d-i-1$	$d+i+1$	$d-i-1$	$d-i-1$
$d+i+1$	$d+i+1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d+i+1$	$d+i+1$	e	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d+i+1$	$d+i+1$	$d+i+1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$

where e is in the closed interval $(d-i,\ d+i)$.

In subcase 2) 2.04 gets, by the inductive hypothesis, a designated value when the values of p, q and r are in the closed interval $(d-i, n-1)$. Hence we have to consider the following truth-table where e is in the closed interval $(d-i,\ n-1)$:

p	q	r	pCr	$qC.\,pCr$	qCr	$pC.\,qCr$	2.04
$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d-i-1$	$d-i-1$	e	n	n	n	n	1
$d-i-1$	e	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
$d-i-1$	e	e	n	n	e	n	1
e	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$
e	$d-i-1$	e	e	n	n	n	1
e	e	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$	$d-i-1$

In subcase 3) 2.04 gets, by the inductive hypothesis, a designated value when the values of p, q and r are in the closed interval $(2, d+i)$. In the following truth-table e is in this interval.

p	q	r	pCr	$qC.\,pCr$	qCr	$pC.\,qCr$	2.04
e	e	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	$d+i+1$	2
e	$d+i+1$	e	e	2	2	2	2
e	$d+i+1$	$d+i+1$	$d+i+1$	2	2	2	2
$d+i+1$	e	e	2	2	e	2	2
$d+i+1$	e	$d+i+1$	2	2	$d+i+1$	2	2
$d+i+1$	$d+i+1$	e	2	2	2	2	2
$d+i+1$	$d+i+1$	$d+i+1$	2	2	2	2	2

Since in these tables all values for 2.04 are designated — d was assumed to be > 1 — we have completed the inductive step in subcases 1)—3). In subcase 4) it follows directly from the inductive hypothesis. Hence we conclude that 2.04 gets a designated truth-value when p, q and r each have a truth-value different from 1 and n.

This shows that the connective corresponding to $c\,(x, y)$ makes 2.04 assertable. Since $c\,(x, y)$ was defined for any n and $d > 1$ we draw the final conclusion that 2.04 is, for any n and d, independent of (C_5) and so U appears in the third and fourth columns of the table, opposite 2.04.

In order to find functions required in the proofs, such as $c\,(x, y)$ above, it is sometimes useful to develop decision methods similar to those presented in section 2.7.

The last part of the proof shows how truth-table technique is modified when we have to demonstrate the assertability of some wff in n-valued propositional calculus, without specifying the number n. Then we cannot simply list all combinations of values for the variables as we can, for instance, in three-valued propositional calculus. We have to consider some systems of truth-tables or use inductive procedures.

Bibliography

Anscombe, G. E. M.: Aristotle and the sea battle. Mind (new series), Vol. 65 (1956), pp. 1—15. [Anscombe]

Baylis, Charles A.: Are Some Propositions Neither True Nor False? Philosophy of Science, Vol. 3 (1936), pp. 156—66. [Baylis]

Becker, Albr.: Bestreitet Aristoteles die Gültigkeit des »Tertium non datur» für Zukunftsaussagen? Actes du congrés international de philosophie scientifique, Paris 1936, Vol. 6, pp. 69—74. [Becker]

Bernstein, B. A.: Modular representations for finite algebras. Proc. Int. Math. Congr., Toronto 1924, Vol. 1, pp. 207—216. [Bernstein]

Birkhoff, G. — von Neumann, J. The logic of quantum mechanics. Annals of Math., 2 s., vol. 37 (1936), pp. 823—43. [Birkhoff—von Neumann]

Bochenski, I. M.: Ancient Formal Logic. Amsterdam 1951. [Bochenski]

Cohen, Jonathan: Three-valued Ethics. Philosophy, Vol. 26 (1951), pp. 208—227. [Cohen]

Dienes, Paul: On ternary logic. Jl. of Symbolic Logic, Vol. 14 (1949), pp. 85—94. [Dienes]

Frey, Gerhard: Bemerkungen zum Problem der mehrwertigen Logiken. Actes du XIéme congrés international de philosophie (1953), Vol. 5, pp. 53—58. [Frey]

Gödel, Kurt: Eine Eigenschaft der Realisierungen des Aussagenkalküls. Ergebnisse eines mathematischen Kolloquiums. (Karl Menger herausg.) Heft 3 (1935), pp. 20—21. [Gödel]

Guthrie, Edwin: The field of logic. Jl. of Philosophy, Psychology and Scientific Methods. Vol. 13 (1916), pp. 152—58 and 336. [Guthrie]

Hempel, Carl: Ein System verallgemeinerten Negationen. Travaux du IX^{e} congrés international de philosophie, Paris 1937, Vol. 6, pp. 26—32. [Hempel]

Kalicki, Jan.: Note on truth-tables. Jl. of Symbolic Logic, Vol. 15 (1950), pp. 174—81. [Kalicki]

Kokoszyńska, Marja: Review of a paper by Lukasiewicz. Jl. of Symbolic Logic, Vol. 3 (1938), pp. 43—44. [Kokoszyńska]

Leblanc, Hugues: An Introduction to Deductive Logic. London—New York 1955. [Leblanc]

Lewis, C. I.: Alternative systems of logic. The Monist, Vol. 42 (1932) pp. 481—507. [Lewis]

Lewis, C. I. — Langford, C. H.: Symbolic Logic. New York-London 1932. [Lewis—Langford]

Linke, Paul F.: Die mehrwertigen Logiken und das Wahrheitsproblem. Zeitschrift für philosophische Forschung, Vol. 3 (1948—49), pp. 376—98 and 530—46. [Linke]

Lovett, E. O.: Mathematics at the international congress of philosophy, Paris 1900. Bull. Am. Math. Soc., Vol. 7 (1900—01), pp. 157—83. [Lovett]

Lukasiewicz, Jan.: O logice trójwartosciowej. Ruch Filozoficzny, Vol. 5 (1920), pp. 169—71. [Lukasiewicz 1]

Philosophische Bemerkungen zu mehrwertigen Systemen des Aussagenkalküls. Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie, Classe III, XXIII Année (1930), pp. 51—77. [Lukasiewicz 2]

Zur Geschichte der Aussagenlogik. Erkenntnis, Vol. 5 (1935), pp. 111—31. [Lukasiewicz 3]

A system of modal logic. The Jl. of Computing Systems, Vol. 1, No. 3 (1953), pp. 111—49. [Lukasiewicz 4]

MacColl, Hugh: The calculus of equivalent statements (fifth paper). Proc. London Math. Soc., Vol. 28 (1896—97), pp. 156—83. [MacColl]

Margenau, Henry: Probability, Many-Valued Logics and Physics. Philosophy of Science, Vol. 6 (1939), pp. 65—87. [Margenau]

Michalski, K.: Le problème de la volonté à Oxford et à Paris au XIV^{e} siècle. Studia philosophica, Vol. 2 (1937), pp. 233—365. [Michalski]

Peirce, C. S.: Collected Papers, Vols. 3—4. Cambridge, Mass. 1933. [Peirce]

Post, Emil L.: Introduction to a general theory of elementary propositions. Am. Jl. Math., Vol. 43 (1921), pp. 163—85. [Post]

Prior, A. N. On propositions neither necessary nor impossible. Jl. of Symbolic Logic, Vol. 18 (1953), pp. 105—08. [Prior 1]

Three-valued logic and future contingents. The Philosophical Quarterly (St. Andrews), Vol. 3 (1953), pp. 317—26. [Prior 2]

Reichenbach, Hans: Wahrscheinlichkeitslogik und Alternativlogik. Erkenntnis, Vol. 5 (1935), pp. 177—78. [Reichenbach 1]

Philosophic Foundations of Quantum Mechanics. Berkeley 1944. [Reichenbach 2]

Rosser, J. B. — Turquette, A. R.: Many-valued Logics. Amsterdam 1952. [Rosser-Turquette]

Skolem, Thoralf: Bemerkungen zum Komprehensionsaxiom. Zeitschr. f. math. Logik und Grundlagen d. Math., Vol. 3 (1957), pp. 1—17. [Skolem]

SWIFT, J. D.: Algebraic properties of n-valued propositional calculi. Am. Math. Mo., Vol. 59 (1952), pp. 612—21. [Swift]

SZMIELEW, WANDA: Review of a paper by Bochvar. Jl. of Symbolic Logic, Vol. 11 (1946), p. 129. [Szmielew]

TARSKI, ALFRED: Logic, Semantics, Metamathematics. Papers from 1923 to 1938. Translated by J. H. Woodger. Oxford 1956. [Tarski]

USHENKO, A. P.: The many-valued logics. The Philosophical Review, Vol. 45 (1936), pp. 611—15. [Ushenko]

VASILIEV, N. A.: Imaginary (non-Aristotelian) logic. Atti del V Congresso Internazionale di Filosofia (Napoli 5—9 Maggio 1924), pp. 107—09. [Vasiliev]

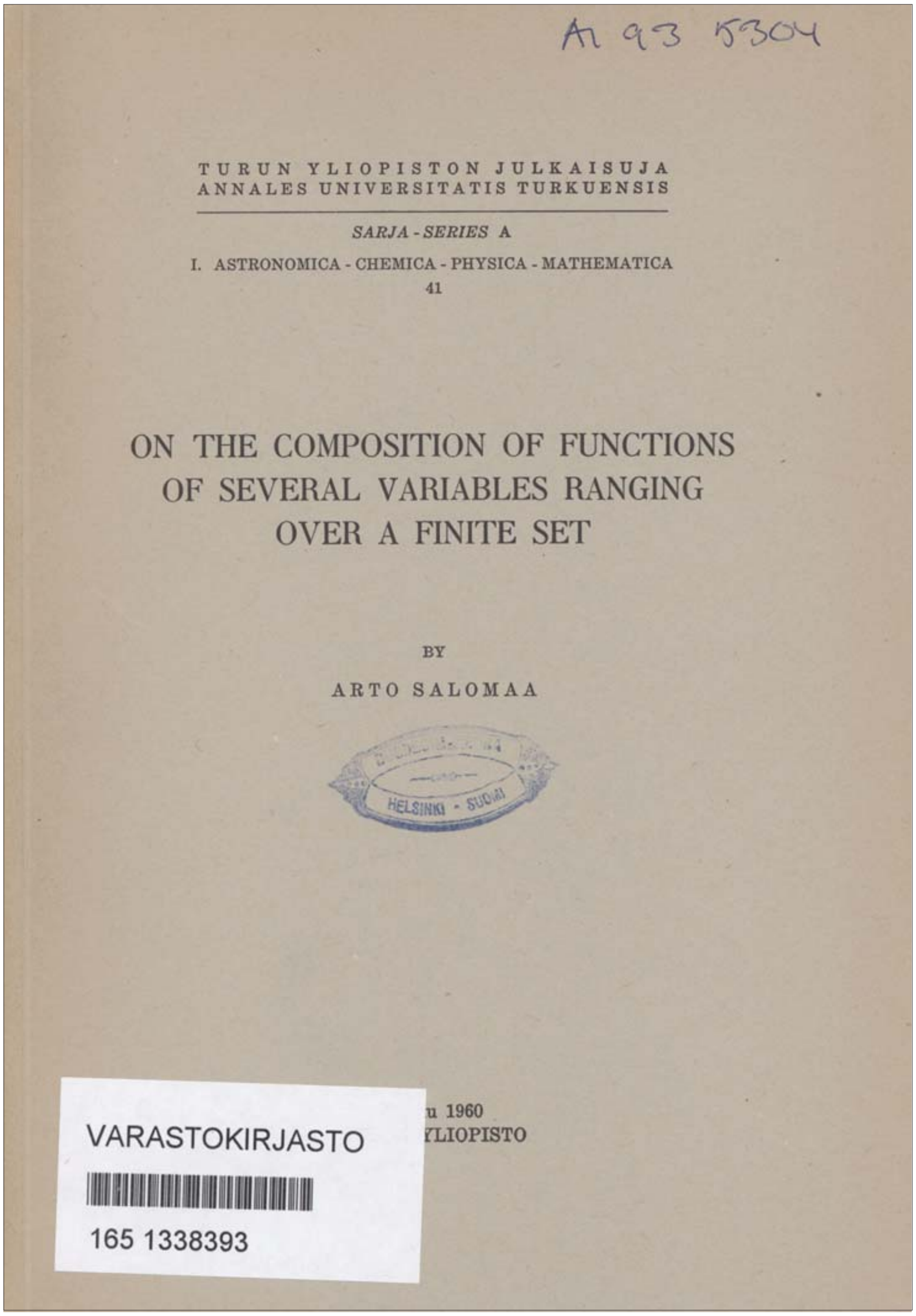
WEBB, D. L.: The algebra of n-valued logic. Comptes Rendus des Séances de la Société des Sciences et des Lettres de Varsovie, Classe III, XXIX Année (1936), pp. 153—68. [Webb]

WHITEHEAD, A. N. — RUSSELL, B.: Principia Mathematica, Vol. I. Second edition. Cambridge 1925. [Whitehead-Russell]

ZAWIRSKI, ZYGMUNT: Les logiques nouvelles et le champ de leur application. Revue de Métaphysique et de Morale, 39 Année (1932), pp. 503—519. [Zawirski 1]

Über das Verhältnis der mehrwertigen Logik zur Wahrscheinlichkeitsrechnung. Studia philosophica, Vol. 1 (1936), pp. 407—442. [Zawirski 2]

ZWICKY, F.: On a new type of reasoning and some of its possible consequences. The Physical Review, Second Series, Vol. 43 (1933), pp. 1031—33. [Zwicky]



TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

SARJA - SERIES A

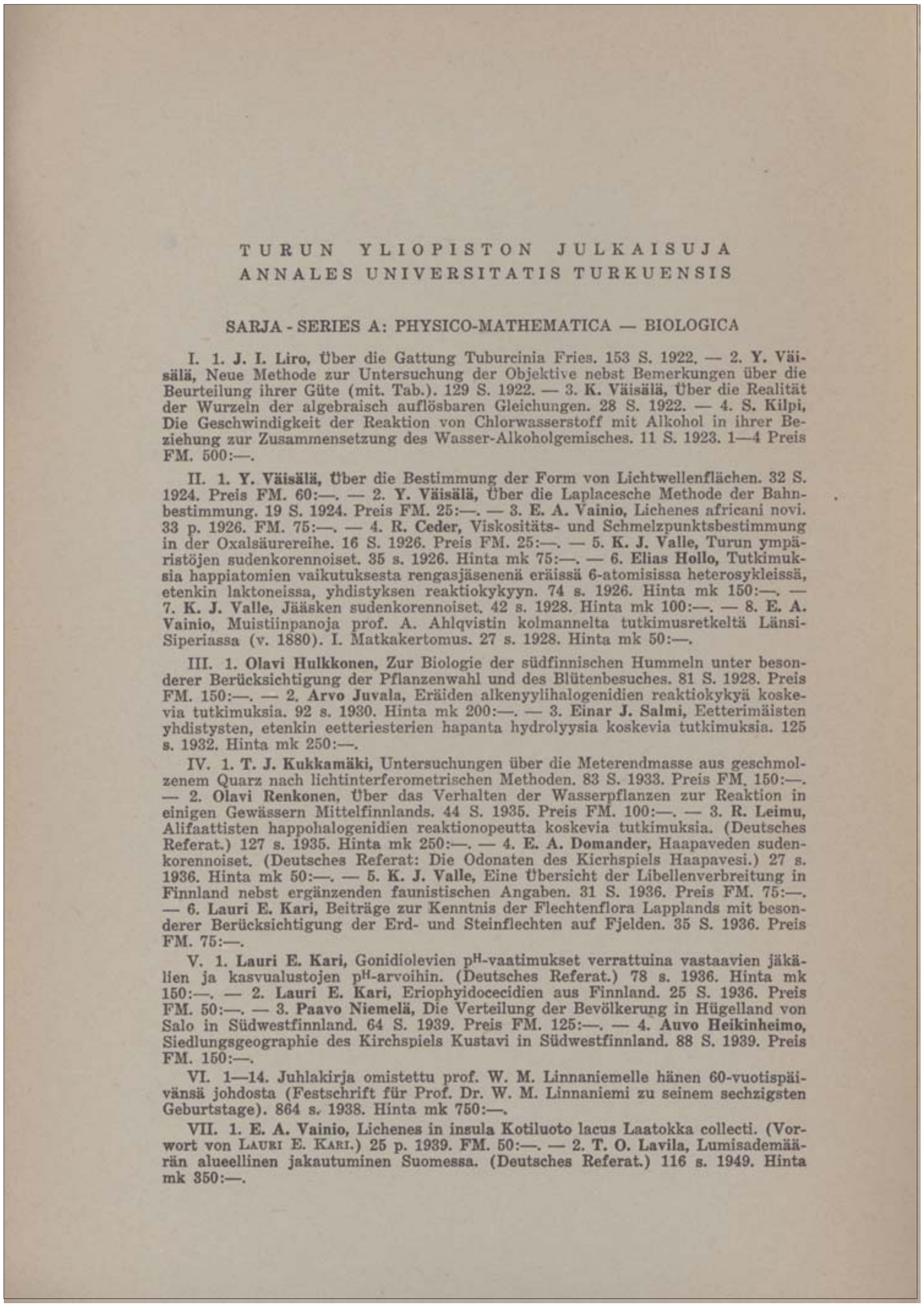
I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA
41

ON THE COMPOSITION OF FUNCTIONS OF SEVERAL VARIABLES RANGING OVER A FINITE SET

BY

ARTO SALOMAA

u 1960
YLIOPISTO



TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

SARJA - SERIES A: PHYSICO-MATHEMATICA — BIOLOGICA

I. 1. **J. I. Liro,** Über die Gattung Tuburcinia Fries. 153 S. 1922. — 2. **Y. Väisälä,** Neue Methode zur Untersuchung der Objektive nebst Bemerkungen über die Beurteilung ihrer Güte (mit. Tab.). 129 S. 1922. — 3. **K. Väisälä,** Über die Realität der Wurzeln der algebraisch auflösbaren Gleichungen. 28 S. 1922. — 4. **S. Kilpi,** Die Geschwindigkeit der Reaktion von Chlorwasserstoff mit Alkohol in ihrer Beziehung zur Zusammensetzung des Wasser-Alkoholgemisches. 11 S. 1923. 1—4 Preis FM. 500:—.

II. 1. **Y. Väisälä,** Über die Bestimmung der Form von Lichtwellenflächen. 32 S. 1924. Preis FM. 60:—. — 2. **Y. Väisälä,** Über die Laplacesche Methode der Bahnbestimmung. 19 S. 1924. Preis FM. 25:—. — 3. **E. A. Vainio,** Lichenes africani novi. 33 p. 1926. FM. 75:—. — 4. **R. Ceder,** Viskositäts- und Schmelzpunktsbestimmung in der Oxalsäurereihe. 16 S. 1926. Preis FM. 25:—. — 5. **K. J. Valle,** Turun ympäristöjen sudenkorennoiset. 35 s. 1926. Hinta mk 75:—. — 6. **Elias Hollo,** Tutkimuksia happiatomien vaikutuksesta rengasjäsenenä eräissä 6-atomisissa heterosykleissä, etenkin laktoneissa, yhdistyksen reaktiokykyyn. 74 s. 1926. Hinta mk 150:—. — 7. **K. J. Valle,** Jääsken sudenkorennoiset. 42 s. 1928. Hinta mk 100:—. — 8. **E. A. Vainio,** Muistiinpanoja prof. A. Ahlqvistin kolmannelta tutkimusretkeltä Länsi-Siperiassa (v. 1880). I. Matkakertomus. 27 s. 1928. Hinta mk 50:—.

III. 1. **Olavi Hulkkonen,** Zur Biologie der südfinnischen Hummeln unter besonderer Berücksichtigung der Pflanzenwahl und des Blütenbesuches. 81 S. 1928. Preis FM. 150:—. — 2. **Arvo Juvala,** Eräiden alkenyylihalogenidien reaktiokykyä koskevia tutkimuksia. 92 s. 1930. Hinta mk 200:—. — 3. **Einar J. Salmi,** Eetterimäisten yhdistysten, etenkin eetteriesterien hapanta hydrolyysia koskevia tutkimuksia. 125 s. 1932. Hinta mk 250:—.

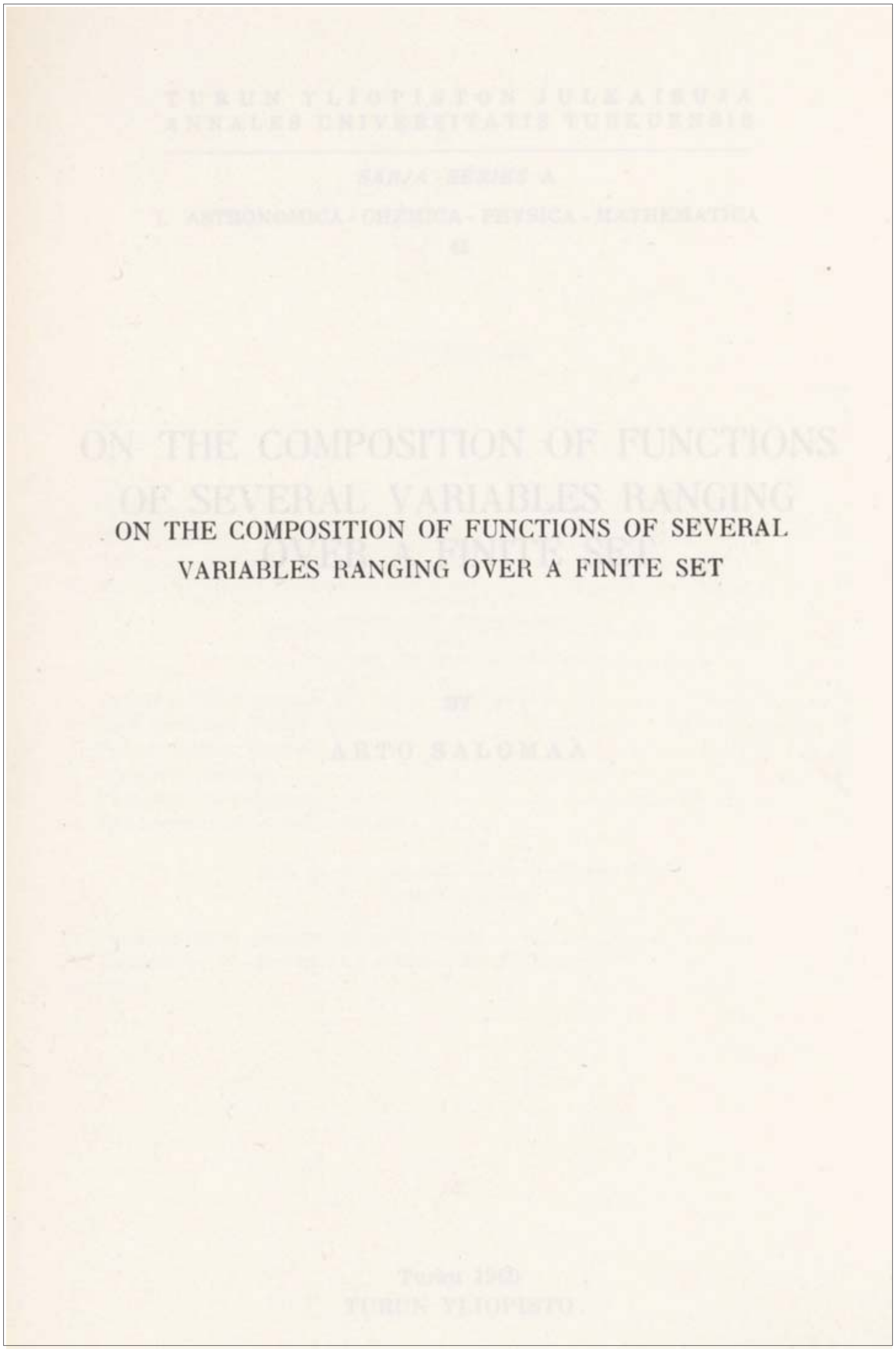
IV. 1. **T. J. Kukkamäki,** Untersuchungen über die Meterendmasse aus geschmolzenem Quarz nach lichtinterferometrischen Methoden. 83 S. 1933. Preis FM. 150:—. — 2. **Olavi Renkonen,** Über das Verhalten der Wasserpflanzen zur Reaktion in einigen Gewässern Mittelfinnlands. 44 S. 1935. Preis FM. 100:—. — 3. **R. Leimu,** Alifaattisten happohalogenidien reaktionopeutta koskevia tutkimuksia. (Deutsches Referat.) 127 s. 1935. Hinta mk 250:—. — 4. **E. A. Domander,** Haapaveden sudenkorennoiset. (Deutsches Referat: Die Odonaten des Kicrhspiels Haapavesi.) 27 s. 1936. Hinta mk 50:—. — 5. **K. J. Valle,** Eine Übersicht der Libellenverbreitung in Finnland nebst ergänzenden faunistischen Angaben. 31 S. 1936. Preis FM. 75:—. — 6. **Lauri E. Kari,** Beiträge zur Kenntnis der Flechtenflora Lapplands mit besonderer Berücksichtigung der Erd- und Steinflechten auf Fjelden. 35 S. 1936. Preis FM. 75:—.

V. 1. **Lauri E. Kari,** Gonidiolevien p^H-vaatimukset verrattuina vastaavien jäkälien ja kasvualustojen p^H-arvoihin. (Deutsches Referat.) 78 s. 1936. Hinta mk 150:—. — 2. **Lauri E. Kari,** Eriophyidocecidien aus Finnland. 25 S. 1936. Preis FM. 50:—. — 3. **Paavo Niemelä,** Die Verteilung der Bevölkerung in Hügelland von Salo in Südwestfinnland. 64 S. 1939. Preis FM. 125:—. — 4. **Auvo Heikinheimo,** Siedlungsgeographie des Kirchspiels Kustavi in Südwestfinnland. 88 S. 1939. Preis FM. 150:—.

VI. 1—14. **Juhlakirja omistettu prof. W. M. Linnaniemelle hänen 60-vuotispäivänsä johdosta (Festschrift für Prof. Dr. W. M. Linnaniemi zu seinem sechzigsten Geburtstage).** 864 s. 1938. Hinta mk 750:—.

VII. 1. **E. A. Vainio,** Lichenes in insula Kotiluoto lacus Laatokka collecti. (Vorwort von LAURI E. KARI.) 25 p. 1939. FM. 50:—. — 2. **T. O. Lavila,** Lumisademäärän alueellinen jakautuminen Suomessa. (Deutsches Referat.) 116 s. 1949. Hinta mk 350:—.

ON THE COMPOSITION OF FUNCTIONS OF SEVERAL VARIABLES RANGING OVER A FINITE SET



TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

SARJA - SERIES A

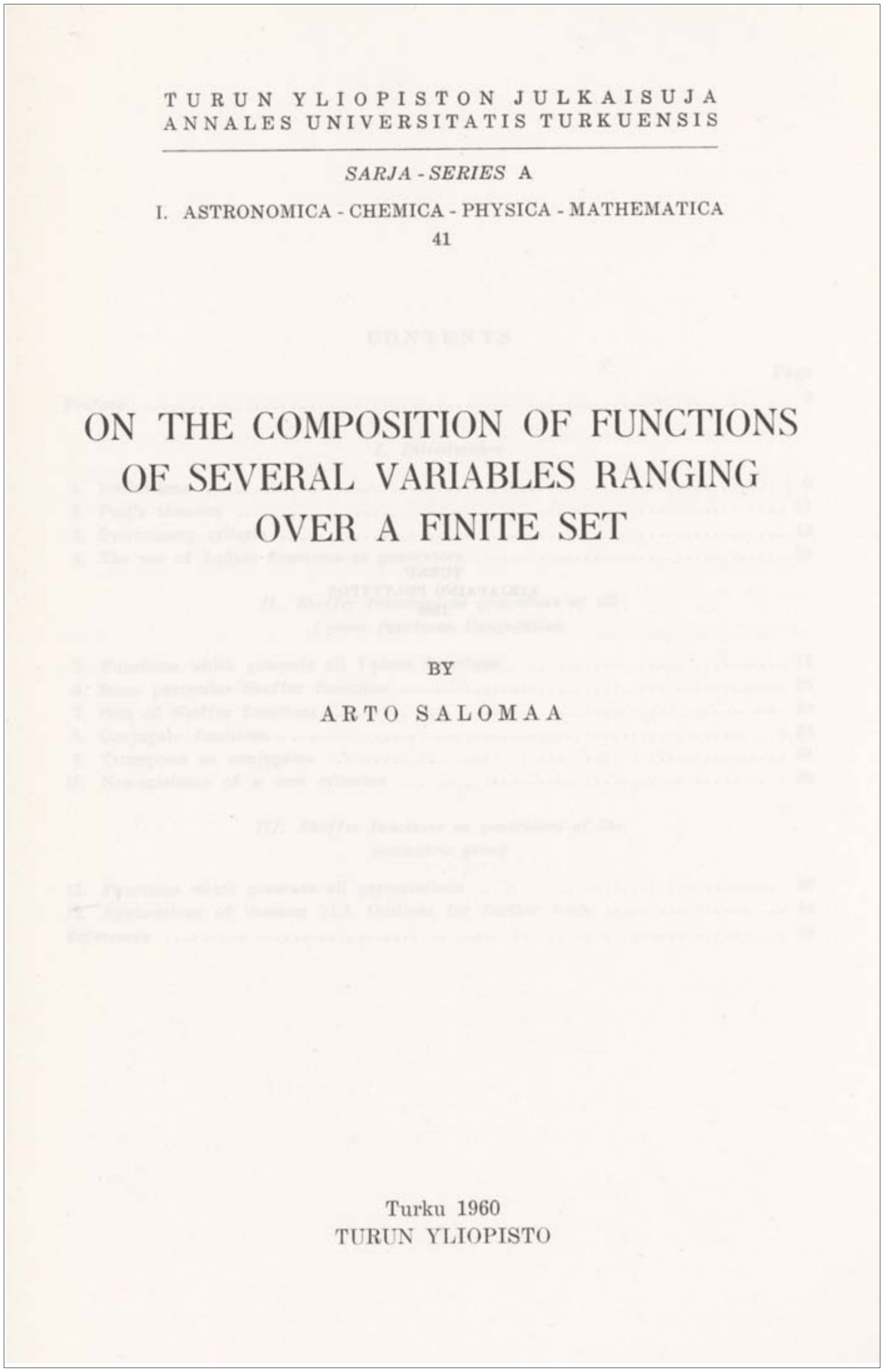
I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA
41

ON THE COMPOSITION OF FUNCTIONS
OF SEVERAL VARIABLES RANGING
OVER A FINITE SET

BY

ARTO SALOMAA

Turku 1960
TURUN YLIOPISTO



TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

SARJA - SERIES A

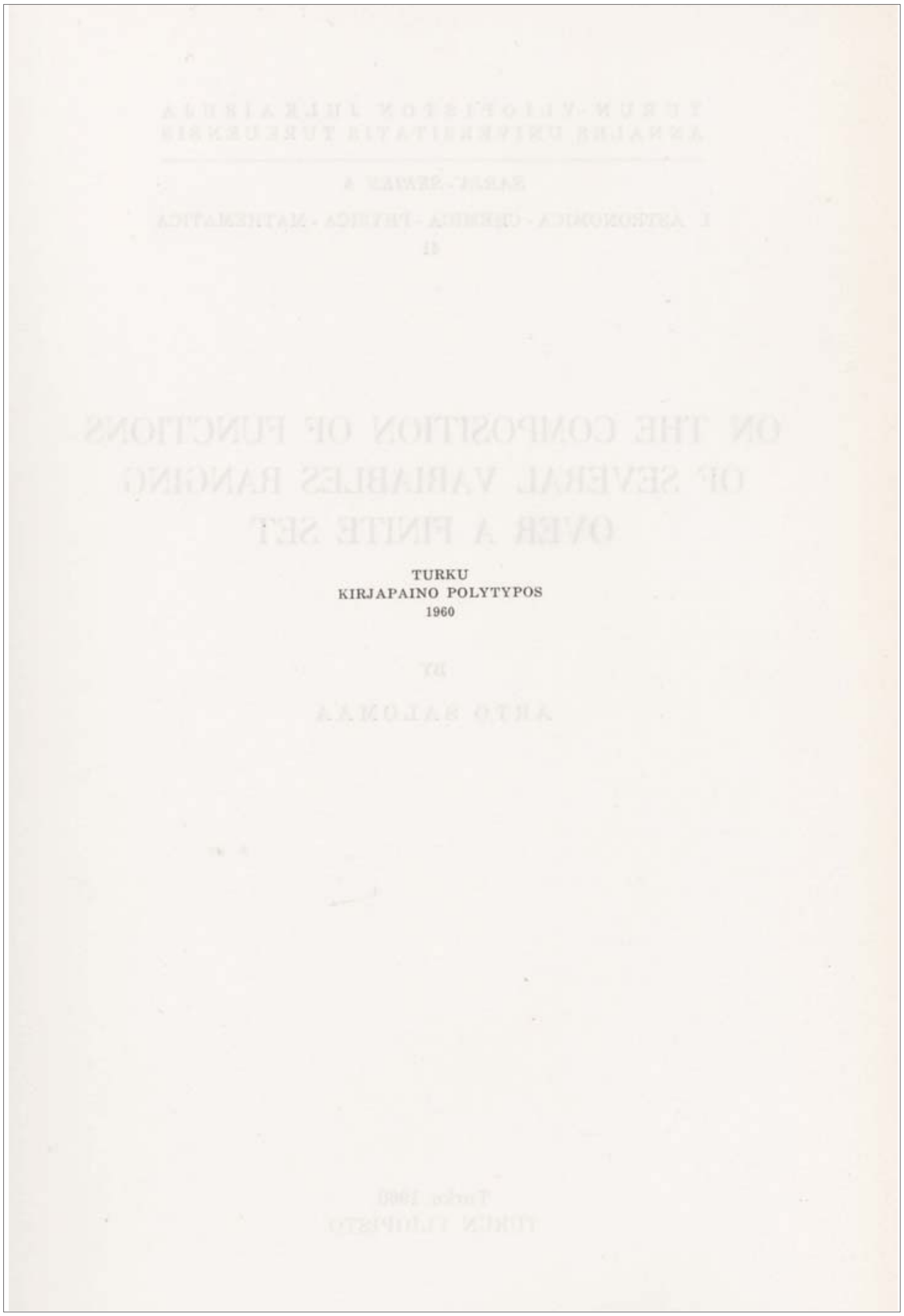
I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA
41

ON THE COMPOSITION OF FUNCTIONS OF SEVERAL VARIABLES RANGING OVER A FINITE SET

BY

ARTO SALOMAA

Turku 1960
TURUN YLIOPISTO



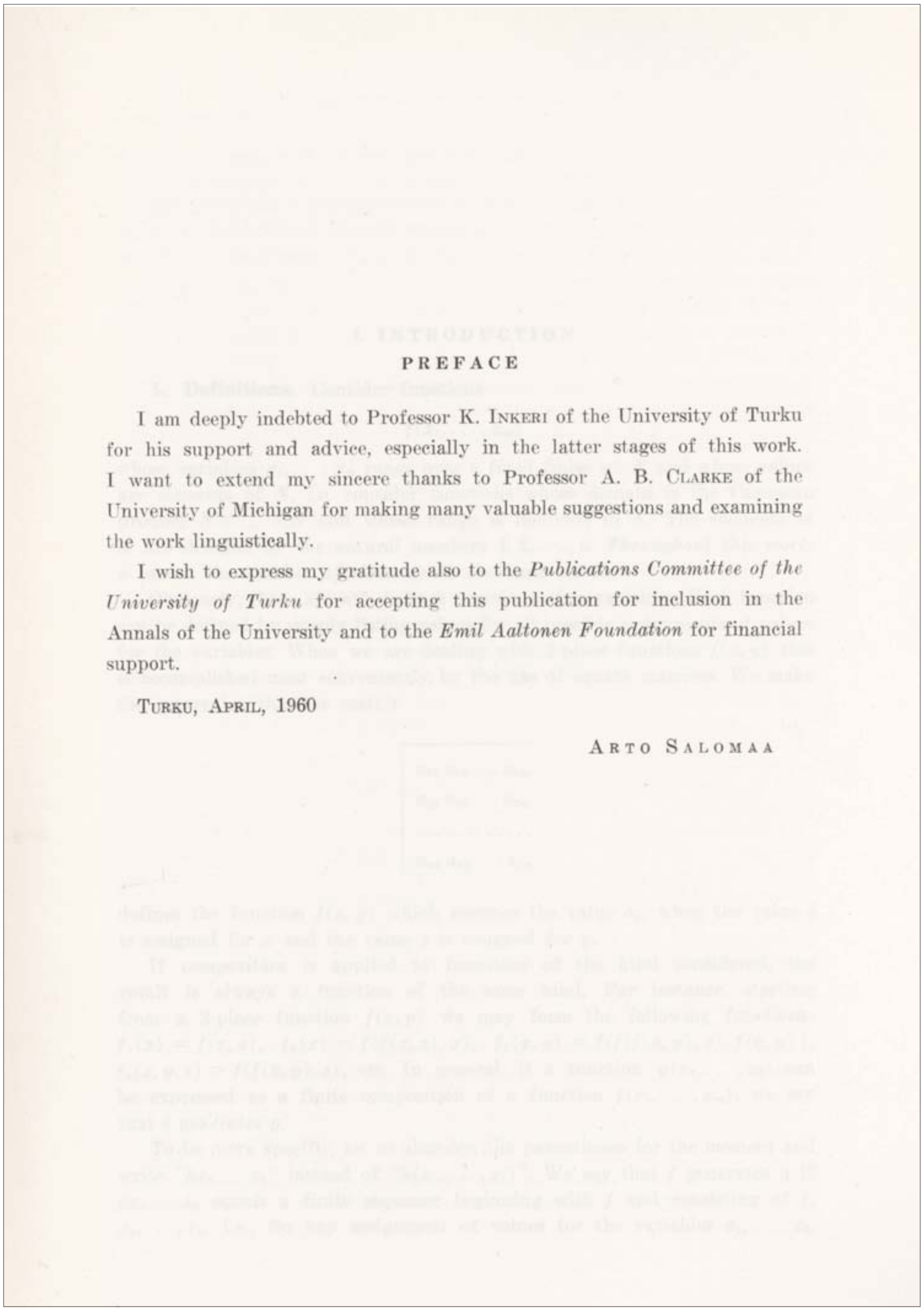
TURKU
KIRJAPAINO POLYTYPOS
1960

CONTENTS

I. Introduction

II. Sheffer functions as generators of all 1-place functions. Conjugation

III. Sheffer functions as generators of the symmetric group



PREFACE

I am deeply indebted to Professor K. Inkeri of the University of Turku for his support and advice, especially in the latter stages of this work. I want to extend my sincere thanks to Professor A. B. Clarke of the University of Michigan for making many valuable suggestions and examining the work linguistically.

I wish to express my gratitude also to the *Publications Committee of the University of Turku* for accepting this publication for inclusion in the Annals of the University and to the *Emil Aaltonen Foundation* for financial support.

Turku, April, 1960

Arto Salomaa

I. INTRODUCTION

1. Definitions. Consider functions

$$f(x_1, \dots, x_m)$$

whose variables $x_1, \dots, x_m$ range over a *fixed* finite set N and whose values are elements of N, i.e. consider functions whose domain is the Cartesian product $N \times \dots \times N$ and whose range is included in N. The elements of N are denoted by the natural numbers $1, 2, \dots, n$. *Throughout this work, n means the number of elements in the basic set N.*

Obviously, there are n^{n^m} distinct functions of m variables. Each function can be defined by simply listing values for all possible assignments of values for the variables. When we are dealing with 2-place functions $f(x, y)$ this is accomplished most conveniently by the use of square matrices. We make the convention that the matrix

$$\begin{array}{|l}
\hline
a_{11}\ a_{12} \dots a_{1n} \\
a_{21}\ a_{22} \dots a_{2n} \\
\dots\dots\dots\dots \\
a_{n1}\ a_{n2} \dots a_{nn}
\end{array}$$

defines the function $f(x, y)$ which assumes the value a_{ij} when the value i is assigned for x and the value j is assigned for y.

If *composition* is applied to functions of the kind considered, the result is always a function of the same kind. For instance, starting from a 2-place function $f(x, y)$ we may form the following functions: $f_1(x) = f(x, x)$, $f_2(x) = f(f(x, x), x)$, $f_3(x, y) = f(f(f(x, y), x), f(x, y))$, $f_4(x, y, z) = f(f(x, y), z)$, etc. In general, if a function $g(x_1, \dots, x_k)$ can be expressed as a finite composition of a function $f(x_1, \dots, x_m)$, we say that *f generates g*.

To be more specific, let us abandon the parentheses for the moment and write "$hx_1 \dots x_l$" instead of "$h(x_1, \dots, x_l)$". We say that f generates g if $gx_1 \dots x_k$ equals a finite sequence beginning with f and consisting of f, $x_1, \dots, x_k$. I.e., for any assignment of values for the variables $x_1, \dots, x_k$,

$$gx_1 \ldots x_k = S(f, x_1, \ldots, x_k)$$

where S is some fixed finite sequence beginning with f and consisting of $f, x_1, \ldots, x_k$. Similarly, we say that g is generated by the functions $f_1, \ldots, f_r$ if $gx_1 \ldots x_k$ equals a finite sequence beginning with some f_i and consisting of $f_1, \ldots, f_r, x_1, \ldots, x_k$.

S is said to be a *composition sequence* of g in terms of f.[1] Thus, $fffxyxfxy$ is a composition sequence of f_3 in terms of f. (In what follows, we shall in most cases use our original notation with parentheses.) Composition sequences are not, in general, unique. In fact, if f generates the identity permutation and an arbitrary function g, then f generates g in infinitely many ways, i.e. g has infinitely many composition sequences in terms of f.

We now present the following fundamental

DEFINITION. *A function $f(x_1, \ldots, x_m)$ which generates every function is termed a Sheffer function.*

We want to emphasize that when we speak of "functions" we always mean functions whose variables range over N and whose values are elements of N.[2] To omit trivial cases in the following proofs, we also assume that N consists of more than one element, i.e. $n > 1$.

We introduce some further terminology and conventions. We use ordinary set-theoretic symbols: $A \cup B$ is the union of the sets A and B, $\{a_1, \ldots, a_k\}$ is the set consisting of the elements $a_1, \ldots, a_k$, and $\{x \mid (\ldots)\}$

[1] The proof of the fact that every composition sequence determines at most one function is omitted.

[2] HISTORICAL REMARKS. The study of the functions of the kind considered has begun in connection with the study of two- and many-valued propositional logics. The interest of Sheffer functions lies not only in the possibility of defining all functions in terms of one function but also in the fact that any propositional logic with only one primitive connective whose truth-function is a Sheffer function is axiomatizable, as shown in [15]. Later on, however, the research has been carried on also independently of logical interpretations.

The well-known "stroke" function introduced by SHEFFER in [12] is the first function presented in the literature which is, according to our definition, a Sheffer function. However, the idea was known already earlier to PEIRCE (cf. [7], 4.264—265). Both Sheffer and Peirce were concerned only with the case $n = 2$. The general approach to the problem was introduced by POST who proved in [10] a theorem essentially the same as theorem 2.1 below. The first decision method for Sheffer functions is due to ZYLIŃSKI, [21]. He applied the method only for the case $n = 2$ but it can readily be generalized, as will be seen in theorem 3.1. SŁUPECKI has proved in [14] a theorem which implies theorem 5.1 below. However, theorem 11.1 gives a much stronger result. We mention, finally, that certain particular functions, defined for any n, have been shown to be Sheffer functions by WEBB, MARTIN, GÖTLIND, EVANS and HARDY in [17]—[19], [4]—[6], [2] and [1].

is the set consisting of all elements x which satisfy the condition formulated in the parentheses. We use the symbol $+'$ to denote that addition is carried out modulo n. I.e. $a+'b$ is that number in the set $\{1, 2, \ldots, n\}$ which is congruent to $a+b$ modulo n. The symbol $-'$ is used in the same way. Finally, by the *value sequence* of a function $f(x_1, \ldots, x_m)$ we mean the sequence of values assumed by f, these values written in the order $f(1, \ldots, 1, 1)$, $f(1, \ldots, 1, 2), \ldots, f(1, \ldots, 1, n)$, $f(1, \ldots, 2, 1)$, $f(1, \ldots, 2, 2)$, $\ldots, f(n, \ldots, n, n)$.

2. Post's theorem. In the definition in the preceding section, it is required that a function f must generate every function in order to be a Sheffer function. It is, therefore, necessary that f generates all of the n^{n^2} 2-place functions. The following theorem[1] shows that this is also sufficient.

THEOREM 2.1. *An i-place function $f(x_1, \ldots, x_i)$ which generates all j-place functions is a Sheffer function, provided $j \geqq 2$.*

Proof. Obviously all k-place functions are obtained from the set of all l-place functions, $k < l$, by identifying some of the variables. Therefore, it suffices to prove the theorem for $j = 2$.

Assume $f(x_1, \ldots, x_i)$ generates all 2-place functions $g(x, y)$. Then it generates also all 1-place functions. Consider now the following family of functions (where b and c run independently through the numbers $1, 2, \ldots, n$):

$$t_c^b(x) = c \text{ when } x = b, \; t_c^b(x) = n \text{ when } x \neq b,$$

and the following functions:

$$f_1(x, y) = \min(x, y),$$
$$f_2(x, y) = \max(x, y).$$

By assumption, $f(x_1, \ldots, x_i)$ generates all these functions. If we abandon the parentheses it is more convenient to use the notation $x_1 f_1 x_2 f_1 x_3$, instead of $f_1 x_1 f_1 x_2 x_3$ or $f_1 f_1 x_1 x_2 x_3$, for the function $\min(x_1, x_2, x_3)$, with a similar convention regarding f_2.

For a fixed m, we define now the following family of functions (where $c, b_1, \ldots, b_m$ run independently through the numbers $1, 2, \ldots, n$):

$$s_c^{b_1, \ldots, b_m}(x_1, \ldots, x_m) = t_c^{b_1}(x_1) f_2 \ldots f_2 t_c^{b_m}(x_m).$$

[1] The theorem is due to Post who presented it in [10] in the form: every function can be expressed as a finite composition of the two functions $f(x, y) = \min(x, y)$ and $g(x) = x+'1$.

It is seen that $s_c^{b_1, \ldots, b_m}(x_1, \ldots, x_m)$ assumes the value c when $x_1 = b_1, \ldots, x_m = b_m$. For all other combinations of values for the variables, the function in question assumes the value n. Let $g(x_1, \ldots, x_m)$ be any m-place function. Then we have

$$\begin{aligned} g(x_1, \ldots, x_m) = {} & s_{g(1, \ldots, 1, 1)}^{1, \ldots, 1, 1}(x_1, \ldots, x_m)\ f_1 s_{g(1, \ldots, 1, 2)}^{1, \ldots, 1, 2}(x_1, \ldots, x_m) f_1 \ldots \\ & f_1 s_{g(1, \ldots, 1, n)}^{1, \ldots, 1, n}(x_1, \ldots, x_m)\ f_1 s_{g(1, \ldots, 2, 1)}^{1, \ldots, 2, 1}(x_1, \ldots, x_m) f_1 \ldots \\ & f_1 s_{g(n, \ldots, n, n)}^{n, \ldots, n, n}(x_1, \ldots, x_m). \end{aligned}$$

So $g(x_1, \ldots, x_m)$ is generated by $f(x_1, \ldots, x_i)$. Since m was arbitrary and g was an arbitrary m-place function, we conclude that $f(x_1, \ldots, x_i)$ is a Sheffer function.

From the proof above we see how any function may be represented as a finite composition of 2-place functions. In what follows we shall confine our attention mainly to 2-place functions. Then we are able to discuss typical algebraic properties, e.g. associativity.

It is clear that if $i = 1$ the hypothesis of theorem 2.1 cannot be satisfied, i.e. a 1-place function is never a Sheffer function. This is due to the fact that 1-place functions generate only 1-place functions, whereas 2-place functions may generate functions of any number of variables. On the other hand, as will be seen in section 5, the requirement $j \geqq 2$ is not essential.

3. Preliminary criteria. We turn now to the discussion of some criteria for deciding whether a given function is a Sheffer function. We prove first the following general

THEOREM 3. 1. *Let $f(x_1, \ldots, x_m)$ be a given function and let $F^{(i)}$ be the sets of functions defined by*

$$F^{(0)} = \{x_1, \ldots, x_h\},$$

$$F^{(i)} = F^{(i-1)} \cup \{z \,|\, z = f(\xi_1, \ldots, \xi_m) \ \text{where} \ \xi_1, \ldots, \xi_m \,\varepsilon\, F^{(i-1)}\},$$

for $i = 1, 2, \ldots$. Then for some $r \leqq n^{n^h}$, every h-place function generated by f is in $F^{(r)}$.[1]

Proof. Let $F_v^{(i)}$ denote the set of value sequences of the functions in $F^{(i)}$. Since the number of all possible value sequences of h-place functions is n^{n^h}, there exists a number $r \leqq n^{n^h}$ such that every value sequence contained in $F_v^{(r)}$ is already contained in $F_v^{(r-1)}$. We shall now prove that the functions

[1] The definitions of the sets $F^{(i)}$ and the general method of proof are based on some ideas contained in [21], [3] and [11]. We present the proof in detail because there is no explicit proof of this important theorem in the literature.

in $F^{(r-1)}$ exhaust all h-place functions which are generated by $f(x_1, \ldots, x_m)$, i.e. that every value sequence contained in any $F_v^{(j)}$, $j \geqq r$, is contained in $F_v^{(r-1)}$.

We write $j = r+k$ and apply induction on k. The assertion holds for $k = 0$, by the definition of r. Suppose it holds for some fixed value k. Consider an arbitrary function

$$f^{(r+k+1)}(x_1, \ldots, x_h)$$

which is in $F^{(r+k+1)}$ but not in $F^{(r+k)}$. It can be written in the form

$$f(f_1, \ldots, f_m)$$

where $f_1, \ldots, f_m$ are functions in $F^{(r+k)}$. By the inductive hypothesis, there are functions $f'_1, \ldots, f'_m$ in $F^{(r-1)}$ which have the same value sequences as $f_1, \ldots, f_m$, respectively. Clearly $f(f'_1, \ldots, f'_m)$ has the same value sequence as $f^{(r+k+1)}$. But $f(f'_1, \ldots, f'_m)$ belongs to $F^{(r)}$ and, therefore, its value sequence belongs to $F_v^{(r)}$. From this we infer, by the definition of r, that the value sequence of $f^{(r+k+1)}$ is in $F_v^{(r-1)}$. But this means that the assertion holds for the value $k+1$ which completes the inductive step. Hence theorem 3. 1 follows.

Theorem 3.1 gives a method of deciding whether the given function $f(x_1, \ldots, x_m)$ is a Sheffer function. Choose $h = 2$ and find the number r. By theorem 2.1, $f(x_1, \ldots, x_m)$ is a Sheffer function if and only if the value sequence of every 2-place function is in the set $F_v^{(r-1)}$.

Given a Sheffer function f, there is a method of finding a composition sequence for any function g in terms of f. This follows directly from the proofs of theorems 2.1 and 3.1. The method presented above is of very little practical value — both for this purpose and for deciding whether a given function is a Sheffer function — since the number of functions in the sets $F^{(i)}$ grows enormously large. In sections 5 and 11 we shall prove theorems which give rise to essential simplifications of this method.

We conclude this section with two negative criteria, i.e. we show that certain properties are never possessed by a Sheffer function. The first one is very simple and is stated in the form of a theorem for referential purposes only.

THEOREM 3.2. *If f is a Sheffer function then there is no proper subset N_1 of the set $\{1, 2, \ldots, n\}$ such that any assignment of numbers in N_1 to the variables of f gives a value of f which belongs to N_1.*[1]

Proof. If there is such an N_1 then f cannot generate any function g whose value does not belong to N_1, for some assignment of numbers in N_1 to the variables of g. Hence, f is not a Sheffer function.

[1] Theorem 3.2 is mentioned both in [6] and in [16]. Martin has introduced in [6] also three other similar closure properties which we are not going to use.

A consequence of theorem 3.2 is that if $f(x_1, \ldots, x_m)$ is a Sheffer function then $f(i, \ldots, i) \neq i$, for any i.

The proof of the following theorem is more complicated. We consider 2-place functions and say that a function is *associative* if

$$\text{(A)} \qquad f(i, f(j,k)) = f(f(i,j),k), \text{ for any } i, j \text{ and } k.$$

THEOREM 3.3. *No 2-place Sheffer function is associative.*

Proof. We show that if (A) holds for some Sheffer function $f(x,y)$ then $f(x,y)$ satisfies certain conditions which imply that $f(x,y)$ is not a Sheffer function and we, therefore, have a contradiction.

Suppose (A) holds for some Sheffer function $f(x,y)$. Then the general associative law is true for $f(x,y)$, i.e. in any composition sequence we can associate the variables in the way we prefer. In particular, the composition sequence of any 1-place function can be written in the "normal form"

$$f(x, f(x, \ldots, f(x, f(x,x)) \ldots)).$$

This notion is expressed more exactly as follows. We say that the composition sequence of a 1-place function is in the normal form if it is $f(x,x)$ or $f(x, \overline{f}(x))$ where $\overline{f}(x)$ is in the normal form.

Since $f(x,y)$ is a Sheffer function it generates the following functions:

$$g_i(x) = x +' i, \text{ for } i = 1, 2, \ldots, n.$$

We write the composition sequences of these functions in the normal form:

$$\begin{aligned} g_1(x) &= f(x, f_1(x)), \\ g_2(x) &= f(x, f_2(x)), \\ &\vdots \\ g_n(x) &= f(x, f_n(x)). \end{aligned}$$

Consider the matrix of $f(x,y)$. From the first of the preceding equations we see that there must be the number $i +' 1$ at some place in the i^{th} row. This is true for any i, $1 \leqq i \leqq n$. And generally, from the j^{th} equation we see that there must be the number $i +' j$ in the i^{th} row. When we let j range over the numbers $1, 2, \ldots, n$ we get the following

LEMMA 3.4. *In the matrix of $f(x,y)$ each row represents a permutation of the numbers $1, 2, \ldots, n$.*

Denote by F the set of all 1-place functions generated by $f(x,y)$. Write the composition sequences of all functions belonging to F in the normal form. We are going to show that there are at most $n!$ functions in F. Since the total number of 1-place functions is n^n, we conclude that $f(x,y)$ is not a Sheffer function, contrary to the hypothesis.

We introduce some notations:

$$f^1(x) = f(x, x),$$
$$f^{j+1}(x) = f(x, f^j(x)).$$

By the associative property, every function in F has the form $f^k(x)$, for some k. We have to show that at most $n!$ of these functions are different. It suffices to show that for some $t \leqq n!$, $f^{t+1} = f^1$.

For some fixed i, consider the sequence $f^1(i)$, $f^2(i), \ldots$. (Here obviously i has the range $1 \leqq i \leqq n$. We do not specify the range of a variable if it is clear from the context.) Because of lemma 3.4 and the definition of $f^j(x)$, if $f^a(i) = f^b(i)$ for some integers a, b (> 1), then also $f^{a-1}(i) = f^{b-1}(i)$. This implies that there is a number n_i $(1 < n_i \leqq n+1)$ such that $f^{n_i}(i) = f^1(i)$. Consequently $f^{n_i+j-1}(i) = f^j(i)$ for all j, and thus the numbers $f^1(i), f^2(i), \ldots$ form a periodic sequence with period of length $\leqq n$.

Let the least common multiple of the numbers $n_i - 1$ $(1 \leqq i \leqq n)$ be t. Then obviously $f^{t+1}(i) = f^1(i)$, for any i. Also $t \leqq n!$ because it is the least common multiple of n numbers, each of which is $\leqq n$. Hence theorem 3.3 follows.

4. The use of 1-place functions as generators.

As we have already pointed out, any composition of 1-place functions is a 1-place function and, therefore, 1-place functions can never be Sheffer functions. In this section we are concerned with the following problem which is important for our subsequent investigations: How many 1-place functions are needed to generate all 1-place functions and, in particular, which 1-place functions are such generators? If $n = 2$ then two functions suffice for this purpose, namely, the transposition (12) and one of the two functions which are not permutations. No less than two functions are sufficient. The solution of this problem, for $n \geqq 3$, is presented in the following theorem. We use the term "a basis of the symmetric group S_n" to mean any two permutations which generate S_n.

THEOREM 4.1. *Assume that $n \geqq 3$. Then three 1-place functions generate all 1-place functions if and only if two of them form a basis of the symmetric group S_n and the third assumes exactly $n-1$ values. No less than three 1-place functions generate all 1-place functions.*[1]

[1] The theorem is, essentially, due to PICCARD. She has shown in [8] that the following three functions $f_1(x)$, $f_2(x)$ and $f_3(x)$ generate all 1-place functions: $f_1(x) = x + '1$; $f_2(x) = x$ for $1 \leqq x \leqq n-2$, $f_2(n-1) = n$, $f_2(n) = n-1$; $f_3(x) = x$ for $2 \leqq x \leqq n$, $f_3(1) = 2$. It had been shown earlier by EILENBERG that no two functions suffice for this purpose in the general case (cf. [13], p. 212). The idea to replace f_3 by any function assuming exactly $n-1$ values is due to Martin, [6].

Proof. Let $\alpha(x)$ and $\beta(x)$ form a basis of S_n and $\gamma(x)$ be a function assuming exactly n—1 values. To prove the first part of the theorem, we have to show that every 1-place function equals a finite composition of α, β and γ. We proceed inductively. Let F_i where $1 \leqq i \leqq n$ be the set of all such 1-place functions which assume exactly i values. Then every function in the set F_n is generated by α, β and γ (as a matter of fact, by α and β alone). We make the following inductive hypothesis: every function in the set F_i $(1 < i \leqq n)$ is generated by α, β and γ.

Let $f(x)$ be an arbitrary function in F_{i-1}. Then there are two numbers p and q where $p \neq q$ such that $f(p) = f(q)$. There is also a number r $(1 \leqq r \leqq n)$ such that $f(x) \neq r$, for any x. Let $g(x)$ be the function defined as follows:

$$g(x) = f(x) \text{ for } x \neq p,\ g(p) = r.$$

By the inductive hypothesis, g is generated by α, β and γ.

Consider the function $\gamma(x)$. Since it assumes exactly n—1 values, there are two distinct numbers k and l such that $\gamma(k) = \gamma(l)$ and, in addition, the numbers $\gamma(x)$ where $x \neq l$ are all different. Furthermore, there is a number u $(1 \leqq u \leqq n)$ such that $\gamma(x) \neq u$, for any x.

Let $s_1(x)$ be the function which maps the number $\gamma(k) = \gamma(l)$ to k, u to l, and $\gamma(x)$ to x when $x \neq k, l$. $s_1(x)$ is a permutation and, therefore, the function

$$\gamma_1(x) = s_1\gamma(x)$$

is generated by α, β and γ. It is seen that $\gamma_1(l) = k$, whereas $\gamma_1(x) = x$ for $x \neq l$.

Let $s_2(x)$ be any permutation such that $s_2(r) = l$ and $s_2(f(p)) = k$. Then it is easily verified that

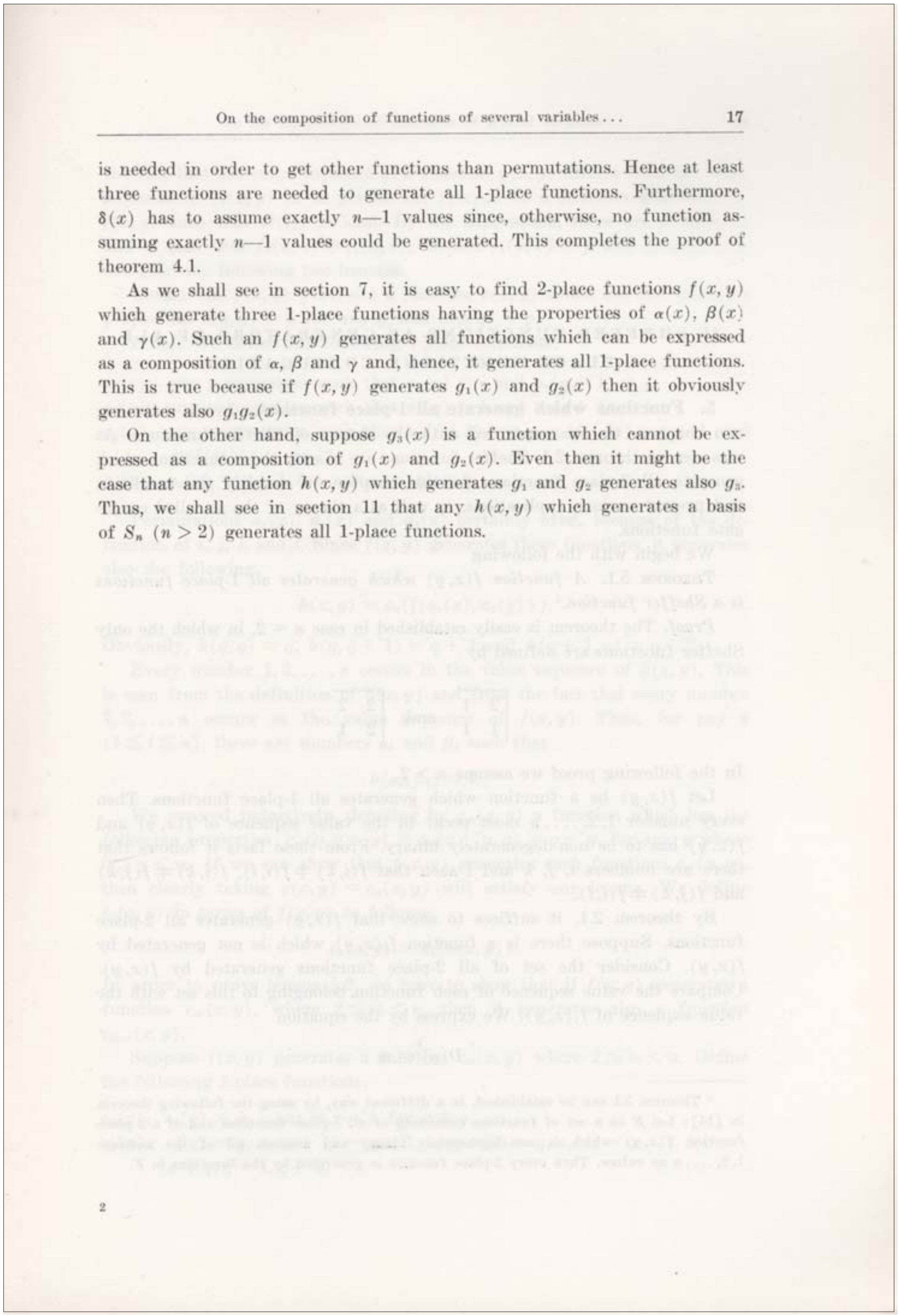
$$f(x) = s_2^{-1}\gamma_1 s_2 g(x)$$

where s_2^{-1} is the inverse of s_2. This means that an arbitrary function in F_{i-1} is generated by α, β and γ. So the induction has been completed, and we have shown that α, β and γ generate all 1-place functions.

The proof of the remaining part of the theorem depends, mainly, on the following simple fact. If in a composition of 1-place functions a function assuming exactly i values occurs, then the whole composition assumes at most i values.

If $n > 2$ then two permutations are needed to generate all permutations, since the symmetric group S_n is not cyclic.[1] One additional function $\delta(x)$

[1] It is a well-known fact that two permutations suffice for this purpose. As an example, we mention the permutations $f_1(x)$ and $f_2(x)$ in the previous footnote. The question of which permutations form a basis of S_n has been studied by Piccard. (Cf. [9] which is an exposition of some of her main results.)



is needed in order to get other functions than permutations. Hence at least three functions are needed to generate all 1-place functions. Furthermore, $\delta(x)$ has to assume exactly n—1 values since, otherwise, no function assuming exactly n—1 values could be generated. This completes the proof of theorem 4.1.

As we shall see in section 7, it is easy to find 2-place functions $f(x, y)$ which generate three 1-place functions having the properties of $\alpha(x)$, $\beta(x)$ and $\gamma(x)$. Such an $f(x, y)$ generates all functions which can be expressed as a composition of α, β and γ and, hence, it generates all 1-place functions. This is true because if $f(x, y)$ generates $g_1(x)$ and $g_2(x)$ then it obviously generates also $g_1g_2(x)$.

On the other hand, suppose $g_3(x)$ is a function which cannot be expressed as a composition of $g_1(x)$ and $g_2(x)$. Even then it might be the case that any function $h(x, y)$ which generates g_1 and g_2 generates also g_3. Thus, we shall see in section 11 that any $h(x, y)$ which generates a basis of S_n $(n > 2)$ generates all 1-place functions.

II. SHEFFER FUNCTIONS AS GENERATORS OF ALL 1-PLACE FUNCTIONS. CONJUGATION

5. Functions which generate all 1-place functions. In the following two chapters we are concerned with the theory of Sheffer functions. As was seen in theorem 2.1, Sheffer functions are exactly those functions which generate all 2-place functions. In this chapter we simplify this condition and present various applications, as well as a theory of the so-called conjugate functions.

We begin with the following

THEOREM 5.1. *A function $f(x,y)$ which generates all 1-place functions is a Sheffer function.*[1]

Proof. The theorem is easily established in case $n = 2$, in which the only Sheffer functions are defined by

$$\begin{array}{|cc} \hline 2 & 1 \\ 1 & 1 \end{array} \quad \text{and} \quad \begin{array}{|cc} \hline 2 & 2 \\ 2 & 1 \end{array}.$$

In the following proof we assume $n > 2$.

Let $f(x,y)$ be a function which generates all 1-place functions. Then every number $1, 2, \dots, n$ must occur in the value sequence of $f(x,y)$ and $f(x,y)$ has to be non-degenerately binary. From these facts it follows that there are numbers i, j, k and l such that $f(i,k) \neq f(i,l)$, $f(i,k) \neq f(j,k)$ and $f(j,k) \neq f(i,l)$.

By theorem 2.1, it suffices to show that $f(x,y)$ generates all 2-place functions. Suppose there is a function $f_1(x,y)$ which is not generated by $f(x,y)$. Consider the set of all 2-place functions generated by $f(x,y)$. Compare the value sequence of each function belonging to this set with the value sequence of $f_1(x,y)$. We express by the equation

$$D(g) = m$$

[1] Theorem 5.1 can be established, in a different way, by using the following theorem in [14]: Let F be a set of functions consisting of all 1-place functions and of a 2-place function $f(x,y)$ which is non-degenerately binary and assumes all of the numbers $1, 2, \dots, n$ as values. Then every 2-place function is generated by the functions in F.

the fact that the value sequence of a function $g(x, y)$ differs from the value sequence of $f_1(x, y)$ in m places. Let $f_2(x, y)$ be a function generated by $f(x, y)$ such that $D(f_2)$ is least. By the supposition, there are numbers u and v such that $f_2(u, v) \neq f_1(u, v)$. Denote $f_1(u, v) = p$ and $f_2(u, v) = q$. We need the following two lemmas.

LEMMA 5.2. *$f(x, y)$ generates a function $c(x, y)$ which has the following properties: $c(q, y) = y$ for any y, and $c(p, q) = p$.*

Proof. We define the following 1-place functions:

$a_1(x)$: any permutation such that $a_1(q) = i$ and $a_1(q +' 1) = j$.
$a_2(x)$: any permutation such that $a_2(q) = k$ and $a_2(q +' 1) = l$.
$a_3(x)$: any permutation such that $a_3(f(i, k)) = q$, $a_3(f(i, l)) = q +' 1$ and $a_3(f(j, k)) = q +' 2$.
$a_4(x)$: $a_4(x) = q +' 1$ for $x \neq q$, $a_4(q) = q$.

Permutations $a_1(x)$, $a_2(x)$ and $a_3(x)$ certainly exist, because of the definition of i, j, k and l. Since $f(x, y)$ generates these functions, it generates also the following

$$b(x, y) = a_3(f(a_1(x), a_2(y))).$$

Obviously, $b(q, q) = q$, $b(q, q +' 1) = q +' 1$ and $b(q +' 1, q) = q +' 2$.

Every number $1, 2, \dots, n$ occurs in the value sequence of $b(x, y)$. This is seen from the definition of $b(x, y)$ and from the fact that every number $1, 2, \dots, n$ occurs in the value sequence of $f(x, y)$. Thus, for any t $(1 \leqq t \leqq n)$, there are numbers α_t and β_t such that

$$b(\alpha_t, \beta_t) = t.$$

We proceed inductively, denoting by $c_m(x, y)$ a function which has the following properties: $c_m(q, q +' y) = c_m(q +' y, q) = q +' y$, for any y where $0 \leqq y < m$. If we can show that $f(x, y)$ generates such functions $c_m(x, y)$, then clearly taking $c(x, y) = c_n(x, y)$ will satisfy our lemma. We define $c_2(x, y)$ in terms of $f(x, y)$ as follows:

$$c_2(x, y) = a_4(b(x, y)).$$

In order to prove lemma 5.2, we have to show that if $f(x, y)$ generates a function $c_m(x, y)$, where $2 \leqq m < n$, then it generates also a function $c_{m+1}(x, y)$.

Suppose $f(x, y)$ generates a function $c_m(x, y)$ where $2 \leqq m < n$. Define the following 1-place functions:

$e_1(x)$: $e_1(q) = q$, $e_1(x) = x -' 1$ for $x \neq q$.
$e_2(x)$: $e_2(q) = q$, $e_2(q +' 1) = q +' 1$, $e_2(q +' 2) = q$, $e_2(x) = x -' 1$ for $x \neq q, q + 1, q +' 2$.

$e_3(x)$: $e_3(q) = q$, $e_3(q +' 1) = q +' 1$, $e_3(x) = \alpha_{x+'1}$ for $x \neq q, q +' 1$.
$e_4(x)$: $e_4(q) = q$, $e_4(q +' 1) = q +' 1$, $e_4(x) = \beta_{x+'1}$ for $x \neq q, q +' 1$.

Thus, $f(x, y)$ generates the following two functions:

$$e_5(x, y) = e_3(c_m(e_1(x), e_1(y)))$$

and

$$e_6(x, y) = e_4(c_m(e_2(x), e_2(y))).$$

As the reader may easily verify, a function $c_{m+1}(x, y)$ can now be defined in terms of $f(x, y)$ as follows:

$$c_{m+1}(x, y) = b(e_5(x, y), e_6(x, y)).$$

This proves lemma 5.2.

LEMMA 5.3. *$f(x, y)$ generates the function $r(x, y)$ defined as follows: $r(u, v) = p$, and $r(x, y) = q$ whenever $(x, y) \neq (u, v)$.*

Proof. Define the following 1-place functions:

$g_1(x)$: $g_1(q) = q +' 1$, $g_1(x) = q$ for $x \neq q$.
$g_2(x)$: $g_2(q +' 2) = q$, $g_2(x) = q +' 1$ for $x \neq q +' 2$.

Consider the function $b(x, y)$ in the proof of lemma 5.2. $f(x, y)$ generates a function $b'(x, y)$ defined as follows:

(i) If $b(q +' 1, q +' 1) = q$ then $b'(x, y) = g_2(b(g_1(x), y))$.
(ii) If $b(q +' 1, q +' 1) \neq q$ then $b'(x, y) = a_4(b(x, y))$ where a_4 is as in the proof of lemma 5.2.

Obviously, $b'(x, y)$ has the following properties: $b'(q, q) = q$, $b'(q, q +' 1) = b'(q +' 1, q) = b'(q +' 1, q +' 1) = q +' 1$.

Define, in addition, the following 1-place functions:

$g_3(x)$: $g_3(u) = q$, $g_3(x) = q +' 1$ for $x \neq u$.
$g_4(x)$: $g_4(v) = q$, $g_4(x) = q +' 1$ for $x \neq v$.
$g_5(x)$: any function such that $g_5(q) = p$ and $g_5(q +' 1) = q$.

The function $r(x, y)$ is now defined in terms of $f(x, y)$ as follows:

$$r(x, y) = g_5(b'(g_3(x), g_4(y))).$$

This completes the proof of lemma 5.3.

We now return to the proof of theorem 5.1. By lemmas 5.2 and 5.3, $f(x, y)$ generates the following function:

$$f'_2(x, y) = c(r(x, y), f_2(x, y)).$$

We see that $f'_2(x, y) = f_2(x, y)$ except when both $x = u$ and $y = v$. In this case we get

$$f_2'(u,v) = p = f_1(u,v).$$

Therefore, $D(f_2') < D(f_2)$. But this contradicts the definition of $f_2(x,y)$. Hence, $f(x,y)$ generates all 2-place functions. By theorem 2.1, $f(x,y)$ is a Sheffer function. The proof of theorem 5.1 has been completed.

Because of theorem 4.1, $f(x,y)$ is a Sheffer function if it generates three 1-place functions, two of which form a basis of the symmetric group S_n and the third of which assumes exactly n—1 values.

Theorem 5.1 can be generalized to the case where the hypothesis is that an m-place function $f(x_1, \dots, x_m)$ generates all 1-place functions. This will be shown in the following

THEOREM 5.4. *A function $f(x_1, \dots, x_m)$ which generates all* 1-*place functions is a Sheffer function.*

Proof. We prove first that $f(x_1, \dots, x_m)$ generates a 2-place function $g(x,y)$ satisfying the following two conditions:

(a) $g(x,y)$ is non-degenerately binary.

(b) $g(x,y)$ assumes all of the numbers $1, 2, \dots, n$ as values.

Obviously, $m \geqq 2$. We use the following notations: $I(x)$ is the identity permutation and $g_j(x)$ is the function assuming always the value j, for $j = 1, 2, \dots, n$.

According to the hypothesis, $I(x)$ is generated by f. Consider a composition sequence of $I(x)$

$$I(x) = f(f_1, \dots, f_m)$$

where each f_ν is the variable x or a function generated by f. Let the variable x occur in this composition sequence k times. Clearly, $k \geqq m$. We replace the ν^{th} occurrence of x by x_ν, for $\nu = 1, 2, \dots, k$. We, thus, obtain a function

$$h(x_1, \dots, x_k)$$

generated by f. Obviously,

$$(1) \qquad h(j, \dots, j) = j,$$

for any j. Furthermore, h depends on at least two of its variables. For suppose h would depend on its ν^{th} variable x_ν only. Let the ν^{th} occurrence of x in the composition sequence of $I(x)$ be in f_μ. Then f would depend on its μ^{th} variable only. This follows because an arbitrary combination of values can be obtained for $f_1, \dots, f_m$ after the x's have been replaced by the x_ν's. This is due to the fact that f assumes all of the numbers $1, 2, \dots, n$ as values. But obviously f depends on at least two of its variables. This is a contradiction, and we conclude that h depends on at least two of its variables.

We are going to show that a function $g(x, y)$ satisfying conditions (a) and (b) is generated by h and the functions $g_j(x)$. Since h and the functions $g_j(x)$ are generated by f, this implies that $g(x, y)$ is generated by f. We need the following

LEMMA 5.5. *Let $\varphi(x_1, \ldots, x_i)$ be a function satisfying the following two conditions:*

(A) $\varphi(j, \ldots, j) = j$, *for any* j.

(B) φ *and the functions* $g_j(x)$ *do not generate any function* $g(x, y)$ *satisfying conditions* (a) *and* (b).

Then, for some ν *where* $1 \leqq \nu \leqq i$,

(C) $\varphi(x_1, \ldots, x_i) = x_\nu$.

Proof. We apply induction on i. For $i = 1$, the assertion follows from the hypothesis (A). The lemma holds true also for $i = 2$. In this case, the function $\varphi(x_1, x_2)$ itself satisfies the condition (b). This implies that φ does not satisfy (a) because, otherwise, it would not satisfy (B). But this means that (C) is satisfied.

We make the following hypothesis of induction: the lemma is true for some fixed value i, $i \geqq 2$. Let

$$\varphi(x_1, x_2, \ldots, x_i, x_{i+1})$$

be an arbitrary function satisfying conditions (A) and (B). To prove the lemma, it suffices to show that φ satisfies the corresponding condition (C).

Consider the function

$$\varphi_1(x_1, x_2, \ldots, x_i) = \varphi(x_1, x_2, \ldots, x_{i-1}, x_i, x_i),$$

i.e. the function obtained from φ by identifying the two last variables. Obviously, φ_1 satisfies conditions (A) and (B) because φ satisfies these conditions. Hence, our hypothesis of induction implies

$$(2) \qquad \varphi_1(x_1, x_2, \ldots, x_i) = \varphi(x_1, x_2, \ldots, x_{i-1}, x_i, x_i) = x_\nu,$$

for some ν with $1 \leqq \nu \leqq i$. We separate two cases.

Case 1. $\nu \neq i$. Consider functions

$$\varphi_{2,u}(x_1, x_2, \ldots, x_i) = \varphi(x_1, x_2, \ldots, x_i, g_u(x_1)), \; u = 1, 2, \ldots, n,$$

i.e. functions obtained from φ by replacing the last variable, in succession, by each of the functions $g_u(x_1)$. In addition, consider functions

$$\begin{aligned}\varphi_{3,u}(x_1, x_i) &= \varphi_{2,u}(x_1, x_1, \ldots, x_1, x_i) \\ &= \varphi(x_1, x_1, \ldots, x_1, x_i, g_u(x_1)), \; u = 1, 2, \ldots, n,\end{aligned}$$

i.e. functions obtained from the functions $\varphi_{2,u}$ by identifying i—1 first variables.

According to (2), each of the functions $\varphi_{3,u}$ satisfies the condition

$$\varphi_{3,u}(x_1, u) = x_1.$$

Thus, each $\varphi_{3,u}$ satisfies condition (b). This implies that no one of the functions $\varphi_{3,u}$ satisfies condition (a) since, otherwise, φ would not satisfy condition (B). Hence, we infer that always

$$\varphi_{3,u}(x_1, x_i) = x_1.$$

Consequently, each of the functions $\varphi_{2,u}$ satisfies condition (A). Since φ satisfies (B) so does each $\varphi_{2,u}$.

Using our hypothesis of induction, we obtain, for each $\varphi_{2,u}$,

$$\varphi_{2,u}(x_1, x_2, \ldots, x_i) = x_{\mu(u)}$$

where $\mu(u)$ indicates that different x_μ's may be obtained for different values of u. However,

$$\varphi_{2,u}(x_1, x_2, \ldots, x_{i-1}, u) = x_\nu.$$

This implies that always

$$\varphi_{2,u}(x_1, x_2, \ldots, x_{i-1}, x_i) = x_\nu.$$

According to the definition of the functions $\varphi_{2,u}$, this means that

$$\varphi(x_1, x_2, \ldots, x_i, x_{i+1}) = x_\nu,$$

i.e. (C) is satisfied.

Case 2. $\nu = i$. In this case,

$$(3) \qquad \varphi_1(x_1, x_2, \ldots, x_i) = \varphi(x_1, x_2, \ldots, x_{i-1}, x_i, x_i) = x_i.$$

Consider the function

$$\varphi_4(x_1, x_2, \ldots, x_i) = \varphi(x_1, x_2, \ldots, x_i, x_1),$$

i.e. the function obtained from φ by identifying the first and the last variable. As before, it is shown that

$$\varphi_4(x_1, x_2, \ldots, x_i) = x_\mu,$$

and, furthermore, that (C) is satisfied if $\mu \neq 1$. Therefore, it suffices to consider the case $\mu = 1$, i.e.

$$(4) \qquad \varphi_4(x_1, x_2, \ldots, x_i) = \varphi(x_1, x_2, \ldots, x_i, x_1) = x_1.$$

Consider functions

$$\varphi_{5,u}(x_2, x_3, \ldots, x_i, x_{i+1}) = \varphi(g_u(x_2), x_2, \ldots, x_i, x_{i+1}), \; u = 1, 2, \ldots, n.$$

By (3), each of the functions $\varphi_{5,u}$ satisfies condition (A). Since they obviously satisfy also condition (B), we may use our hypothesis of induction. We obtain first

$$\varphi_{5,u}(x_2, x_3, \ldots, x_i, x_{i+1}) = x_{\mu(u)}.$$

However, (4) implies that always

$$\varphi_{5,u}(x_2, x_3, \ldots, x_i, u) = u.$$

Hence,

$$\varphi_{5,u}(x_2, x_3, \ldots, x_i, x_{i+1}) = x_{i+1}.$$

But this means that

$$\varphi(x_1, x_2, \ldots, x_i, x_{i+1}) = x_{i+1}.$$

This proves lemma 5.5.

We now return to the proof of theorem 5.4. Suppose no function $g(x, y)$ satisfying conditions (a) and (b) is generated by h and the functions $g_j(x)$. By equation (1) and lemma 5.5, this implies that

$$h(x_1, \ldots, x_k) = x_\mu,$$

for some μ where $1 \leqq \mu \leqq k$. But this is a contradiction, since we have shown that h depends on at least two of its variables. Consequently, h and the functions $g_j(x)$ generate a function $g(x, y)$ satisfying conditions (a) and (b). Therefore, f generates a function $g(x, y)$ satisfying conditions (a) and (b).

Suppose now $n \geqq 3$. Using the method presented in the proof of theorem 5.1, we can show that all 2-place functions are generated by $g(x, y)$ and all 1-place functions. Hence, all 2-place functions are generated by f. By theorem 2.1, f is a Sheffer function. This proves theorem 5.4 for $n \geqq 3$.

Suppose $n = 2$. Since $f(x_1, \ldots, x_m)$ generates all 1-place functions, $f(1, \ldots, 1) = 2$ and $f(2, \ldots, 2) = 1$. We are going to show that f generates one of the following two functions:

$$\text{(5)} \qquad \begin{array}{|cc} \hline 2 & 2 \\ 2 & 1 \end{array}\ , \quad \begin{array}{|cc} \hline 2 & 1 \\ 1 & 1 \end{array}\ .$$

Since both of these functions are Sheffer functions, this implies that f is a Sheffer function.

Assume neither one of the functions (5) is generated by f. Let P be the transposition (12). Then we claim that

$$\text{(6)} \qquad f(x_1, \ldots, x_m) = P(f(P(x_1), \ldots, P(x_m))).$$

Suppose this equation does not hold, for some assignment of values $u_1, \ldots, u_m$ for the variables $x_1, \ldots, x_m$. Hence,

$$f(u_1, \ldots, u_m) = f(P(u_1), \ldots, P(u_m)).$$

Let $u_{s_1} = \ldots = u_{s_r} = 1$ and $u_{s_{r+1}} = \ldots = u_{s_m} = 2$. Clearly, $1 \leqq r < m$. We identify the variables of f in the following way: $x_{s_1} = \ldots = x_{s_r} = x$ and $x_{s_{r+1}} = \ldots = x_{s_m} = y$. In this manner, we obtain a function $\overline{f}(x, y)$ generated by f. But clearly, $\overline{f}(x, y)$ is one of the functions (5). This is a contradiction, and we conclude that (6) holds true.

Formula (6) implies that f does not generate the function $g_1(x)$ assuming always the value 1, which is contrary to the hypothesis. For let

$$g_1(x) = f(f_1, \ldots, f_m)$$

be a composition sequence of $g_1(x)$. By repeated application of (6), we obtain

$$g_1(x) = P(f(f_1^{\prime}, \ldots, f_m^{\prime}))$$

where each $f_\nu^{\prime}$ is obtained from f_ν by replacing x by $P(x)$. But this is impossible, since $g_1(P(x)) = g_1(x)$. This proves theorem 5.4 for $n = 2$. Hence, we have completed the proof in all cases.

Theorems 2.1 and 5.4 imply the following general

THEOREM 5.6. *An i-place function which generates all j-place functions is a Sheffer function.*

It is clear that the hypothesis of theorem 5.6 is never satisfied for $i = 1$. In sections 6 and 7, we are going to present some 2-place functions which generate all 1-place functions and, hence, are Sheffer functions.

Theorem 5.4 suggests the following improvement of the criterion resulting from theorem 3.1. Choose $h = 1$ and find the number r $(r \leqq n^n)$. The function $f(x_1, \ldots, x_m)$ is a Sheffer function if and only if all n^n 1-place functions belong to $F^{(r-1)}$.

This method is also of practical value, at least if n is small. We illustrate it by the following example. Consider the case $n = 4$, and let a 2-place function $f(x, y)$ be defined by the following matrix (cf. the convention made in section 1):

$$\begin{array}{|cccc}
\hline
2 & 3 & 2 & 4 \\
1 & 3 & 2 & 2 \\
4 & 2 & 4 & 4 \\
1 & 4 & 3 & 1
\end{array}\ .$$

Then the value sequences in the sets $F_\nu^{(i)}$ will be as follows (we write every sequence only once).

$F_v^{(0)}$: 1234;

$F_v^{(1)}$: 2341;

$F_v^{(2)}$: 3412, 3241;

$F_v^{(3)}$: 4123, 4312, 4441, 4213, 2413, 2212, 2244, 4422, 4334;

$F_v^{(4)}$: 4212, . .

We need not go further. The value sequences 2341 and 3241 represent permutations which form a basis of S_4. The value sequence 4212 represents a function which assumes exactly 3 ($= n-1$) values. Hence, $f(x, y)$ is a Sheffer function.

6. Some particular Sheffer functions. We now apply theorem 5.1 to show that certain functions are Sheffer functions. These functions are of interest also from the point of view of the many-valued propositional calculus. Some results in this direction will be published in another paper.

Consider the function $\delta(x, y)$ defined as follows:

$$\delta(x, y) = n \text{ for } x \leqq n-1, \; \delta(n, y) = y +' 1.$$

THEOREM 6.1. *$\delta(x, y)$ is a Sheffer function.*

Proof. The proof is based on the following

LEMMA 6.2. *$\delta(x, y)$ generates the functions $b_i(x)$, $i = 1, 2, \ldots, n$, satisfying $b_i(x) = 1$ for $x \leqq n-i$ and $b_i(x) = n$ for $x > n-i$.*

Proof. We see that

$$b_1(x) = \delta(\delta(x, x), \delta(x, x)).$$

The following auxiliary functions are generated by $\delta(x, y)$:

$$d_i(x) = \delta(c_i(x), c_i(x)) \qquad \text{for } 1 \leqq i \leqq n-1$$

where

$$c_1(x) = \delta(\delta(x, x), x),$$
$$c_{j+1}(x) = \delta(d_j(x), c_j(x)) \qquad \text{for } 1 \leqq j < n-1.$$

We see that always

$$b_{j+1}(x) = \delta(d_j(x), d_j(x)) \qquad \text{for } 1 \leqq j \leqq n-1.$$

Therefore, lemma 6.2 follows.

It is now seen by an inductive argument that $\delta(x, y)$ generates all 1-place functions. By lemma 6.2, $\delta(x, y)$ generates the function $b_n(x)$ which assumes the value n for all argument values. We make the following hypothesis of induction: $\delta(x, y)$ generates all 1-place functions which assume the value n for all argument values $\leqq n-i$ where $0 \leqq i < n$. (I.e. $\delta(x, y)$ generates an arbitrary 1-place function whose value sequence begins with $n-i$ n's.) Let $g(x)$ be an arbitrary function assuming the value n for all argument values $\leqq n-i-1$. Denote $g(n-i) = u$, and define a function $g_1(x)$ as follows:

$$g_1(x) = n \text{ for } x \leqq n-i,\ g_1(x) = g(x) - u \text{ for } x > n-i.$$

By the hypothesis of induction, $g_1(x)$ is generated by $\delta(x, y)$. Define now, in succession:

$$\varphi_1(x) = \delta(b_{i+1}(x), g_1(x)),$$
$$\varphi_{j+1}(x) = \delta(b_{i+1}(x), \varphi_j(x)) \text{ for } j = 1, \dots, u-1.$$

By lemma 6.2, the φ-functions are generated by $\delta(x, y)$. Clearly,

$$\varphi_u(x) = g(x).$$

We, thus, have the following result: $\delta(x, y)$ generates an arbitrary 1-place function assuming the value n for all argument values $\leqq n-i-1$. The induction has been completed, and we conclude that $\delta(x, y)$ generates all 1-place functions. By theorem 5.1, $\delta(x, y)$ is a Sheffer function.

For a generalization of theorem 6.1, consider functions $\delta'(x, y)$ such that in their matrices all rows, except the i^{th} row, consist of the same number a. By theorem 3.2, such a function is not a Sheffer function if $a \neq i$. Suppose $a = i$ and denote $\delta'(i, y) = \alpha(y)$. Then the matrix of $\delta'(x, y)$ is as follows:

$$\begin{array}{|cccc}
\hline
i & i & \dots & i \\
. & . & \dots & . \\
\alpha(1) & \alpha(2) & \dots & \alpha(n) \\
. & . & \dots & . \\
i & i & \dots & i
\end{array}$$

where the α's are in the i^{th} row. We have the following

THEOREM 6.3. *$\delta'(x, y)$ is a Sheffer function if and only if $\alpha(y)$ is a circular permutation of the numbers $1, 2, \dots, n$.*

Proof. The "if"-part of the theorem is shown to be true in the same way as theorem 6.1. For the "only if"-part, let $\alpha(y)$ first be a permutation which is not circular. Then there is a number k such that, in the cyclic representation of $\alpha(y)$, k does not occur in the same cycle as i. It is easy to see that the 1-place function which assumes always the value k cannot be generated by $\delta'(x, y)$.

Let $\alpha(y)$ be a 1-place function which is not a permutation. If $\alpha(y)$ assumes i as a value then one of the numbers $1, 2, \dots, n$ does not occur in the matrix of $\delta'(x, y)$. By theorem 3.2, $\delta'(x, y)$ is not a Sheffer function.

If $\alpha(y)$ does not assume i as a value then the 1-place function which assumes always the value i cannot be generated by $\delta'(x, y)$. This completes the proof.

When we let i range over the numbers $1, 2, \ldots, n$ and, for each i, let $\alpha(y)$ range over the $(n-1)!$ circular permutations we get $n!$ functions $\delta'(x, y)$, each of which is a Sheffer function by theorem 6.3. If we consider columns instead of rows then a similar argument gives another $n!$ Sheffer functions. The latter ones are all different from the former ones, provided $n > 2$.

In the following theorem we assume $n > 2$.

THEOREM 6.4. *Let $h(x, y)$ be the function defined as follows:*

$$h(1,1) = 2, \textit{ otherwise } h(x,y) = 1 \textit{ for } x \geqq y;$$
$$h(1,n) = n, \textit{ otherwise } h(x,y) = y - x + 2 \textit{ for } x < y.$$

Then $h(x, y)$ is a Sheffer function.

Proof. Denote

$$a_1(x) = h(h(x,x),x),$$
$$a_2(x) = h(h(x,x),h(x,x)),$$
$$a_3(x) = h(a_2(x),x),$$
$$a_4(x) = h(h(x,x),a_2(x))$$

and

$$a_5(x) = h(x, a_1(x)).$$

Clearly, $a_1(x)$ is a function assuming exactly $n-1$ values. $a_3(x)$ is the transposition (12). Furthermore, if $n = 3$ then $a_5(x)$ is the circular permutation (123). If $n > 3$ denote

$$b_1(x) = h(a_5(x), a_4(x)),$$
$$b_{i+1}(x) = h(a_5(x), b_i(x)) \text{ for } 1 \leqq i \leqq n-4.$$

Define, finally,

$$a_6(x) = h(b_{n-3}(x), x).$$

Then $a_6(x)$ is the circular permutation $(12 \ldots n)$. It forms together with the transposition (12) a basis of the symmetric group S_n. Hence, $h(x, y)$ generates a basis of S_n and a function assuming exactly $n-1$ values. By theorems 4.1 and 5.1, $h(x, y)$ is a Sheffer function.

7. Sets of Sheffer functions.

Theorems 4.1 and 5.1 give us a method for the direct construction of sets of Sheffer functions. For instance, we may define a function $f(x, y)$ in such a manner that $f(x, x)$ and $f(x, f(x,x))$ form a basis of the symmetric group S_n and $f(f(x, x), x)$ assumes exactly $n-1$ values. This is always possible when $n > 2$. Such a definition gives us at least n^{n^2-3n} Sheffer functions. We illustrate this method by the following example where we assume $n > 2$.

Let $f(x,y)$ be any function which satisfies the following conditions:

$$f(x,x) = x+'1 \text{ for any } x;$$
$$f(1,2) = 2,\ f(2,3) = 1,\ f(x,x+'1) = x \text{ for } x \neq 1, 2;$$
$$f(2,1) = 2,\ f(x+'1,x) = x \text{ for } x \neq 1.$$

Thus the matrix of $f(x,y)$ is, in case $n=3$,

$$\begin{array}{|ccc} \hline 2 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 2 & 1 \end{array}$$

and, in case $n>3$,

$$\begin{array}{|ccccc} \hline 2 & 2 & & & n \\ 2 & 3 & 1 & & \\ & 2 & \cdot & \cdot & \\ & & \cdot & n & n-1 \\ n & & & n-1 & 1 \end{array}$$

By theorems 4.1 and 5.1, such an $f(x,y)$ is always a Sheffer function, no matter how we choose numbers for the undefined entries. Since there are n^2-3n undefined entries, we get n^{n^2-3n} Sheffer functions.

In this section we prove three theorems, each of which gives us n^{n^2-2n} Sheffer functions. In theorems 7.1 and 7.4 we assume $n>2$, in theorem 7.2 we assume $n>3$.

THEOREM 7.1. *Any function $f(x,y)$ such that*

$$f(x,x) = x+'1 \textit{ for any } x$$

and

$$f(1,2) = 2,\ f(x,x+'1) = x \textit{ for } x \neq 1$$

is a Sheffer function.

Proof. It is seen that $f(x,x)$ is the circular permutation $(12\ldots n)$, whereas $f(x,f(x,x))$ is a function assuming exactly $n-1$ values. It suffices to show that $f(x,y)$ generates the $(n-1)$-cycle $(23\ldots n)$. The latter forms together with $(12\ldots n)$ a basis of the symmetric group S_n.

To show that the $(n-1)$-cycle $(23\ldots n)$ is generated, we proceed as follows. We define first the following auxiliary functions:

$$a_0(x) = x,$$
$$a_1(x) = f(x,f(x,x)),$$
$$a_i(x) = f(a_{i-1}(x), f(a_{i-2}(x), a_{i-2}(x))) \text{ for } 2 \leq i \leq n-2.$$

Clearly, $a_i(1) = i+1$ and $a_i(x) = x$ for $x \neq 1$. Let now

$$b_1(x) = f(f(a_{n-3}(x), a_{n-3}(x)), f(a_{n-3}(x), a_{n-3}(x)))$$

and

$$b_2(x) = f(a_{n-2}(x), a_{n-2}(x)).$$

Then $f(b_2(x), b_1(x))$ is the $(n-1)$-cycle $(23\ldots n)$. Hence theorem 7.1 follows.

THEOREM 7.2. *Let $f(x,y)$ be any function which has the following properties:*

$$f(x,x) = 1 \text{ for } x \neq 1,$$
$$f(1,2) = 3$$

and

$$f(2,1) = 4,\ f(3,1) = 2,\ f(x,1) = x+1 \text{ for } x \neq 2,3.$$

Then $f(x,y)$ is a Sheffer function.

Proof. Define

$$a_1(x) = f(x, f(x,x)),$$
$$a_2(x) = f(f(x,x), f(f(x,x), f(x,x))),$$
$$a_3(x) = f(a_2(x), a_2(x))$$

and

$$a_4(x) = f(x, a_3(x)).$$

Then $a_1(x)$ is the circular permutation $(1324\ldots n)$ and $a_4(x)$ is a function assuming exactly $n-1$ values. The proof is completed if we can show that $f(x,y)$ generates the transposition (23). This transposition together with the generated circular permutation forms a basis of the symmetric group S_n.

We use the term "the f-square of a function $g(x)$" to mean the function $f(g(x), g(x))$. By the notation $g^2(x)$ we mean the function $gg(x)$. Other powers of $g(x)$ are used analogously. We need the following

LEMMA 7.3. *$f(x,y)$ generates any 1-place function which assumes only the numbers 1 and 2 as values.*

Proof. The function $a_3(x)$ above assumes always the value 1. By f-squaring it, we obtain the function which assumes always the value 2. Furthermore, by f-squaring the functions $a_1^{\nu}(x)$ where $\nu = 1, 2, \ldots, n$, we obtain all (1-place) functions which assume the value 2 once and the value 1 $n-1$ times. By f-squaring all these functions, we obtain all functions which assume the value 1 once and the value 2 $n-1$ times.

We now make the following inductive hypothesis: $f(x,y)$ generates all functions which assume the value 2 i times and the value 1 $n-i$ times, where $1 \leqq i < n-1$. Let $h(x)$ be an arbitrary function which assumes the value 2 $i+1$ times and the value 1 $n-(i+1)$ times. Choose a number k such that $h(k) = 2$. Let $h_1(x)$ be the function defined as follows:

$$h_1(k) = 1,\ h_1(x) = h(x) \text{ for } x \neq k.$$

By the inductive hypothesis, $h_1(x)$ is generated by $f(x,y)$. Let $h_2(x)$ be the f-square of $h_1(x)$. $f(x,y)$ generates also the following function $h_3(x)$:

$$h_3(k) = 1,\ h_3(x) = 2 \text{ for } x \neq k.$$

Consider the function $f(h_2(x), h_3(x))$. Obviously, if we f-square this function twice we obtain the function $h(x)$. Since $h(x)$ was an arbitrary function assuming the value 2 $i+1$ times and the value 1 $n-(i+1)$ times, we conclude that $f(x,y)$ generates all functions of this kind. This completes the induction, and we obtain the lemma.

To show that $f(x,y)$ generates the transposition (23), we now proceed as follows. Consider the following two functions $b_1(x)$ and $b_2(x)$:

$$b_1(1) = b_1(2) = 2,\ b_1(x) = 1 \text{ for } x \neq 1, 2;$$

and

$$b_2(1) = b_2(4) = 2,\ b_2(3) = 1,\ b_2(x) = x-1 \text{ for } x \neq 1, 3, 4.$$

Clearly, the transposition (23) can be expressed as $f(b_2(x), b_1(x))$. According to lemma 7.3, $f(x,y)$ generates the function $b_1(x)$. To complete the proof, we have to show that $f(x,y)$ generates $b_2(x)$.

Suppose first that n is even. We use the following auxiliary functions:

$r_1(x)$: $r_1(1) = 2$, $r_1(2) = 1$; otherwise $r_1(x) = 1$ if x is odd and $r_1(x) = 2$ if x is even.

$r_{i+1}(x)$ for $1 \leqq i < n-3$: $r_{i+1}(x) = f(r_i(x), s_i(x))$

where $s_i(x)$ is defined as follows:

$$s_i(x) = r_i(x) \text{ for } x \leqq n-i,\ s_i(x) = 1 \text{ for } x > n-i.$$

By lemma 7.3, the function $r_1(x)$ as well as all of the functions $s_i(x)$ are generated by $f(x,y)$. Therefore, all of the functions $r_i(x)$ are generated by $f(x,y)$. But clearly,

$$b_2(x) = r_{n-3}(x).$$

This completes the proof in case n is even. In case n is odd the proof will remain exactly the same, except that instead of $r_1(x)$ we have to take the f-square of $r_1(x)$. Hence theorem 7.2 follows.

Theorem 7.4. *Any function $f(x,y)$ such that*

$$f(x,x) = x+1 \text{ for any } x$$

and

$$f(1,2) = 2,\ f(2,3) = 1,\ f(x, x+1) = x \text{ for } x \neq 1, 2$$

is a Sheffer function.

Proof. We see that $f(x,x)$ and $f(x,f(x,x))$ produce the circular permutation $(12\ldots n)$ and the transposition (12). These two permutations form a basis of the symmetric group S_n. Using this fact, we are going to show that $f(x,y)$ generates a (1-place) function assuming exactly $n-1$ values. We separate two cases.

Case 1. $f(2,1) \neq 3$. Let $p_1(x)$ be the transposition (12). Then $f(x,p_1(x))$ gives us a function which assumes exactly $n-1$ values.

Case 2. $f(2,1) = 3$. In this case, we have three subcases.

Subcase 2a. $f(1,3) = 1$ or $f(1,3) = 2$. Consider the $(n-1)$-cycle $p_2(x) = (n\; n-1 \ldots 431)$. (In case $n = 3$ we take $p_2(x)$ to be the transposition (31).) Then $f(p_2(x),x)$ defines a function assuming exactly $n-1$ values.

Subcase 2b. $f(1,3) = 3$. Let $p_3(x)$ be the $(n-1)$-cycle $(134\ldots n)$, i.e. p_3 is the inverse of p_2. Define

$$q_1(x) = f(x, p_3(x)).$$

Then $q_1(1) = q_1(2) = 3$ and $q_1(x) = x$ for $x \neq 1, 2$. Let $p_4(x)$ be the $(n-2)$-cycle $(n\; n-1 \ldots 43)$. Define

$$q_2(x) = f(p_4(x), p_2q_1(x)).$$

Then $q_2(1) = 2$, $q_2(2) = 3$, $q_2(3) = n$ and $q_2(x) = x$ for $x \neq 1, 2, 3$. Hence, $q_2(x)$ is a function assuming exactly $n-1$ values.

Subcase 2c. $f(1,3) = u \neq 1, 2, 3$. Define

$$q_3(x) = f(x, p_3(x)).$$

Then $q_3(1) = u$, $q_3(2) = 3$ and $q_3(x) = x$ for $x \neq 1, 2$. Let $p_5(x)$ be the permutation $(4u)$ and $p_6(x)$ the product $(13)(4u)$. Define

$$q_4(x) = p_6q_3p_5(x).$$

It is seen that $q_4(1) = 4$, $q_4(2) = q_4(3) = 1$ and $q_4(x) = x$ for $x \neq 1, 2, 3$. If we, finally, let $p_7(x)$ be the 3-cycle (143), it is easily verified that the function

$$q_5(x) = f(p_7(x), q_4(x))$$

assumes exactly $n-1$ values. This completes the proof of theorem 7.4.

Theorem 7.4 is a special case of the general theorem 11.1. It is to be noted that in the proofs of theorems 7.1 and 7.2 the generation of the three desired 1-place functions took place entirely "through" the given $2n$ entries of the matrix of the function considered. No assumptions at all were needed about other entries of the matrix. This was not the case with the proof of theorem 7.4 where we had to consider, in addition to the given $2n$ entries, also two other entries. In fact, if this had not been done we would not have obtained any 1-place functions other than permutations.

Each of the theorems proved in this section gives us a method of filling $2n$ of the n^2 entries of the matrix of a 2-place function in such a way as to always yield a Sheffer function, regardless of how the remaining n^2-2n entries are filled. Since in this manner a large variety of Sheffer functions is obtained, these theorems can be used to prove the non-existence of certain negative criteria for Sheffer functions. An example of this will be given in section 10.

8. Conjugate functions. Let P be an arbitrary permutation belonging to the symmetric group S_n. We apply P to the elements of our basic set $\{1, 2, \ldots, n\}$. Then a given function $f(x, y)$ is changed into another function which we denote by $f_P(x, y)$. In fact,

$$f_P(x, y) = P(f(P^{-1}(x), P^{-1}(y))) \tag{1}$$

where P^{-1} is the inverse of P. We say that $f_P(x, y)$ is *conjugate* to $f(x,y)$.[1] In particular, if

$$f_P(x, y) = f(x, y)$$

we say that $f(x, y)$ is *self-conjugate under* P. If P is different from the identity permutation we also say, shortly, that $f(x, y)$ is *self-conjugate.* It is easy to see that if q is the number of permutations under which $f(x, y)$ is self-conjugate then the number of distinct conjugates of $f(x, y)$ equals $\frac{n!}{q}$. We confine our attention to 2-place functions. However, the considerations presented in this section remain valid for functions of more than two variables.

The relation "conjugate to" is reflexive, symmetric and transitive. Thus we have a partition of all functions into equivalence classes. We are going to see that the property of being a Sheffer function is preserved in this partition and that any Sheffer function has the largest possible number of distinct conjugates. We need the following simple

LEMMA 8.1. *If g, f, r and s are functions satisfying*

$$g(x, y) = f(r(x, y), s(x, y)),$$

then

$$g_P(x, y) = f_P(r_P(x, y), s_P(x, y))$$

for any permutation P.

[1] Conjugate functions correspond to the well-known "dual" functions in the case $n = 2$. The more general notion introduced above is due to SWIFT, [16]. Swift's paper contains an error: It is claimed (p. 613) that a subgroup of the symmetric group which leaves a function invariant leaves also all conjugates of this function invariant. This is the case only when the subgroup in question is a normal divisor.

The proof of this lemma is obvious from equation (1). It might be added that it is not necessary that r and s actually depend on both variables, and either one of them may reduce to a single variable. It is easy to see that lemma 8.1 implies the following

THEOREM 8.2. *Let $f(x, y)$ be a function self-conjugate under a permutation P. Then every function generated by $f(x, y)$ is also self-conjugate under P.*

For any permutation P different from identity, there are functions which are not self-conjugate under P. Therefore, theorem 8.2 implies that no Sheffer function is self-conjugate. This means that every Sheffer function possesses $n!$ conjugates. On the other hand, all conjugates $f_P(x, y)$ of a Sheffer function $f(x, y)$ are Sheffer functions. Namely, given any $g(x, y)$, we first form a composition sequence of $g_{P^{-1}}(x, y)$ in terms of $f(x, y)$. From this we obtain, using lemma 8.1, a composition sequence of $g(x, y)$ in terms of $f_P(x, y)$. Thus we have proved the following

THEOREM 8.3. *The number of* (2-*place*) *Sheffer functions is divisible by $n!$.*

The determination of this number, for an arbitrary n, is a difficult task.[1] It seems to be closely linked with the unsolved problem of determining the number of all bases of the symmetric group S_n. Lower bounds for the number of all Sheffer functions can be obtained by using theorems presented in section 7 or, better, theorem 12.1.

The theory of conjugate functions can be used to obtain new Sheffer functions from known ones. As a matter of fact, the $n!$ Sheffer functions $\delta'(x, y)$ given in theorem 6.3 are exactly the conjugates of the function $\delta(x, y)$ in theorem 6.1. Similarly, new sets of Sheffer functions are obtained if conjugation is applied to the functions given in the theorems of section 7. The method can be used also to simplify some proofs in the literature.[2]

9. Transposes as conjugates.

By the *transpose* of a function $f(x, y)$ we mean the function $f_{tr}(x, y)$ such that

$$f_{tr}(i, j) = f(j, i) \quad \text{for any } i \text{ and } j.$$

I.e. the matrix of $f_{tr}(x, y)$ is the transpose of the matrix of $f(x, y)$.

There are functions $f(x, y)$ such that the transpose of f is different from all conjugates of f. For instance, any non-symmetric function $f(x, y)$ with $f(x, x) = x + 1$ for $x \neq n$, $f(n, n) = n$, has this property. On the other hand, it is easy to find functions $f(x, y)$ such that the transposes of these

[1] In the cases $n = 2$ and $n = 3$ the number is known to be 2 and 3774, respectively. The former result is to be found in [21], the latter in [6].

[2] For instance, it is easy to see that some of the Sheffer functions presented in [4] are conjugate to one another.

functions are also conjugates. In other words, for some permutation P, the equation

$$f_{tr}(x, y) = f_P(x, y)$$

is true. In this section we discuss the problem of whether it is possible to find such functions satisfying this condition which, in addition, are Sheffer functions.

If a Sheffer function $f(x, y)$ is symmetric, i.e. $f(x, y) = f_{tr}(x, y)$, then we obtain a trivial solution to this problem by choosing P to be the identity permutation. No other permutation could be used here since no Sheffer function is self-conjugate. Using theorems 7.1 and 7.4 it is easy to construct symmetric Sheffer functions.

To obtain a non-trivial solution, we have to consider non-symmetric Sheffer functions. The solution is presented in the following

Theorem 9.1. *For all values of $n \geqq 4$, there is a non-symmetric Sheffer function $f(x, y)$ whose transpose is one of its conjugates. If $n < 4$ there is no such Sheffer function.*

Proof. To prove the first part of the theorem, we assume $n \geqq 4$ and define a function $t(x, y)$ as follows:

$$t(2,1) = 4,\ t(3,1) = 2,\ t(x,1) = x +' 1 \text{ for } x \neq 2, 3;$$
$$t(1,3) = t(4,1),\ t(1,4) = 2,\ t(1,x) = x +' 1 \text{ for } x \neq 3, 4;$$
$$t(x,y) = 1 \text{ if } x \neq 1 \text{ and } y \neq 1.$$

$t(x, y)$ satisfies the hypothesis of theorem 7.2 and, hence, is a Sheffer function. Let P_1 be the transposition (34). Then it is readily seen that

$$t_{P_1}(x, y) = t_{tr}(x, y).$$

This proves the first part of the theorem.

The second part is clear in the case $n = 2$ since in this case there is no non-symmetric Sheffer function.

Assume, finally, $n = 3$. Let $f(x, y)$ be a non-symmetric Sheffer function and P a permutation such that

$$f_{tr}(x, y) = f_P(x, y).$$

P has to be different from the identity permutation because $f(x, y)$ is non-symmetric. The function $g(x) = f(x, x)$ is self-conjugate under P. Furthermore, $g(x) \neq x$ for any x, by theorem 3.2. These conditions can be satisfied only if the value sequence of $g(x)$ equals

$$231 \text{ or } 312$$

and P is one of the 3-cycles

$$(123) \text{ or } (132).$$

Suppose $P = (123)$. Then we get, using the formula (1) in section 8, the following equations:

$$\begin{aligned} f(2,1) &= P(f(3,1)), \\ f(3,1) &= P(f(3,2)), \\ f(3,2) &= P(f(1,2)), \\ f(1,2) &= P(f(1,3)), \\ f(1,3) &= P(f(2,3)), \\ f(2,3) &= P(f(2,1)). \end{aligned}$$

Since P^3 is the identity, these equations imply that $f(x, y)$ is symmetric, contrary to our assumption. The proof is similar in case $P = (132)$.

10. Non-existence of a sum criterion. In the case $n = 2$ it can be shown that if the sum

$$f(1,1)+f(1,2)+f(2,1)+f(2,2)$$

of all numbers in the matrix of a function $f(x, y)$ is even then $f(x, y)$ is not a Sheffer function. The result is established by showing the closure of the property in question under the forming of new functions as a finite composition of $f(x, y)$ (cf. [20]). This gives rise to a plausible conjecture for the general case: There is some property of the sum $V(f)$ of all numbers in the matrix of a 2-place function $f(x, y)$ which guarantees that $f(x, y)$ is a Sheffer function, or there is some property of $V(f)$ which guarantees that $f(x, y)$ is not a Sheffer function. However, the following considerations show that this is futile.

Obviously for any function $f(x, y)$,

$$n^2 \leqq V(f) \leqq n^3.$$

Consider any number b such that $n^2 \leqq b \leqq n^3$. There is a function $f(x, y)$ which is not a Sheffer function and for which $V(f) = b$. This is true because, given any b where $n^2 \leqq b \leqq n^3$, we can construct a function $f(x, y)$ such that either $f(1, 1) = 1$ or $f(n, n) = n$. And a function having either one of these properties is not a Sheffer function, by theorem 3.2. Therefore, there is no property of the sum $V(f)$ which would guarantee that $f(x, y)$ is a Sheffer function.

On the other hand, there is a trivial property of $V(f)$ which guarantees that $f(x, y)$ is not a Sheffer function, namely,

$$V(f) < n^2 + \tfrac{1}{2}(n-1)n \text{ or } V(f) > n^3 - \tfrac{1}{2}(n-1)n.$$

This is true because in these cases all of the numbers $1, 2, \ldots, n$ do not occur in the matrix of $f(x, y)$. However, except this trivial property there is no other property of $V(f)$ which would guarantee that $f(x, y)$ is not a Sheffer function, provided $n > 2$. This result is a consequence of the following

THEOREM 10.1. *Assume that $n > 2$ and a is any number such that*

$$n^2 + \tfrac{1}{2}(n-1)n \leqq a \leqq n^3 - \tfrac{1}{2}(n-1)n.$$

Then there is a Sheffer function $f(x, y)$ such that the sum $V(f)$ of all numbers in the matrix of $f(x, y)$ equals a.

Proof. The theorem is true in the case $n = 3$.[1] In the following proof we assume $n \geqq 4$.

Using theorem 7.2 we obtain Sheffer functions $f(x, y)$ satisfying the condition $V(f) = a$, provided

$$n^2 + \tfrac{1}{2}(n-1)n + 1 \leqq a \leqq (n^2 - 2n)n + \tfrac{1}{2}n(n+1) + n + 1.$$

Consider the set of Sheffer functions resulting as conjugate functions from the set presented in theorem 7.2 using the permutation

$$P = (1\,n)(2\,n-1).$$

Given any a with

$$(n^2 - 2n) + (n^2 - 1) + \tfrac{1}{2}n(n+1) \leqq a \leqq n^3 - \tfrac{1}{2}(n-1)n - 1,$$

we can choose a Sheffer function $f(x, y)$ with $V(f) = a$ from this set.

Clearly these two intervals overlap. Thus given any a with

$$n^2 + \tfrac{1}{2}(n-1)n < a < n^3 - \tfrac{1}{2}(n-1)n,$$

we obtain a Sheffer function $f(x, y)$ with $V(f) = a$.

In addition, we have to show that the theorem holds true also for the endpoints of this interval. The function $\delta(x, y)$ in theorem 6.1 is a Sheffer function for which

$$V(\delta) = n^3 - \tfrac{1}{2}(n-1)n.$$

Let P' be the transposition $(1n)$. Then the function $\delta_{P'}(x, y)$ is a Sheffer function with

$$V(\delta_{P'}) = n^2 + \tfrac{1}{2}(n-1)n.$$

This completes the proof.

[1] This is seen immediately by considering Sheffer functions presented in the literature for this special case (cf. [6] and [16]). A list of the required functions is, beginning with a function $f(x, y)$ for which $V(f) = 12$:

$$10_1,\ 1_2,\ 1_1,\ 3_2,\ 14_1,\ 2_2,\ 15_1,\ 6_2,\ 6_1,\ 5_2,\ 9_1,\ 1_5,\ 10_6$$

where we have made use of the notation in [16], p. 618.

This special case can also be taken care of by proving a theorem analogous to theorem 7.2 and then proceeding as in the proof above. For this, cf. the proof of theorem 12.1.

III. SHEFFER FUNCTIONS AS GENERATORS OF THE SYMMETRIC GROUP

11. Functions which generate all permutations. In theorem 5.1 it was shown that if a function $f(x, y)$ generates all 1-place functions then it is a Sheffer function. We are now going to take one step further. We consider functions $f(x, y)$ which generate all permutations of the numbers $1, 2, \ldots, n$, i.e. which generate the symmetric group S_n. Our aim is to prove that such a function is a Sheffer function. We have to assume $n > 2$. The symmetric group S_2 is cyclic and, hence, is generated by a 1-place function. And we know that a 1-place function can never be a Sheffer function.

THEOREM 11.1. *A function $f(x, y)$ which generates the symmetric group S_n is a Sheffer function, provided $n \geqq 3$.*[1]

Proof. Let $f(x, y)$ be an arbitrary but fixed function which generates all permutations of the numbers $1, 2, \ldots, n$. To prove theorem 11.1, we have to show that $f(x, y)$ generates a (1-place) function assuming exactly $n—1$ values. Then $f(x, y)$ is a Sheffer function, by theorems 5.1 and 4.1.

It is convenient for our purposes to introduce a classification of all 1-place functions. A function $g(x)$ is said to be of *genus* γ $(1 \leqq \gamma \leqq n)$ if it assumes exactly γ (distinct) values. A function $g(x)$ of genus γ is said to be of *type*

$$[a_1, a_2, \ldots, a_\gamma]$$

where the a's are natural numbers satisfying $a_1 + a_2 + \ldots + a_\gamma = n$ if, for each ν where $1 \leqq \nu \leqq \gamma$, there is a number b_ν such that $g(x)$ assumes b_ν as a value exactly a_ν times. This implies that all of the numbers b_ν are distinct. Obviously we do not change the type if we change the order of the numbers a_ν. The type of a function $g(x)$ tells us how many values $g(x)$ assumes and how many times it assumes each value. It does not tell us what these values are or in what order they are assumed.

[1] We remind the reader of the convention made in section 1, namely, that n is the number of elements in our basic set N. Theorem 11.1 is obviously false if the variables of $f(x, y)$ range over a set having more than n elements.

Our aim is to show that $f(x, y)$ generates a function of genus $n-1$. Clearly, every function of genus $n-1$ is of type

$$[2, \underbrace{1, \ldots, 1}_{n-2 \text{ terms}}].$$

We prove first several lemmas, beginning with

Lemma 11.2. *If $f(x, y)$ generates one function of a certain type then it generates every function of this type.*

Proof. Let $g(x)$ be a function generated by $f(x, y)$. A function $\overline{g}(x)$ which assumes exactly the values of $g(x)$ in an arbitrarily chosen order can be expressed as follows:

$$\overline{g}(x) = gs_\nu(x)$$

where $s_\nu(x)$ is a suitable permutation. On the other hand, for any function $\overline{\overline{g}}(x)$ which is of the same type as $g(x)$, we have

$$\overline{\overline{g}}(x) = s_\mu \overline{g}(x)$$

where $s_\mu(x)$ is a permutation and $\overline{g}(x)$ assumes exactly the values of $g(x)$ in some order. Hence,

$$\overline{\overline{g}}(x) = s_\mu g s_\nu(x)$$

where $s_\mu(x)$ and $s_\nu(x)$ are suitably chosen permutations. Since $f(x, y)$ generates all permutations, it generates $\overline{\overline{g}}(x)$ and we obtain lemma 11.2.

Lemma 11.3. *$f(x, y)$ generates a function of genus smaller than n. If $n \geqq 4$, $f(x, y)$ generates a function whose genus γ satisfies $1 < \gamma < n$.*

Proof. Since $f(x, y)$ generates the symmetric group S_n it has to depend on both of its variables, i.e. it has to be non-degenerately binary. This implies that there are four numbers u_1, u_2, u_3 and u_4 where $u_1 \neq u_3$ and $u_2 \neq u_4$ such that

$$f(u_1, u_2) = f(u_3, u_4).$$

Let now $s_1(x)$ be any permutation mapping 1 to u_1 and 2 to u_3. Let $s_2(x)$ be any permutation mapping 1 to u_2 and 2 to u_4. Such permutations certainly exist because $u_1 \neq u_3$ and $u_2 \neq u_4$. By the hypothesis, the function

$$f(s_1(x), s_2(x))$$

is generated by $f(x, y)$. This function is of genus smaller than n. This completes the proof of the first part of the lemma.

Assume that $n \geqq 4$. If $f(s_1(x), s_2(x))$ is of genus greater than 1, then the proof of our lemma has been completed. Assume it is of genus 1. Since all functions of genus 1 are of the same type, we conclude by lemma 11.2 that all functions of genus 1 are generated by $f(x, y)$.

In the same way as in the proof of theorem 5.1 we see that there are four numbers i, j, k and l such that $f(i, k) \neq f(j, k)$, $f(i, k) \neq f(i, l)$ and $f(j, k) \neq f(i, l)$. Obviously $f(x, y)$ satisfies the two requirements needed for this.

Suppose $f(i, x) \neq f(j, k)$, for any x. Let $g_i(x)$ be the function assuming always the value i. Then

$$f(g_i(x), x)$$

is a function generated by $f(x, y)$. Clearly, it is of a genus γ where $1 < \gamma < n$.

Suppose then that $f(i, x) = f(j, k)$, for some value of x, say $x = v_1$. Necessarily, $v_1 \neq k$ and $v_1 \neq l$. Choose from the set $\{1, 2, \ldots, n\}$ a number $v_2 \neq k, l, v_1$ and a number $v_3 \neq i, j$. This is possible because $n \geqq 4$. Let $s_3(x)$ be any permutation mapping 1 to v_3, 2 to j and 3 to i. Let $s_4(x)$ be any permutation mapping 1 to v_2, 2 to k and 3 to v_1 or to l, depending whether $f(v_3, v_2) \neq f(j, k)$ or $f(v_3, v_2) = f(j, k)$. Such permutations always exist. By the hypothesis, $f(x, y)$ generates the function

$$f(s_3(x), s_4(x)).$$

But the genus γ of this function satisfies the condition $1 < \gamma < n$. Therefore, we have proved lemma 11.3 in all cases.

LEMMA 11.4. *If $f(x, y)$ generates a function of type $[a_1, a_2, \ldots, a_t]$ where $1 < t < n$, then it generates a function of type $[a_1 + a_2, a_3, \ldots, a_t]$.*

Proof. Let $f(x, y)$ generate a function $h(x)$ of type $[a_1, a_2, \ldots, a_t]$ where $1 < t < n$. By lemma 11.2, $f(x, y)$ generates all functions of this type. The inequality $t < n$ implies that there are two distinct numbers p_1 and p_2 such that $h(p_1) = h(p_2)$. In addition, there are $t—2$ numbers p_3, $p_4, \ldots, p_t$ such that the following two conditions are satisfied:

(i) $p_\mu \neq p_\nu$ whenever $\mu \neq \nu$.
(ii) $h(p_\mu) \neq h(p_\nu)$ whenever $\mu \neq \nu$ and $\mu, \nu \geqq 2$.

We now define a function $\bar{h}(x)$ as follows: If $1 \leqq x \leqq a_1$ then $\bar{h}(x) = p_1$. If $a_1 + \ldots + a_\nu < x \leqq a_1 + \ldots + a_\nu + a_{\nu+1}$ where $1 \leqq \nu < t$ then $\bar{h}(x) = p_{\nu+1}$. Obviously, $\bar{h}(x)$ is of type $[a_1, a_2, \ldots, a_t]$ and, hence, $\bar{h}(x)$ is generated by $f(x, y)$. This implies that also the function $h\bar{h}(x)$ is generated by $f(x, y)$. Furthermore, $h\bar{h}(x)$ is of type

$$[a_1 + a_2, a_3, \ldots, a_t].$$

This proves the lemma.

By lemma 11.3 and, if necessary, repeated application of lemma 11.4 we obtain the following

LEMMA 11.5. *$f(x,y)$ generates a function of genus 2, provided $n \geqq 4$.*

We need two more lemmas in order to show that $f(x,y)$ generates a function of genus $n-1$.

LEMMA 11.6. *If $f(x,y)$ generates a function of type $[n-1, 1]$ then it generates a function of genus $n-1$.*

Proof. Let $f(x,y)$ generate a function of type $[n-1, 1]$. The proof of lemma 11.6 is by induction. We make the following inductive hypothesis: $f(x,y)$ generates a function of type

$$[n-m, \underbrace{1, \ldots, 1}_{m \text{ terms}}]$$

where $1 \leqq m < n-1$. We are going to show that this implies that a function of type

$$[n-m-1, \underbrace{1, \ldots, 1}_{m+1 \text{ terms}}]$$

is generated by $f(x,y)$. This proves lemma 11.6 because it shows that a function of type

$$[2, \underbrace{1, \ldots, 1}_{n-2 \text{ terms}}]$$

is generated by $f(x,y)$, i.e. a function of genus $n-1$ is generated by $f(x,y)$.

By the inductive hypothesis and lemma 11.2, all functions of type

$$[n-m, \underbrace{1, \ldots, 1}_{m \text{ terms}}]$$

are generated by $f(x,y)$. Furthermore, by repeated application of lemma 11.4 and by lemma 11.2 we see that $f(x,y)$ generates any (1-place) function which assumes some value at least $n-m$ times.

Let i, j, k and l be the same numbers as in the proof of lemma 11.3. Denote $f(i,k) = q_1$, $f(i,l) = q_2$ and $f(j,k) = q_3$. We know that these three numbers are all distinct. If $m > 1$, choose $m-1$ pairs (x_ν, y_ν) where $1 \leqq \nu \leqq m-1$ in such a manner that the following condition is satisfied: The numbers $q_1, q_2, \ldots, q_{m+2}$, where we denote $q_{\nu+3} = f(x_\nu, y_\nu)$, for $1 \leqq \nu \leqq m-1$, are all distinct. Such a choice is possible because $f(x,y)$ assumes all of the numbers $1, 2, \ldots, n$ as values and $m \leqq n-2$.

Define now two functions $h_1(x)$ and $h_2(x)$ as follows:

$h_1(x) = i$ for $1 \leqq x \leqq n-m-1$ and $x = n-m+1$,
$h_1(x) = j$ for $x = n-m$,
$h_1(x) = x_\nu$ for $x = n-m+1+\nu$ (where $1 \leqq \nu \leqq m-1$);

and

$$h_2(x) = k \text{ for } 1 \leqq x \leqq n-m,$$
$$h_2(x) = l \text{ for } x = n-m+1,$$
$$h_2(x) = y_\nu \text{ for } x = n-m+1+\nu \quad (\text{where } 1 \leqq \nu \leqq m-1).$$

$h_1(x)$ assumes the value i at least $n-m$ times and $h_2(x)$ assumes the value k at least $n-m$ times. Hence, they are both generated by $f(x,y)$. Consequently, the function

$$f(h_1(x), h_2(x))$$

is generated by $f(x,y)$. This function is of type

$$[n-m-1, \underbrace{1, \ldots, 1}_{m+1 \text{ terms}}].$$

This completes the inductive step, and we obtain lemma 11.6.

Lemma 11.7. *If $f(x,y)$ generates a function of type $[n-a, a]$ where $1 < a < n-1$ then it generates a function of type $[n-1, 1]$, provided that not both $n = 4$ and $a = 2$.*

Proof. We may assume $n \geqq 4$ because the lemma is vacuously true in the case $n = 3$. By the hypothesis and lemma 11.2, $f(x,y)$ generates all functions of type $[n-a, a]$ where $1 < a < n-1$. Let i, j, k, l, q_1, q_2 and q_3 be the same numbers as in the proof of the previous lemma.

Define two functions $e_1(x)$ and $e_2(x)$ as follows:

$$e_1(x) = i \text{ for } 1 \leqq x \leqq n-a,$$
$$e_1(x) = j \text{ for } n-a+1 \leqq x \leqq n;$$

and

$$e_2(x) = k \text{ for } 1 \leqq x \leqq n-a-1 \text{ and } x = n-a+1,$$
$$e_2(x) = l \text{ for } x = n-a \text{ and } n-a+1 < x \leqq n.$$

Both $e_1(x)$ and $e_2(x)$ are of type $[n-a, a]$ and, hence, are generated by $f(x,y)$. Consider the function

$$f(e_1(x), e_2(x)).$$

It is generated by $f(x,y)$. Its type depends on the value $f(j,l)$ in the following way:

(i) If $f(j,l) = q_1$ then the type is $[n-2, 1, 1]$.
(ii) If $f(j,l) = q_2$ or $f(j,l) = q_3$ then the type is $[n-a-1, a, 1]$.
(iii) If $f(j,l) \neq q_1, q_2, q_3$ then the type is $[n-a-1, a-1, 1, 1]$.

If we are dealing with the case (i) or the case (ii) then we may conclude, by lemma 11.4, that $f(x,y)$ generates a function of type $[n-1, 1]$. The same conclusion holds also in the case (iii), provided that not both

$n-a-1 = 1$ and $a-1 = 1$, i.e. provided that not both $n = 4$ and $a = 2$. Since we have excluded this case in the statement of lemma 11.7, we have completed the proof.

We are now in the position to establish our theorem 11.1, except for two special cases, namely, $n = 3$ and $n = 4$. Suppose $n \geqq 5$. Then, by lemma 11.5, $f(x, y)$ generates a function of genus 2, i.e. a function of type $[n-a, a]$ where $1 \leqq a \leqq n-1$. This implies, by lemma 11.7, that $f(x, y)$ generates a function of type $[n-1, 1]$. Hence, by lemma 11.6, $f(x, y)$ generates a function of genus $n-1$. This completes the proof of theorem 11.1, provided $n \geqq 5$.

The two gaps in the proof above, $n = 3$ and $n = 4$, remain to be filled.

Assume $n = 4$. By lemma 11.3, $f(x, y)$ generates a function of genus 2 or a function of genus 3. If it generates a function of genus 3 the proof has been completed. Every function of genus 2 is of type $[3, 1]$ or of type $[2, 2]$. If a function of type $[3, 1]$ is generated then we may use lemma 11.6 to obtain a function of genus 3.

Suppose $f(x, y)$ generates no function of genus 3 and no function of type $[3, 1]$. Hence, it generates a function of type $[2, 2]$. By lemmas 11.2 and 11.4, all functions of types $[2, 2]$ and $[4]$ are generated by $f(x, y)$.

Consider the main diagonal of the matrix of $f(x, y)$, i.e. the function $f(x, x)$. Obviously, $f(x, x) \neq x$, for any x. This implies, by our supposition, that $f(x, x)$ is a 4-cycle, a product of two transpositions or a function of type $[2,2]$. Furthermore, $f(x, x)$ is self-conjugate under one of the following permutations: $(12)(34)$, $(13)(24)$, $(14)(23)$. For if $f(x, x)$ is a 4-cycle, it is self-conjugate under the square of the same 4-cycle, this being one of the three permutations. If $f(x, x)$ is a product of two transpositions, it is self-conjugate under the same product. Finally, if $f(x, x)$ is of type $[2,2]$, there are two distinct numbers b_1 and b_2 such that $f(b_1, b_1) = b_2$ and $f(b_2, b_2) = b_1$. The transposition $(b_1 b_2)$ occurs in one of the three permutations considered and $f(x, x)$ is self-conjugate under this permutation.

Let $f(x, x)$ be self-conjugate under $P = (ab)(cd)$. Clearly, $P^{-1} = P$. We claim that also $f(x, y)$ is self-conjugate under P. If this were not the case, then there were numbers x_1 and y_1, $x_1 \neq y_1$, such that $f(x_1, y_1) \neq P(f(P(x_1), P(y_1)))$. Consider the functions $c_1(x)$ and $c_2(x)$ defined as follows:

$$c_1(1) = c_1(2) = x_1,\ c_1(3) = c_1(4) = P(x_1);$$

and

$$c_2(1) = x_1,\ c_2(2) = y_1,\ c_2(3) = P(x_1),\ c_2(4) = P(y_1).$$

$c_1(x)$ is of type $[2, 2]$. $c_2(x)$ is of type $[2, 2]$ or $[1, 1, 1, 1]$, depending whether $P(x_1) = y_1$ or $P(x_1) \neq y_1$. Hence, $f(x, y)$ generates both $c_1(x)$ and $c_2(x)$. This implies that $f(x, y)$ generates the function

$$c_3(x) = f(c_1(x), c_2(x)).$$

Because $f(x, x)$ is self-conjugate under P, $c_3(1) = P(c_3(3))$. Hence, by our supposition, also $c_3(2) = P(c_3(4))$. But because of the choice of x_1 and y_1, $c_3(2) \neq P(c_3(4))$.

This is a contradiction, and we conclude that $f(x, y)$ is self-conjugate under P. But this implies, by theorem 8.2, that $f(x, y)$ does not generate all permutations. Consequently, theorem 11.1 holds in the case $n = 4$.

Finally, assume $n = 3$. By lemma 11.3, $f(x, y)$ generates a function of a genus smaller than 3. If $f(x, y)$ generates a function of genus 2, then the proof has been completed.

Suppose $f(x, y)$ generates no function of genus 2. Hence, it generates a function of genus 1 (which is of type [3]). By lemma 11.2, all functions of genus 1 are generated by $f(x, y)$. This means that $f(x, y)$ has the following property Q: Whenever $f_1(x)$ and $f_2(x)$ are functions of types [1, 1, 1] or [3] then also $f(f_1(x), f_2(x))$ is a function of one of these types.

Consider the function $f(x, x)$. Property Q and the inequality $f(x, x) \neq x$ which is true for any x imply that $f(x, x)$ is a circular permutation, i.e. the value sequence of $f(x, x)$ is either 231 or 312. On the other hand, given the values of $f(x, x)$ and one additional value of $f(x, y)$, say $f(1, 2)$, the remaining values of $f(x, y)$ are determined by property Q. There are two possibilities for the value sequence of $f(x, x)$ and three possibilities for the value $f(1, 2)$. Hence, $f(x, y)$ is defined by one of the following six matrices:

$$\begin{array}{|ccc}\hline 2 & 1 & 3 \\ 1 & 3 & 2 \\ 3 & 2 & 1 \end{array}\,,\quad \begin{array}{|ccc}\hline 2 & 2 & 2 \\ 3 & 3 & 3 \\ 1 & 1 & 1 \end{array}\,,\quad \begin{array}{|ccc}\hline 2 & 3 & 1 \\ 2 & 3 & 1 \\ 2 & 3 & 1 \end{array}\,,\quad \begin{array}{|ccc}\hline 3 & 1 & 2 \\ 3 & 1 & 2 \\ 3 & 1 & 2 \end{array}\,,\quad \begin{array}{|ccc}\hline 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \end{array}\,,\quad \begin{array}{|ccc}\hline 3 & 3 & 3 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{array}\,.$$

But all of these six functions are self-conjugate under the permutation $P = (123)$. By theorem 8.2, no one of them generates all permutations. This contradicts our hypothesis about $f(x, y)$. The proof for the case $n = 3$ has been completed. Thus, we have established our theorem 11.1 in all cases.

12. Applications of theorem 11.1. Outlines for further work. An immediate consequence of theorem 11.1 (in case $n \geqq 3$) is the following criterion C: $f(x, y)$ is a Sheffer function if and only if it generates two permutations $s_1(x)$ and $s_2(x)$ which form a basis of the symmetric group S_n. For instance, we can choose $s_1(x)$ to be the n-cycle $(12 \ldots n)$ and $s_2(x)$ to be the transposition (12). This criterion gives an improvement of the method presented in section 5 of determining whether a given function $f(x, y)$ is a Sheffer function. Thus, in the example at the end of section 5, we need not form the sets $F_v^{(3)}$ and $F_v^{(4)}$ because we are able to see already from the sets $F_v^{(1)}$ and $F_v^{(2)}$ that the function in question is a Sheffer function.

The criterion C is *optimal* in the following sense. Let C_1 be a criterion of the form: $f(x, y)$ is a Sheffer function if and only if it generates every function belonging to the set S. We assume that the functions in S do not themselves generate all functions because, otherwise, C_1 is a trivial criterion. C_1 is said to be optimal if in it we cannot replace S by any proper subset of S. I.e. C_1 is optimal if, for every proper subset S_1 of S, there is a function $f(x, y)$ which is not a Sheffer function and which generates all functions in S_1. Our criterion C is clearly optimal, no matter what the number n of elements in our basic set N is, with the only restriction $n \geqq 3$. There are, namely, even 1-place functions which generate one of the functions $s_1(x)$ and $s_2(x)$. Theorem 11.1 shows that the criterion resulting from theorem 5.1 is not optimal.

By theorem 3.2, the main diagonal of the matrix of every Sheffer function $f(x, y)$ has the property:

$$f(x, x) \not\equiv x \quad \text{for any } x.$$

In what follows we construct Sheffer functions with an arbitrary preassigned main diagonal satisfying this condition. That is, given any function $g(x)$ such that $g(x) \not\equiv x$ for any x, we prove that there is a Sheffer function $f(x, y)$ with $f(x, x) = g(x)$. This is obviously true when $n = 2$. In the following theorem we assume $n \geqq 3$.

THEOREM 12.1. *Let $g(x)$ be a function such that $g(x) \not\equiv x$, for any x. Then there are at least n^{n^2-3n} Sheffer functions $f(x, y)$ with $f(x, x) = g(x)$. If, in addition, $g(x)$ is a permutation or a function of type $[n-1, 1]$ then there are at least n^{n^2-2n} Sheffer functions $f(x, y)$ with $f(x, x) = g(x)$.*

Proof. We use the following theorem of Piccard (cf. [9], pp. 80—86). For any permutation $s_1(x)$ different from the identity, there is a permutation $s_2(x)$ such that $s_1(x)$ and $s_2(x)$ form a basis of the symmetric group S_n, provided that not both $n = 4$ and $s_1(x)$ is one of the permutations $(12)(34)$, $(13)(24)$, $(14)(23)$.

Assume first $g(x)$ is a permutation. By the hypothesis, it is different from the identity permutation. Suppose it is also different from the three exceptional permutations listed above. Then, according to Piccard's theorem, there is a permutation $\bar{g}(x)$ such that $g(x)$ and $\bar{g}(x)$ generate the symmetric group S_n. Let now $f(x, y)$ be any function which satisfies the following conditions:

$$f(x, x) = g(x)$$

and

$$f(x, f(x, x)) = \bar{g}(x).$$

Since always $g(x) \neq x$, these two conditions are mutually consistent. There are n^{n^2-2n} functions $f(x, y)$ satisfying these two conditions. Each of them is a Sheffer function, by theorem 11.1.

Suppose $n = 4$ and $g(x)$ is one of the three exceptional permutations, say (12)(34). We may choose $\bar{g}(x)$ to be the function whose value sequence is 1341. The rest of the procedure above remains the same. The reader may easily verify that any function whose matrix is of the form

$$\begin{array}{|cccc} \hline 2 & 1 & & \\ 3 & 1 & & \\ & & 4 & 4 \\ & & 1 & 3 \end{array}$$

is a Sheffer function.

Assume next that $g(x)$ is a function of type $[n-1, 1]$. Then the required n^{n^2-2n} Sheffer functions $f(x, y)$ are obtained as conjugates of the functions given in theorem 7.2, provided $n \geqq 4$. If $n = 3$ we have to use a theorem analogous to theorem 7.2. (For instance, it is readily verified that any function whose matrix is of the form

$$\begin{array}{|ccc} \hline 2 & 2 & \\ 3 & 1 & \\ 1 & & 1 \end{array}$$

is a Sheffer function.)

Finally, assume that $g(x)$ is neither a permutation nor a function of type $[n-1, 1]$. Choose a permutation $s_1(x)$ such that, for any x, $s_1(x) \neq x$ and $s_1(x) \neq g(x)$. Such a permutation $s_1(x)$ exists, by our assumption concerning $g(x)$. Obviously $s_1(x)$ can also be chosen to be different from the three exceptional permutations above. According to Piccard's theorem, there is a permutation $s_2(x)$ which together with $s_1(x)$ forms a basis of the symmetric group S_n. Let now $f(x, y)$ be any function satisfying the following conditions:

$$f(x, x) = g(x),$$
$$f(x, f(x, x)) = s_1(x)$$

and

$$f(x, s_1(x)) = s_2(x).$$

By the hypothesis and the choice of $s_1(x)$, these three conditions are mutually consistent.There are n^{n^2-3n} functions $f(x, y)$ satisfying them. By theorem 11.1, each of these functions is a Sheffer function. This completes the proof.

It seems probable that theorem 12.1 can be strengthened to yield n^{n^2-2n} Sheffer functions $f(x, y)$ with $f(x, x) = g(x)$ also when $g(x)$ does not satisfy the additional condition required in theorem 12.1. In its present form, theorem 12.1 gives the following lower bound for the number of all Sheffer functions $f(x, y)$:

$$u_n \cdot n^{n^2-2n} + ((n-1)^n - u_n) \cdot n^{n^2-3n}$$

where

$$u_n = n(n-1) + \sum_{i=0}^{n} \binom{n}{i} (-1)^i (n-i)! \ .$$

Thus, in case $n = 4$ we obtain 1391616 Sheffer functions.

We present finally two conjectures which suggest improvements of theorem 11.1.

Conjecture 1. *A function $f(x, y)$ which generates the alternating group A_n is a Sheffer function, provided $n \geqq 4$.*

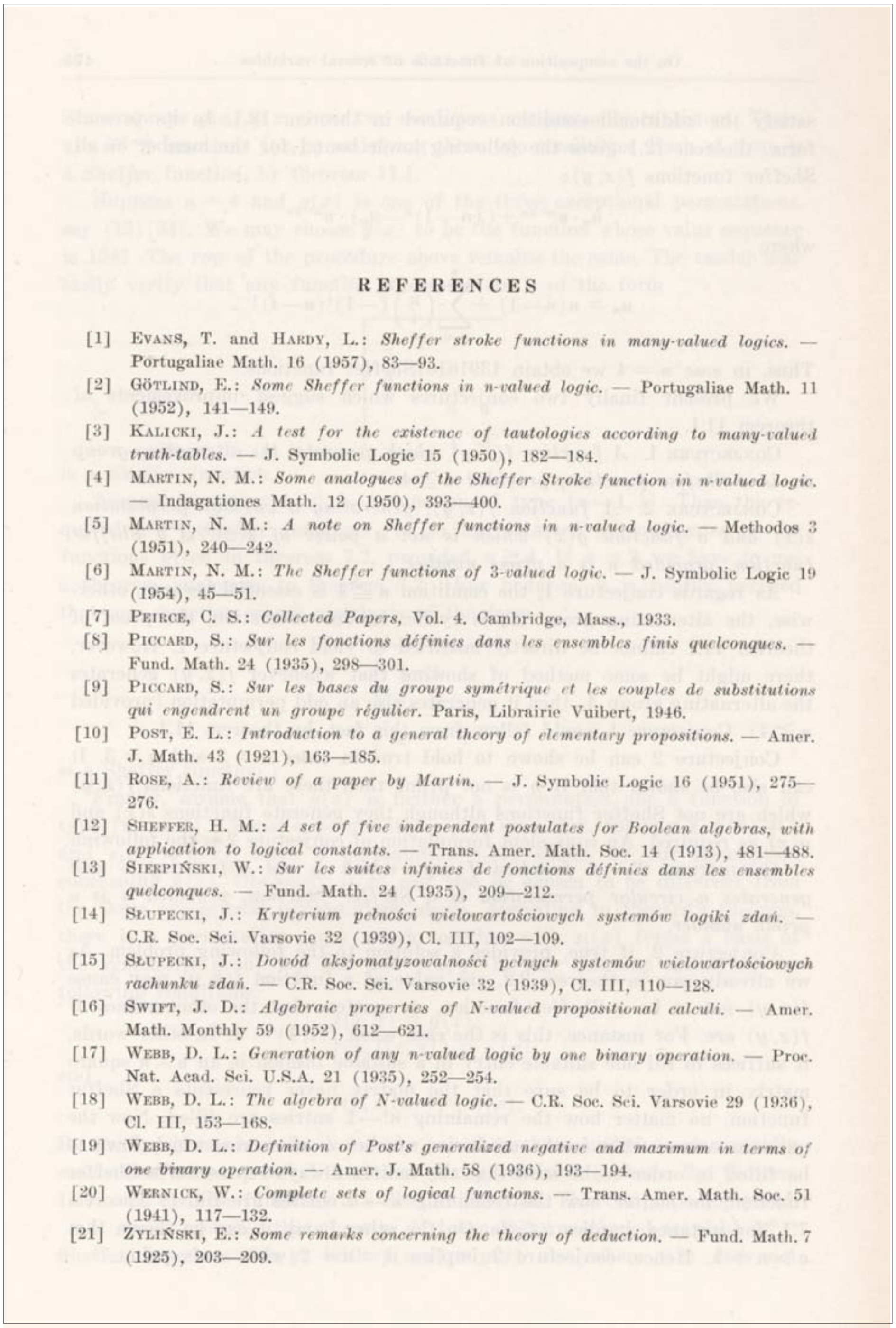
Conjecture 2. *A function $f(x, y)$, generating a circular permutation $s(x)$ and a function $g(x)$ which is not a power of $s(x)$, is a Sheffer function, provided n is a prime number.*

As regards conjecture 1, the condition $n \geqq 4$ is essential because, otherwise, the alternating group A_n is cyclic. In our estimation, the proof of theorem 11.1 cannot be directly modified to yield conjecture 1. However, there might be some method of showing that whenever $f(x, y)$ generates the alternating group A_n then it generates also an odd permutation (provided $n \geqq 4$). Conjecture 1 would follow from this fact, by theorem 11.1.

Conjecture 2 can be shown to hold true in cases $n = 2$ and $n = 3$. It can also be shown that if n is not prime then there are functions $f(x, y)$ which are not Sheffer functions although they generate functions $s(x)$ and $g(x)$ as required. An equivalent formulation of conjecture 2 is the following

Conjecture 2′. *A function $f(x, y)$ which is not self-conjugate and generates a circular permutation is a Sheffer function, provided n is a prime number.*

Conjecture 2, if true, provides a solution to the following problem. As we already saw in theorem 3.2, one value of a function $f(x, y)$ may cause $f(x, y)$ not to be a Sheffer function, no matter what the other values of $f(x, y)$ are. For instance, this is the case when $f(1, 1) = 1$. In other words, it suffices to fill one suitable entry in a suitable fashion in an $n \times n$ square matrix in order to be sure that the matrix never represents a Sheffer function, no matter how the remaining n^2-1 entries are filled. Now the question arises: what is the minimum number a of entries which have to be filled in order to be sure that the matrix always represents a Sheffer function, no matter how the remaining n^2-a entries are filled? Theorem 7.1, for instance, implies $a \leqq 2n$. On the other hand, it can be shown that $a > n + 1$. Hence, conjecture 2 implies $a = n + 2$ when n is prime.



REFERENCES

[1] Evans, T. and Hardy, L.: *Sheffer stroke functions in many-valued logics.* — Portugaliae Math. 16 (1957), 83—93.

[2] Götlind, E.: *Some Sheffer functions in n-valued logic.* — Portugaliae Math. 11 (1952), 141—149.

[3] Kalicki, J.: *A test for the existence of tautologies according to many-valued truth-tables.* — J. Symbolic Logic 15 (1950), 182—184.

[4] Martin, N. M.: *Some analogues of the Sheffer Stroke function in n-valued logic.* — Indagationes Math. 12 (1950), 393—400.

[5] Martin, N. M.: *A note on Sheffer functions in n-valued logic.* — Methodos 3 (1951), 240—242.

[6] Martin, N. M.: *The Sheffer functions of 3-valued logic.* — J. Symbolic Logic 19 (1954), 45—51.

[7] Peirce, C. S.: *Collected Papers,* Vol. 4. Cambridge, Mass., 1933.

[8] Piccard, S.: *Sur les fonctions définies dans les ensembles finis quelconques.* — Fund. Math. 24 (1935), 298—301.

[9] Piccard, S.: *Sur les bases du groupe symétrique et les couples de substitutions qui engendrent un groupe régulier.* Paris, Librairie Vuibert, 1946.

[10] Post, E. L.: *Introduction to a general theory of elementary propositions.* — Amer. J. Math. 43 (1921), 163—185.

[11] Rose, A.: *Review of a paper by Martin.* — J. Symbolic Logic 16 (1951), 275—276.

[12] Sheffer, H. M.: *A set of five independent postulates for Boolean algebras, with application to logical constants.* — Trans. Amer. Math. Soc. 14 (1913), 481—488.

[13] Sierpiński, W.: *Sur les suites infinies de fonctions définies dans les ensembles quelconques.* — Fund. Math. 24 (1935), 209—212.

[14] Słupecki, J.: *Kryterium pełności wielowartościowych systemów logiki zdań.* — C.R. Soc. Sci. Varsovie 32 (1939), Cl. III, 102—109.

[15] Słupecki, J.: *Dowód aksjomatyzowalności pełnych systemów wielowartościowych rachunku zdań.* — C.R. Soc. Sci. Varsovie 32 (1939), Cl. III, 110—128.

[16] Swift, J. D.: *Algebraic properties of N-valued propositional calculi.* — Amer. Math. Monthly 59 (1952), 612—621.

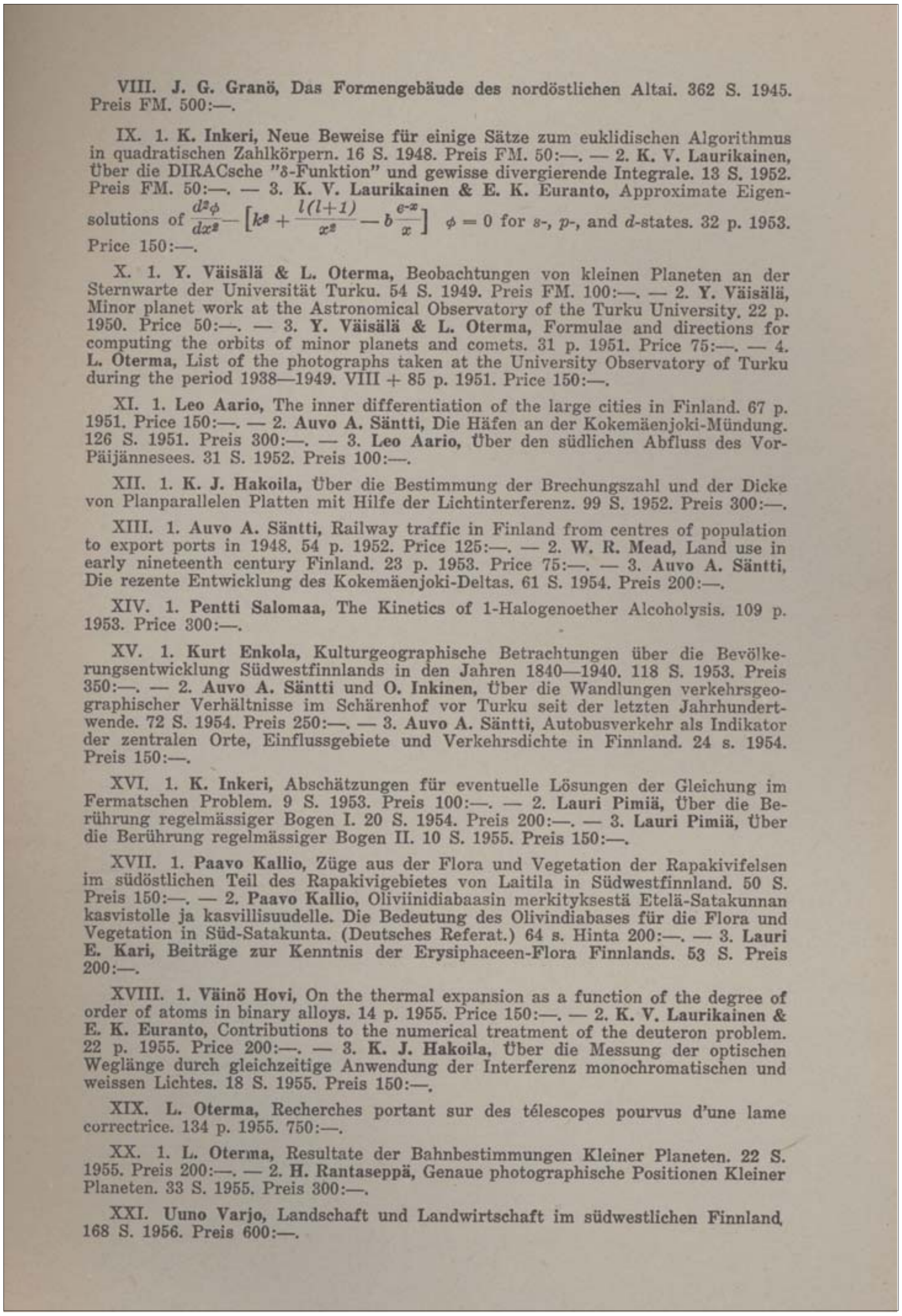
[17] Webb, D. L.: *Generation of any n-valued logic by one binary operation.* — Proc. Nat. Acad. Sci. U.S.A. 21 (1935), 252—254.

[18] Webb, D. L.: *The algebra of N-valued logic.* — C.R. Soc. Sci. Varsovie 29 (1936), Cl. III, 153—168.

[19] Webb, D. L.: *Definition of Post's generalized negative and maximum in terms of one binary operation.* — Amer. J. Math. 58 (1936), 193—194.

[20] Wernick, W.: *Complete sets of logical functions.* — Trans. Amer. Math. Soc. 51 (1941), 117—132.

[21] Zyliński, E.: *Some remarks concerning the theory of deduction.* — Fund. Math. 7 (1925), 203—209.



VIII. **J. G. Granö,** Das Formengebäude des nordöstlichen Altai. 362 S. 1945. Preis FM. 500:—.

IX. 1. **K. Inkeri,** Neue Beweise für einige Sätze zum euklidischen Algorithmus in quadratischen Zahlkörpern. 16 S. 1948. Preis FM. 50:—. — 2. **K. V. Laurikainen,** Über die DIRACsche "δ-Funktion" und gewisse divergierende Integrale. 13 S. 1952. Preis FM. 50:—. — 3. **K. V. Laurikainen & E. K. Euranto,** Approximate Eigensolutions of $\frac{d^2\phi}{dx^2} - \left[k^2 + \frac{l(l+1)}{x^2} - b\frac{e^{-x}}{x}\right] \phi = 0$ for *s*-, *p*-, and *d*-states. 32 p. 1953. Price 150:—.

X. 1. **Y. Väisälä & L. Oterma,** Beobachtungen von kleinen Planeten an der Sternwarte der Universität Turku. 54 S. 1949. Preis FM. 100:—. — 2. **Y. Väisälä,** Minor planet work at the Astronomical Observatory of the Turku University. 22 p. 1950. Price 50:—. — 3. **Y. Väisälä & L. Oterma,** Formulae and directions for computing the orbits of minor planets and comets. 31 p. 1951. Price 75:—. — 4. **L. Oterma,** List of the photographs taken at the University Observatory of Turku during the period 1938—1949. VIII + 85 p. 1951. Price 150:—.

XI. 1. **Leo Aario,** The inner differentiation of the large cities in Finland. 67 p. 1951. Price 150:—. — 2. **Auvo A. Säntti,** Die Häfen an der Kokemäenjoki-Mündung. 126 S. 1951. Preis 300:—. — 3. **Leo Aario,** Über den südlichen Abfluss des Vor-Päijännesees. 31 S. 1952. Preis 100:—.

XII. 1. **K. J. Hakoila,** Über die Bestimmung der Brechungszahl und der Dicke von Planparallelen Platten mit Hilfe der Lichtinterferenz. 99 S. 1952. Preis 300:—.

XIII. 1. **Auvo A. Säntti,** Railway traffic in Finland from centres of population to export ports in 1948. 54 p. 1952. Price 125:—. — 2. **W. R. Mead,** Land use in early nineteenth century Finland. 23 p. 1953. Price 75:—. — 3. **Auvo A. Säntti,** Die rezente Entwicklung des Kokemäenjoki-Deltas. 61 S. 1954. Preis 200:—.

XIV. 1. **Pentti Salomaa,** The Kinetics of 1-Halogenoether Alcoholysis. 109 p. 1953. Price 300:—.

XV. 1. **Kurt Enkola,** Kulturgeographische Betrachtungen über die Bevölkerungsentwicklung Südwestfinnlands in den Jahren 1840—1940. 118 S. 1953. Preis 350:—. — 2. **Auvo A. Säntti** und **O. Inkinen,** Über die Wandlungen verkehrsgeographischer Verhältnisse im Schärenhof vor Turku seit der letzten Jahrhundertwende. 72 S. 1954. Preis 250:—. — 3. **Auvo A. Säntti,** Autobusverkehr als Indikator der zentralen Orte, Einflussgebiete und Verkehrsdichte in Finnland. 24 s. 1954. Preis 150:—.

XVI. 1. **K. Inkeri,** Abschätzungen für eventuelle Lösungen der Gleichung im Fermatschen Problem. 9 S. 1953. Preis 100:—. — 2. **Lauri Pimiä,** Über die Berührung regelmässiger Bogen I. 20 S. 1954. Preis 200:—. — 3. **Lauri Pimiä,** Über die Berührung regelmässiger Bogen II. 10 S. 1955. Preis 150:—.

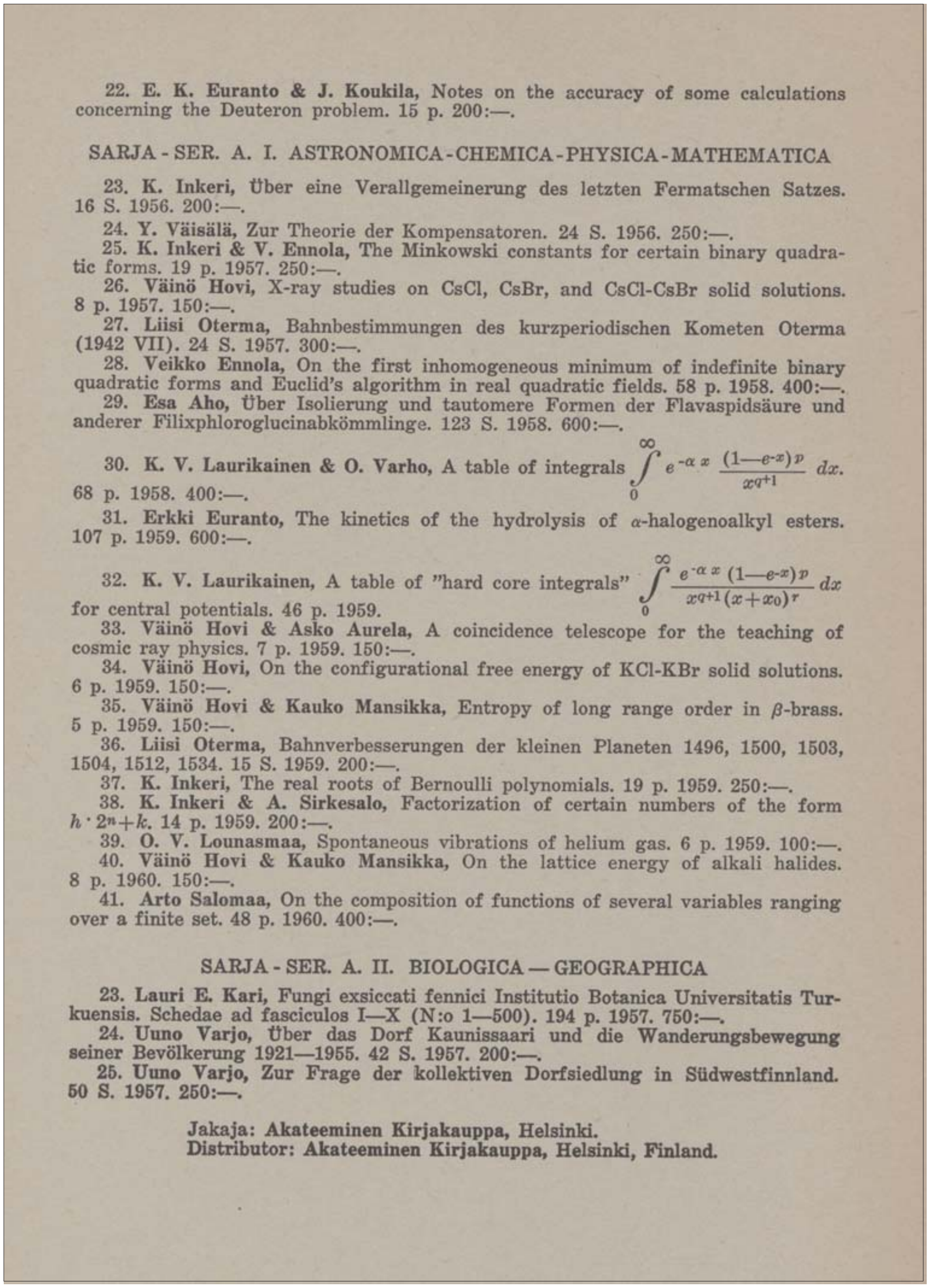
XVII. 1. **Paavo Kallio,** Züge aus der Flora und Vegetation der Rapakivifelsen im südöstlichen Teil des Rapakivigebietes von Laitila in Südwestfinnland. 50 S. Preis 150:—. — 2. **Paavo Kallio,** Oliviinidiabaasin merkityksestä Etelä-Satakunnan kasvistolle ja kasvillisuudelle. Die Bedeutung des Olivindiabases für die Flora und Vegetation in Süd-Satakunta. (Deutsches Referat.) 64 s. Hinta 200:—. — 3. **Lauri E. Kari,** Beiträge zur Kenntnis der Erysiphaceen-Flora Finnlands. 53 S. Preis 200:—.

XVIII. 1. **Väinö Hovi,** On the thermal expansion as a function of the degree of order of atoms in binary alloys. 14 p. 1955. Price 150:—. — 2. **K. V. Laurikainen & E. K. Euranto,** Contributions to the numerical treatment of the deuteron problem. 22 p. 1955. Price 200:—. — 3. **K. J. Hakoila,** Über die Messung der optischen Weglänge durch gleichzeitige Anwendung der Interferenz monochromatischen und weissen Lichtes. 18 S. 1955. Preis 150:—.

XIX. **L. Oterma,** Recherches portant sur des télescopes pourvus d'une lame correctrice. 134 p. 1955. 750:—.

XX. 1. **L. Oterma,** Resultate der Bahnbestimmungen Kleiner Planeten. 22 S. 1955. Preis 200:—. — 2. **H. Rantaseppä,** Genaue photographische Positionen Kleiner Planeten. 33 S. 1955. Preis 300:—.

XXI. **Uuno Varjo,** Landschaft und Landwirtschaft im südwestlichen Finnland, 168 S. 1956. Preis 600:—.



22. **E. K. Euranto & J. Koukila,** Notes on the accuracy of some calculations concerning the Deuteron problem. 15 p. 200:—.

SARJA - SER. A. I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA

23. **K. Inkeri,** Über eine Verallgemeinerung des letzten Fermatschen Satzes. 16 S. 1956. 200:—.

24. **Y. Väisälä,** Zur Theorie der Kompensatoren. 24 S. 1956. 250:—.

25. **K. Inkeri & V. Ennola,** The Minkowski constants for certain binary quadratic forms. 19 p. 1957. 250:—.

26. **Väinö Hovi,** X-ray studies on CsCl, CsBr, and CsCl-CsBr solid solutions. 8 p. 1957. 150:—.

27. **Liisi Oterma,** Bahnbestimmungen des kurzperiodischen Kometen Oterma (1942 VII). 24 S. 1957. 300:—.

28. **Veikko Ennola,** On the first inhomogeneous minimum of indefinite binary quadratic forms and Euclid's algorithm in real quadratic fields. 58 p. 1958. 400:—.

29. **Esa Aho,** Über Isolierung und tautomere Formen der Flavaspidsäure und anderer Filixphloroglucinabkömmlinge. 123 S. 1958. 600:—.

30. **K. V. Laurikainen & O. Varho,** A table of integrals $\int_0^\infty e^{-\alpha x} \frac{(1-e^{-x})^p}{x^{q+1}}\, dx$. 68 p. 1958. 400:—.

31. **Erkki Euranto,** The kinetics of the hydrolysis of α-halogenoalkyl esters. 107 p. 1959. 600:—.

32. **K. V. Laurikainen,** A table of "hard core integrals" $\int_0^\infty \frac{e^{-\alpha x} (1-e^{-x})^p}{x^{q+1}(x+x_0)^r}\, dx$ for central potentials. 46 p. 1959.

33. **Väinö Hovi & Asko Aurela,** A coincidence telescope for the teaching of cosmic ray physics. 7 p. 1959. 150:—.

34. **Väinö Hovi,** On the configurational free energy of KCl-KBr solid solutions. 6 p. 1959. 150:—.

35. **Väinö Hovi & Kauko Mansikka,** Entropy of long range order in β-brass. 5 p. 1959. 150:—.

36. **Liisi Oterma,** Bahnverbesserungen der kleinen Planeten 1496, 1500, 1503, 1504, 1512, 1534. 15 S. 1959. 200:—.

37. **K. Inkeri,** The real roots of Bernoulli polynomials. 19 p. 1959. 250:—.

38. **K. Inkeri & A. Sirkesalo,** Factorization of certain numbers of the form $h \cdot 2^n + k$. 14 p. 1959. 200:—.

39. **O. V. Lounasmaa,** Spontaneous vibrations of helium gas. 6 p. 1959. 100:—.

40. **Väinö Hovi & Kauko Mansikka,** On the lattice energy of alkali halides. 8 p. 1960. 150:—.

41. **Arto Salomaa,** On the composition of functions of several variables ranging over a finite set. 48 p. 1960. 400:—.

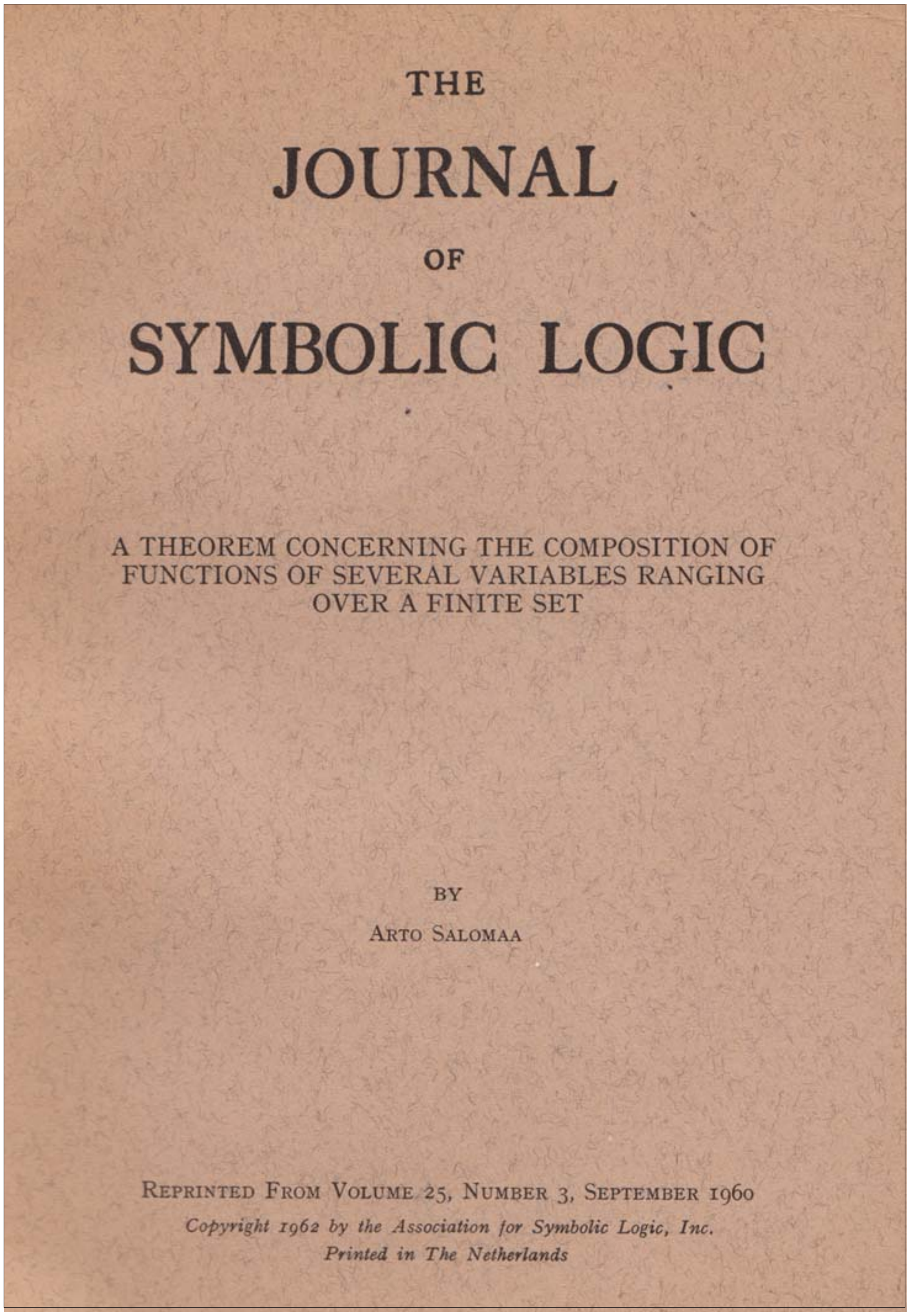
SARJA - SER. A. II. BIOLOGICA — GEOGRAPHICA

23. **Lauri E. Kari,** Fungi exsiccati fennici Institutio Botanica Universitatis Turkuensis. Schedae ad fasciculos I—X (N:o 1—500). 194 p. 1957. 750:—.

24. **Uuno Varjo,** Über das Dorf Kaunissaari und die Wanderungsbewegung seiner Bevölkerung 1921—1955. 42 S. 1957. 200:—.

25. **Uuno Varjo,** Zur Frage der kollektiven Dorfsiedlung in Südwestfinnland. 50 S. 1957. 250:—.

Jakaja: Akateeminen Kirjakauppa, Helsinki.
Distributor: Akateeminen Kirjakauppa, Helsinki, Finland.



THE

JOURNAL

OF

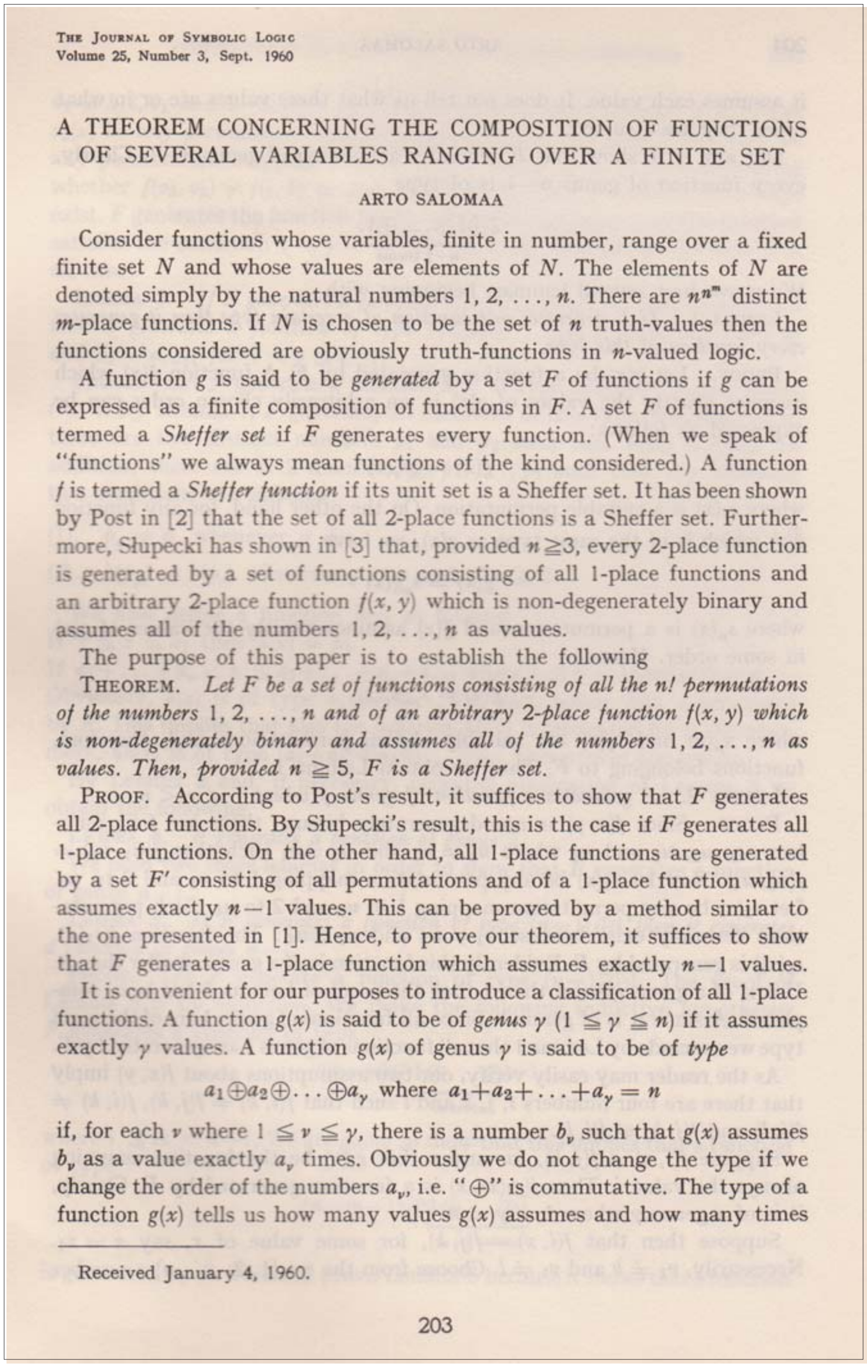
SYMBOLIC LOGIC

A THEOREM CONCERNING THE COMPOSITION OF FUNCTIONS OF SEVERAL VARIABLES RANGING OVER A FINITE SET

BY

ARTO SALOMAA

REPRINTED FROM VOLUME 25, NUMBER 3, SEPTEMBER 1960



THE JOURNAL OF SYMBOLIC LOGIC
Volume 25, Number 3, Sept. 1960

A THEOREM CONCERNING THE COMPOSITION OF FUNCTIONS OF SEVERAL VARIABLES RANGING OVER A FINITE SET

ARTO SALOMAA

Consider functions whose variables, finite in number, range over a fixed finite set N and whose values are elements of N. The elements of N are denoted simply by the natural numbers $1, 2, \ldots, n$. There are n^{n^m} distinct m-place functions. If N is chosen to be the set of n truth-values then the functions considered are obviously truth-functions in n-valued logic.

A function g is said to be *generated* by a set F of functions if g can be expressed as a finite composition of functions in F. A set F of functions is termed a *Sheffer set* if F generates every function. (When we speak of "functions" we always mean functions of the kind considered.) A function f is termed a *Sheffer function* if its unit set is a Sheffer set. It has been shown by Post in [2] that the set of all 2-place functions is a Sheffer set. Furthermore, Słupecki has shown in [3] that, provided $n \geqq 3$, every 2-place function is generated by a set of functions consisting of all 1-place functions and an arbitrary 2-place function $f(x, y)$ which is non-degenerately binary and assumes all of the numbers $1, 2, \ldots, n$ as values.

The purpose of this paper is to establish the following

THEOREM. *Let F be a set of functions consisting of all the $n!$ permutations of the numbers $1, 2, \ldots, n$ and of an arbitrary 2-place function $f(x, y)$ which is non-degenerately binary and assumes all of the numbers $1, 2, \ldots, n$ as values. Then, provided $n \geqq 5$, F is a Sheffer set.*

PROOF. According to Post's result, it suffices to show that F generates all 2-place functions. By Słupecki's result, this is the case if F generates all 1-place functions. On the other hand, all 1-place functions are generated by a set F' consisting of all permutations and of a 1-place function which assumes exactly $n-1$ values. This can be proved by a method similar to the one presented in [1]. Hence, to prove our theorem, it suffices to show that F generates a 1-place function which assumes exactly $n-1$ values.

It is convenient for our purposes to introduce a classification of all 1-place functions. A function $g(x)$ is said to be of *genus* γ $(1 \leqq \gamma \leqq n)$ if it assumes exactly γ values. A function $g(x)$ of genus γ is said to be of *type*

$$a_1 \oplus a_2 \oplus \ldots \oplus a_\gamma \text{ where } a_1 + a_2 + \ldots + a_\gamma = n$$

if, for each ν where $1 \leqq \nu \leqq \gamma$, there is a number b_ν such that $g(x)$ assumes b_ν as a value exactly a_ν times. Obviously we do not change the type if we change the order of the numbers a_ν, i.e. "$\oplus$" is commutative. The type of a function $g(x)$ tells us how many values $g(x)$ assumes and how many times

Received January 4, 1960.

it assumes each value. It does not tell us what these values are or in what order they are assumed.

Our aim is to show that F generates a function of genus $n-1$. Clearly, every function of genus $n-1$ is of type

$$2\oplus\underbrace{1\oplus\ldots\oplus 1}_{n-2 \text{ terms}}.$$

We prove first several lemmas, beginning with

LEMMA 1. *If F generates one function of a certain type then it generates every function of this type.*

PROOF. Let $g(x)$ be a function generated by F. A function $\bar{g}(x)$ which assumes exactly the values of $g(x)$ in an arbitrarily chosen order can be expressed as follows:

$$\bar{g}(x) = gs_\nu(x)$$

where $s_\nu(x)$ is a suitable permutation. On the other hand, for any function $\bar{\bar{g}}(x)$ which is of the same type as $g(x)$, we have

$$\bar{\bar{g}}(x) = s_\mu \bar{g}(x)$$

where $s_\mu(x)$ is a permutation and $\bar{g}(x)$ assumes exactly the values of $g(x)$ in some order. Hence,

$$\bar{\bar{g}}(x) = s_\mu g s_\nu(x)$$

where $s_\mu(x)$ and $s_\nu(x)$ are suitably chosen permutations and, therefore, functions belonging to F. Thus we obtain Lemma 1.

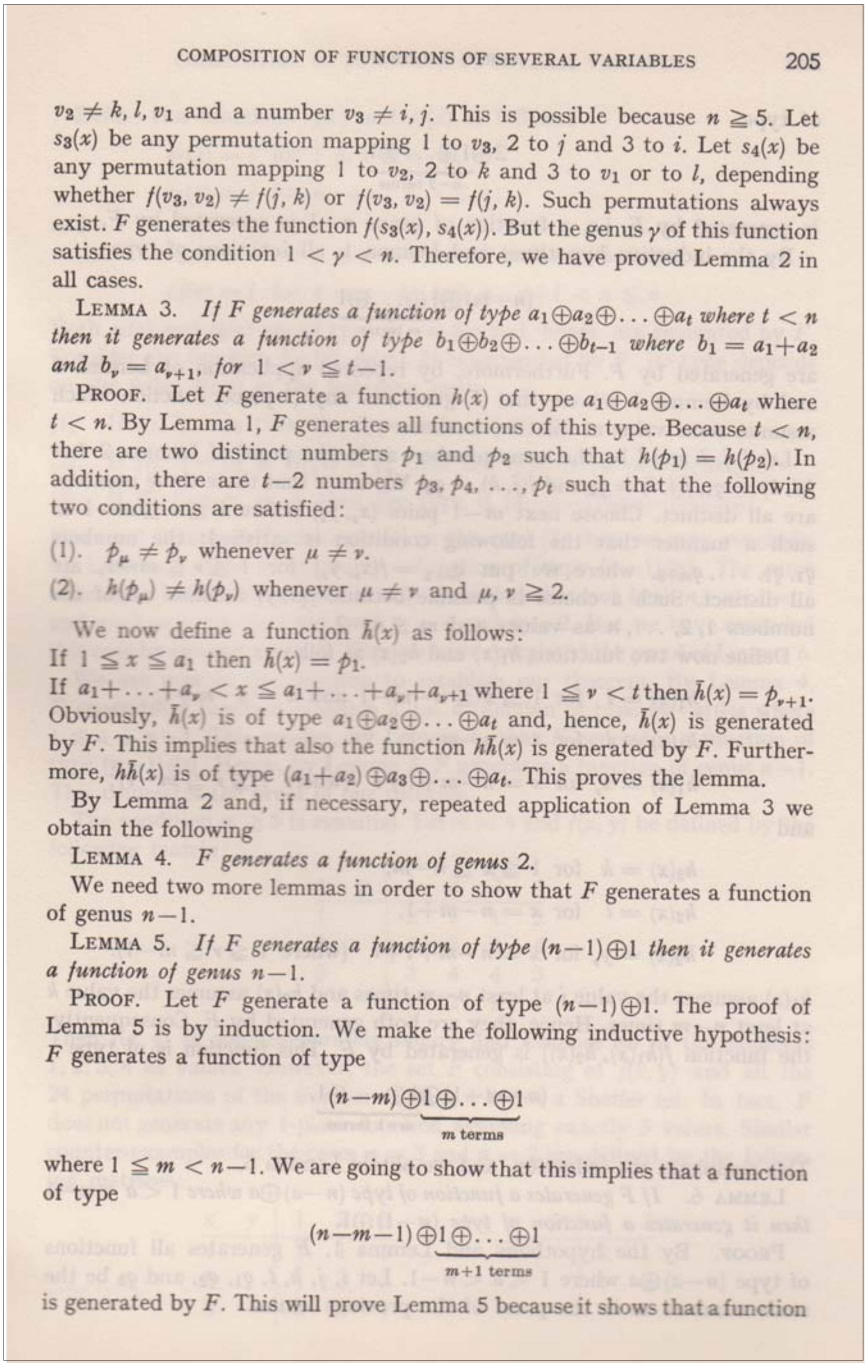
LEMMA 2. *F generates a function of genus γ where $1 < \gamma < n$.*

PROOF. Since $f(x, y)$ is non-degenerately binary, there are four numbers u_1, u_2, u_3 and u_4 where $u_1 \neq u_3$ and $u_2 \neq u_4$ such that $f(u_1, u_2) = f(u_3, u_4)$. Now let $s_1(x)$ be any permutation mapping 1 to u_1 and 2 to u_3. Let $s_2(x)$ be any permutation mapping 1 to u_2 and 2 to u_4. Such permutations certainly exist because $u_1 \neq u_3$ and $u_2 \neq u_4$. The function $f(s_1(x), s_2(x))$ is generated by F. Evidently this function is of a genus smaller than n. If it is of a genus greater than 1 then the proof of Lemma 2 has been completed. Assume it is of genus 1. Since all functions of genus 1 are of the same type we conclude by Lemma 1 that all functions of genus 1 are generated by F.

As the reader may easily verify, our two assumptions about $f(x, y)$ imply that there are four numbers i, j, k and l such that $f(i, k) \neq f(j, k)$, $f(i, k) \neq f(i, l)$ and $f(j, k) \neq f(i, l)$.

Suppose $f(i, x) \neq f(j, k)$, for any x. Let $g_i(x)$ be the function assuming always the value i. Then $f(g_i(x), x)$ is a function generated by F. Clearly, it is of a genus γ where $1 < \gamma < n$.

Suppose then that $f(i, x) = f(j, k)$, for some value of x, say $x = v_1$. Necessarily, $v_1 \neq k$ and $v_1 \neq l$. Choose from the set $\{1, 2, \ldots, n\}$ a number



$v_2 \neq k, l, v_1$ and a number $v_3 \neq i, j$. This is possible because $n \geqq 5$. Let $s_3(x)$ be any permutation mapping 1 to v_3, 2 to j and 3 to i. Let $s_4(x)$ be any permutation mapping 1 to v_2, 2 to k and 3 to v_1 or to l, depending whether $f(v_3, v_2) \neq f(j, k)$ or $f(v_3, v_2) = f(j, k)$. Such permutations always exist. F generates the function $f(s_3(x), s_4(x))$. But the genus γ of this function satisfies the condition $1 < \gamma < n$. Therefore, we have proved Lemma 2 in all cases.

LEMMA 3. *If F generates a function of type $a_1 \oplus a_2 \oplus \ldots \oplus a_t$ where $t < n$ then it generates a function of type $b_1 \oplus b_2 \oplus \ldots \oplus b_{t-1}$ where $b_1 = a_1 + a_2$ and $b_\nu = a_{\nu+1}$, for $1 < \nu \leqq t-1$.*

PROOF. Let F generate a function $h(x)$ of type $a_1 \oplus a_2 \oplus \ldots \oplus a_t$ where $t < n$. By Lemma 1, F generates all functions of this type. Because $t < n$, there are two distinct numbers p_1 and p_2 such that $h(p_1) = h(p_2)$. In addition, there are $t-2$ numbers $p_3, p_4, \ldots, p_t$ such that the following two conditions are satisfied:

(1). $p_\mu \neq p_\nu$ whenever $\mu \neq \nu$.

(2). $h(p_\mu) \neq h(p_\nu)$ whenever $\mu \neq \nu$ and $\mu, \nu \geqq 2$.

We now define a function $\bar{h}(x)$ as follows:
If $1 \leqq x \leqq a_1$ then $\bar{h}(x) = p_1$.
If $a_1 + \ldots + a_\nu < x \leqq a_1 + \ldots + a_\nu + a_{\nu+1}$ where $1 \leqq \nu < t$ then $\bar{h}(x) = p_{\nu+1}$.
Obviously, $\bar{h}(x)$ is of type $a_1 \oplus a_2 \oplus \ldots \oplus a_t$ and, hence, $\bar{h}(x)$ is generated by F. This implies that also the function $h\bar{h}(x)$ is generated by F. Furthermore, $h\bar{h}(x)$ is of type $(a_1 + a_2) \oplus a_3 \oplus \ldots \oplus a_t$. This proves the lemma.

By Lemma 2 and, if necessary, repeated application of Lemma 3 we obtain the following

LEMMA 4. *F generates a function of genus 2.*

We need two more lemmas in order to show that F generates a function of genus $n-1$.

LEMMA 5. *If F generates a function of type $(n-1) \oplus 1$ then it generates a function of genus $n-1$.*

PROOF. Let F generate a function of type $(n-1) \oplus 1$. The proof of Lemma 5 is by induction. We make the following inductive hypothesis: F generates a function of type

$$(n-m) \oplus \underbrace{1 \oplus \ldots \oplus 1}_{m \text{ terms}}$$

where $1 \leqq m < n-1$. We are going to show that this implies that a function of type

$$(n-m-1) \oplus \underbrace{1 \oplus \ldots \oplus 1}_{m+1 \text{ terms}}$$

is generated by F. This will prove Lemma 5 because it shows that a function of type

$$2\oplus\underbrace{1\oplus\ldots\oplus 1}_{n-2\text{ terms}}$$

is generated by F, i.e. a function of genus $n-1$ is generated by F.

By the inductive hypothesis and Lemma 1, all functions of type

$$(n-m)\oplus\underbrace{1\oplus\ldots\oplus 1}_{m\text{ terms}}$$

are generated by F. Furthermore, by repeated application of Lemma 3 and by Lemma 1 we see that F generates any (1-place) function which assumes some value at least $n-m$ times.

Let i, j, k and l be the same numbers as in the proof of Lemma 2. Let $f(i, k) = q_1$, $f(i, l) = q_2$ and $f(j, k) = q_3$. We know that these three numbers are all distinct. Choose next $m-1$ pairs (x_ν, y_ν) where $1 \leqq \nu \leqq m-1$ in such a manner that the following condition is satisfied: the numbers $q_1, q_2, \ldots, q_{m+2}$, where we put $q_{\nu+3} = f(x_\nu, y_\nu)$ for $1 \leqq \nu \leqq m-1$, are all distinct. Such a choice is possible because $f(x, y)$ assumes all of the numbers $1, 2, \ldots, n$ as values and $m \leqq n-2$.

Define now two functions $h_1(x)$ and $h_2(x)$ as follows:

$$h_1(x) = i \quad \text{for } 1 \leqq x \leqq n-m-1 \text{ and } x = n-m+1,$$

$$h_1(x) = j \quad \text{for } x = n-m,$$

$$h_1(x) = x_\nu \quad \text{for } x = n-m+1+\nu \quad (\text{where } 1 \leqq \nu \leqq m-1);$$

and

$$h_2(x) = k \quad \text{for } 1 \leqq x \leqq n-m,$$

$$h_2(x) = l \quad \text{for } x = n-m+1,$$

$$h_2(x) = y_\nu \quad \text{for } x = n-m+1+\nu \quad (\text{where } 1 \leqq \nu \leqq m-1).$$

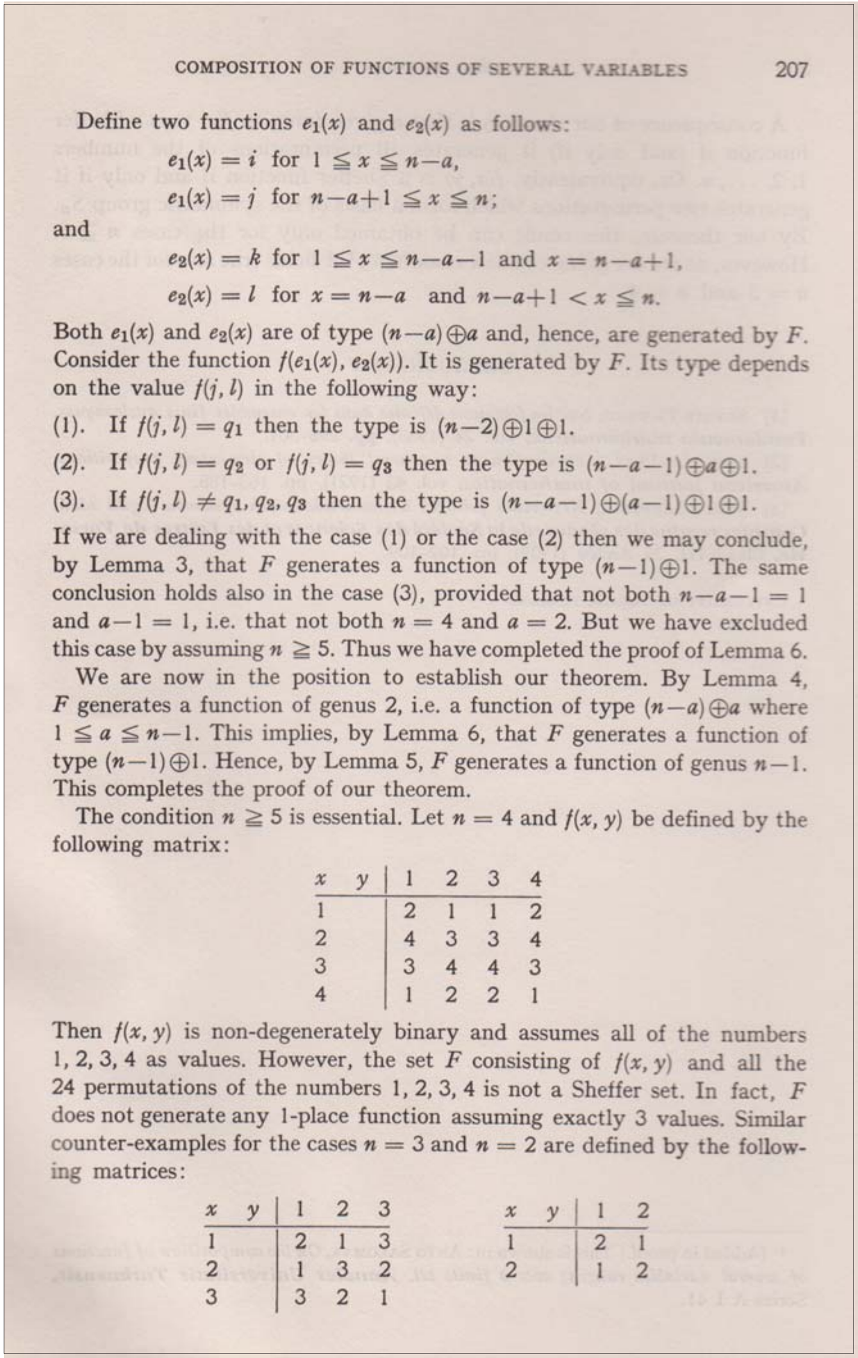
$h_1(x)$ assumes the value i at least $n-m$ times and $h_2(x)$ assumes the value k at least $n-m$ times. Hence, they are both generated by F. Consequently, the function $f(h_1(x), h_2(x))$ is generated by F. This function is of type

$$(n-m-1)\oplus\underbrace{1\oplus\ldots\oplus 1}_{m+1\text{ terms}}.$$

This completes the induction, and we obtain Lemma 5.

LEMMA 6. *If F generates a function of type $(n-a)\oplus a$ where $1 < a < n-1$ then it generates a function of type $(n-1)\oplus 1$.*

PROOF. By the hypothesis and Lemma 1, F generates all functions of type $(n-a)\oplus a$ where $1 < a < n-1$. Let i, j, k, l, q_1, q_2, and q_3 be the same numbers as in the proof of the previous lemma.



Define two functions $e_1(x)$ and $e_2(x)$ as follows:

$$e_1(x) = i \text{ for } 1 \leqq x \leqq n-a,$$
$$e_1(x) = j \text{ for } n-a+1 \leqq x \leqq n;$$

and

$$e_2(x) = k \text{ for } 1 \leqq x \leqq n-a-1 \text{ and } x = n-a+1,$$
$$e_2(x) = l \text{ for } x = n-a \text{ and } n-a+1 < x \leqq n.$$

Both $e_1(x)$ and $e_2(x)$ are of type $(n-a) \oplus a$ and, hence, are generated by F. Consider the function $f(e_1(x), e_2(x))$. It is generated by F. Its type depends on the value $f(j, l)$ in the following way:

(1). If $f(j, l) = q_1$ then the type is $(n-2) \oplus 1 \oplus 1$.

(2). If $f(j, l) = q_2$ or $f(j, l) = q_3$ then the type is $(n-a-1) \oplus a \oplus 1$.

(3). If $f(j, l) \neq q_1, q_2, q_3$ then the type is $(n-a-1) \oplus (a-1) \oplus 1 \oplus 1$.

If we are dealing with the case (1) or the case (2) then we may conclude, by Lemma 3, that F generates a function of type $(n-1) \oplus 1$. The same conclusion holds also in the case (3), provided that not both $n-a-1 = 1$ and $a-1 = 1$, i.e. that not both $n = 4$ and $a = 2$. But we have excluded this case by assuming $n \geqq 5$. Thus we have completed the proof of Lemma 6.

We are now in the position to establish our theorem. By Lemma 4, F generates a function of genus 2, i.e. a function of type $(n-a) \oplus a$ where $1 \leqq a \leqq n-1$. This implies, by Lemma 6, that F generates a function of type $(n-1) \oplus 1$. Hence, by Lemma 5, F generates a function of genus $n-1$. This completes the proof of our theorem.

The condition $n \geqq 5$ is essential. Let $n = 4$ and $f(x, y)$ be defined by the following matrix:

x y	1	2	3	4
1	2	1	1	2
2	4	3	3	4
3	3	4	4	3
4	1	2	2	1

Then $f(x, y)$ is non-degenerately binary and assumes all of the numbers 1, 2, 3, 4 as values. However, the set F consisting of $f(x, y)$ and all the 24 permutations of the numbers 1, 2, 3, 4 is not a Sheffer set. In fact, F does not generate any 1-place function assuming exactly 3 values. Similar counter-examples for the cases $n = 3$ and $n = 2$ are defined by the following matrices:

x y	1	2	3
1	2	1	3
2	1	3	2
3	3	2	1

x y	1	2
1	2	1
2	1	2

A consequence of our theorem is that a given function $f(x, y)$ is a Sheffer function if (and only if) it generates all permutations of the numbers $1, 2, \dots, n$. Or, equivalently, $f(x, y)$ is a Sheffer function if and only if it generates two permutations which form a basis of the symmetric group S_n. By our theorem, this result can be obtained only for the cases $n \geqq 5$. However, as we are going to show elsewhere,[1] it holds true also for the cases $n = 3$ and $n = 4$.

BIBLIOGRAPHY

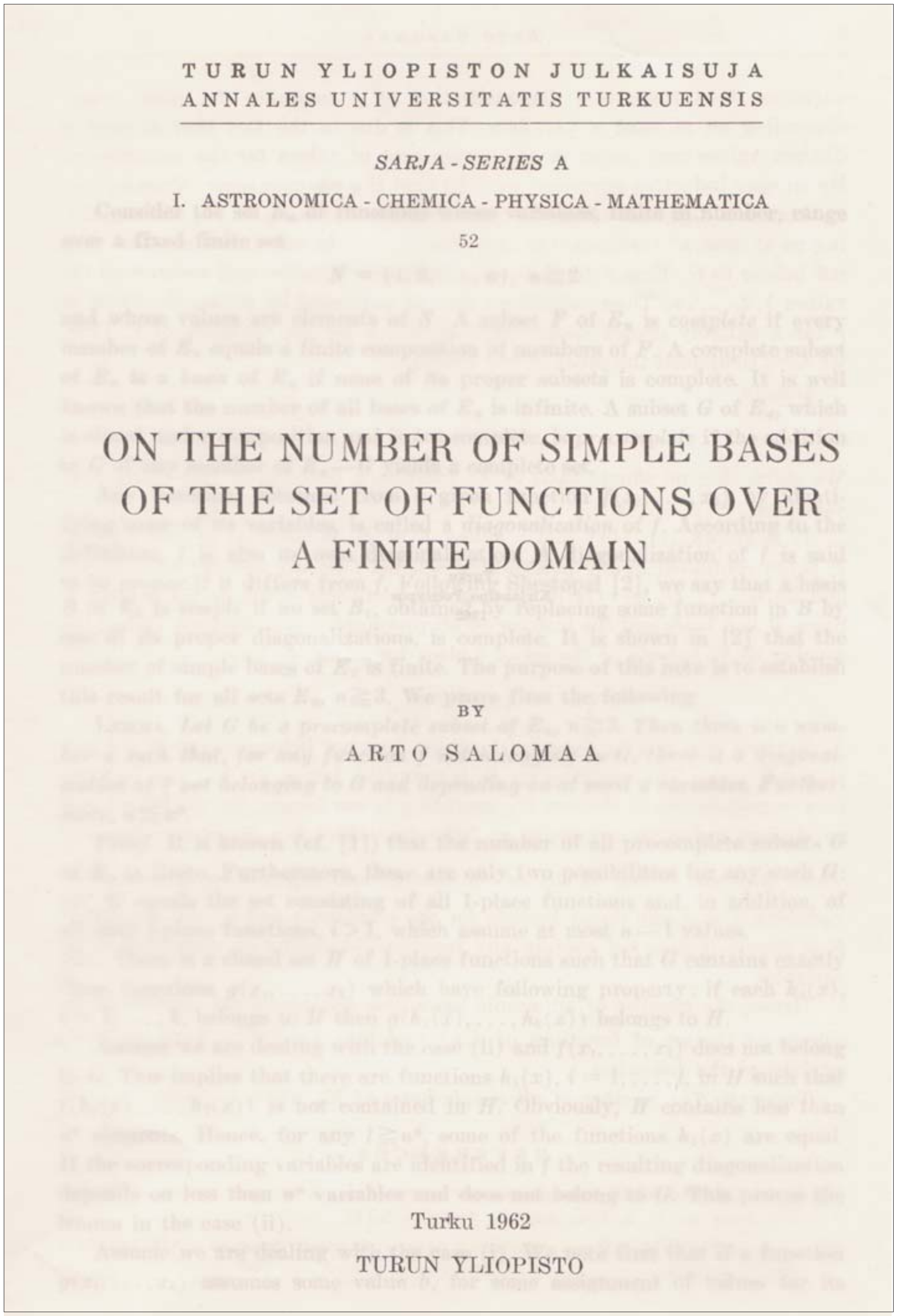
[1] SOPHIE PICCARD, *Sur les fonctions définies dans les ensembles finis quelconques*, **Fundamenta mathematicae**, vol. 24 (1935), pp. 298–301.

[2] EMIL L. POST, *Introduction to a general theory of elementary propositions*, **American journal of mathematics**, vol. 43 (1921), pp. 163–185.

[3] JERZY SŁUPECKI, *Kryterium pełności wielowartościowych systemów logiki zdań*, **Comptes rendus des séances de la Société des Sciences et des Lettres de Varsovie**, Classe III, 32 Année (1939), pp. 102–109.

UNIVERSITY OF TURKU, FINLAND

[1] (Added in proof.) This is shown in: ARTO SALOMAA, *On the composition of functions of several variables ranging over a finite set*, **Annales Universitatis Turkuensis**, Series A I 41.



TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

SARJA - SERIES A

I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA

52

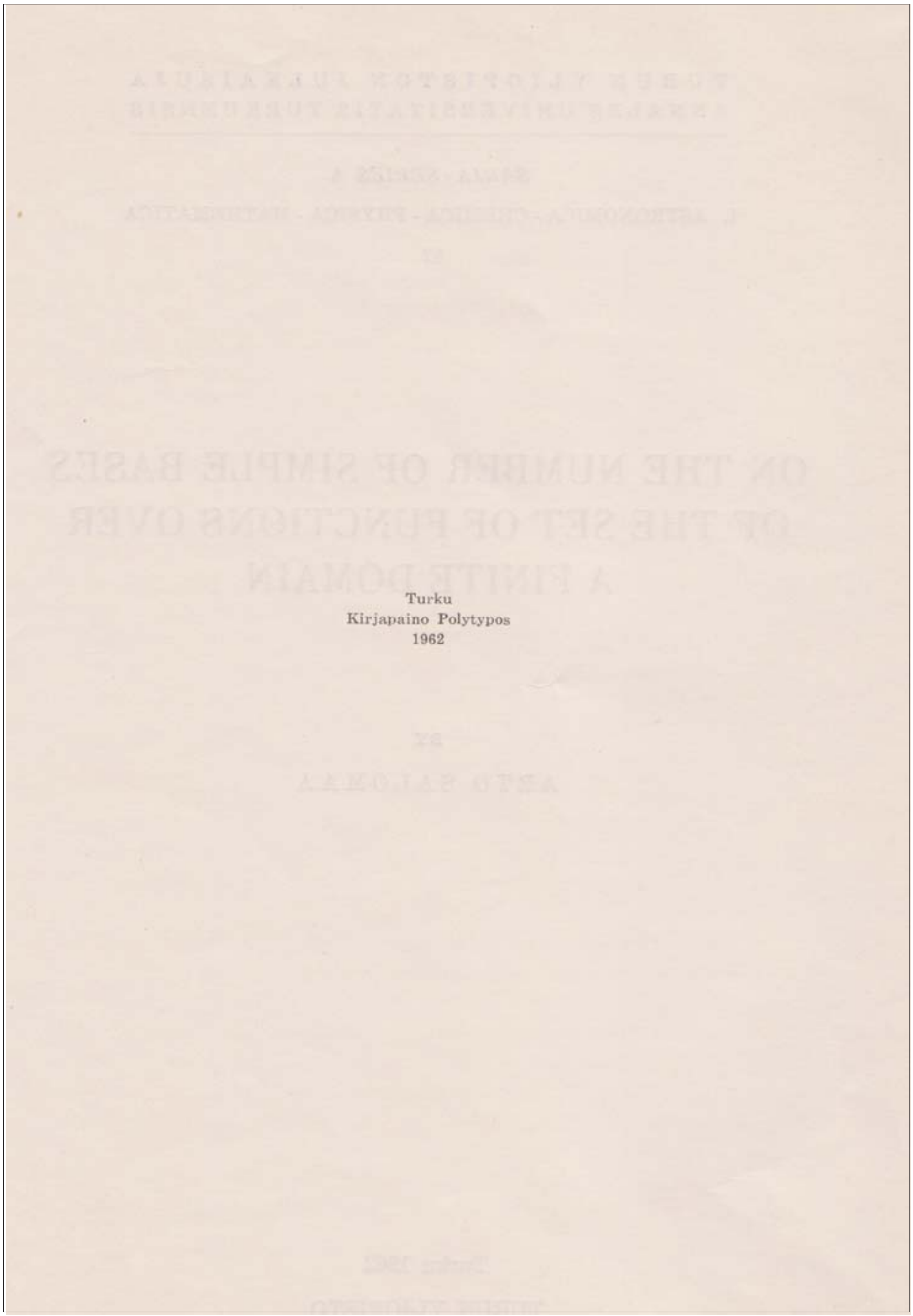
ON THE NUMBER OF SIMPLE BASES OF THE SET OF FUNCTIONS OVER A FINITE DOMAIN

BY

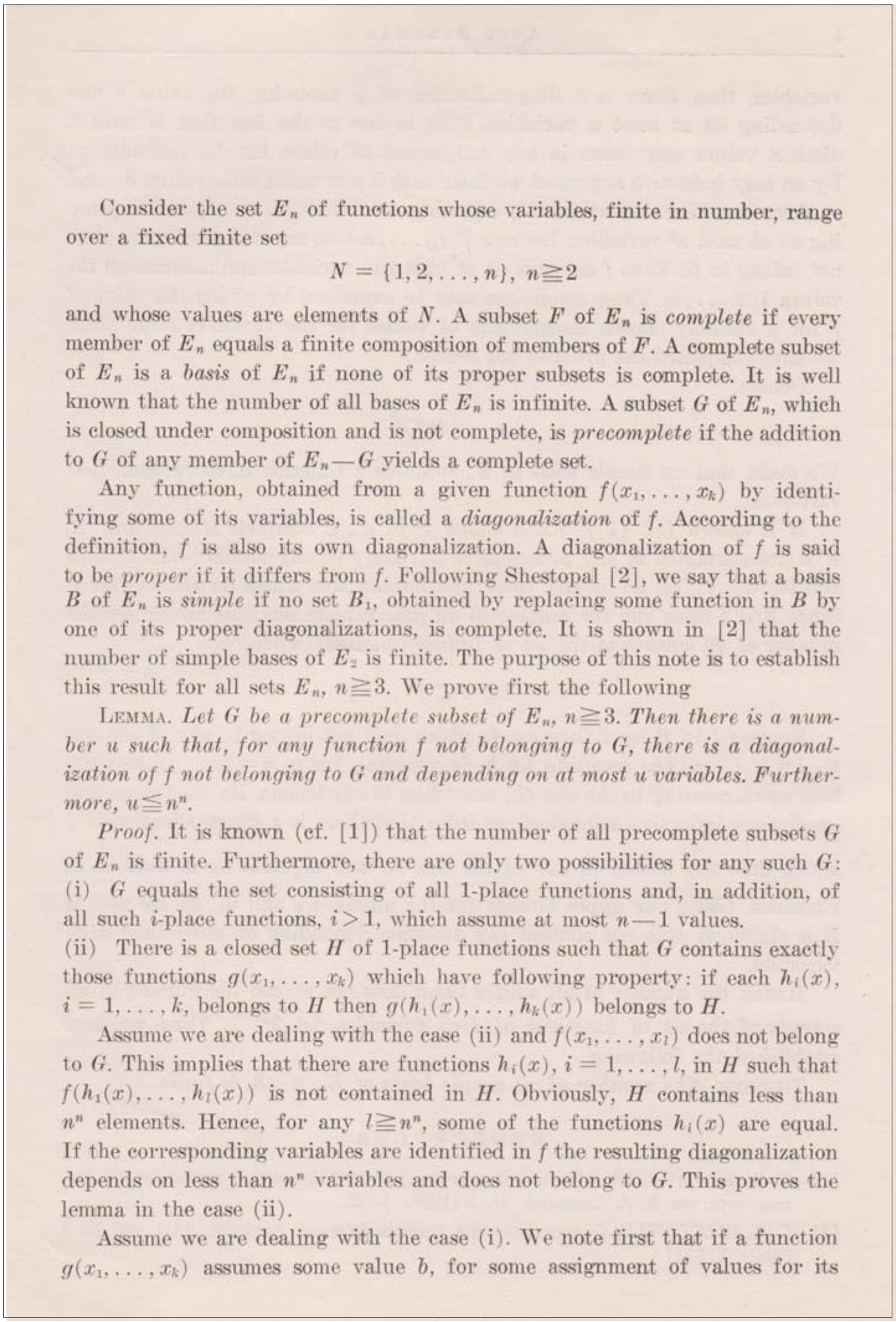
ARTO SALOMAA

Turku 1962

TURUN YLIOPISTO



Turku
Kirjapaino Polytypos
1962



Consider the set E_n of functions whose variables, finite in number, range over a fixed finite set

$$N = \{1, 2, \ldots, n\},\ n \geqq 2$$

and whose values are elements of N. A subset F of E_n is *complete* if every member of E_n equals a finite composition of members of F. A complete subset of E_n is a *basis* of E_n if none of its proper subsets is complete. It is well known that the number of all bases of E_n is infinite. A subset G of E_n, which is closed under composition and is not complete, is *precomplete* if the addition to G of any member of $E_n - G$ yields a complete set.

Any function, obtained from a given function $f(x_1, \ldots, x_k)$ by identifying some of its variables, is called a *diagonalization* of f. According to the definition, f is also its own diagonalization. A diagonalization of f is said to be *proper* if it differs from f. Following Shestopal [2], we say that a basis B of E_n is *simple* if no set B_1, obtained by replacing some function in B by one of its proper diagonalizations, is complete. It is shown in [2] that the number of simple bases of E_2 is finite. The purpose of this note is to establish this result for all sets E_n, $n \geqq 3$. We prove first the following

LEMMA. *Let G be a precomplete subset of E_n, $n \geqq 3$. Then there is a number u such that, for any function f not belonging to G, there is a diagonalization of f not belonging to G and depending on at most u variables. Furthermore, $u \leqq n^n$.*

Proof. It is known (cf. [1]) that the number of all precomplete subsets G of E_n is finite. Furthermore, there are only two possibilities for any such G:
(i) G equals the set consisting of all 1-place functions and, in addition, of all such i-place functions, $i > 1$, which assume at most $n - 1$ values.
(ii) There is a closed set H of 1-place functions such that G contains exactly those functions $g(x_1, \ldots, x_k)$ which have following property: if each $h_i(x)$, $i = 1, \ldots, k$, belongs to H then $g(h_1(x), \ldots, h_k(x))$ belongs to H.

Assume we are dealing with the case (ii) and $f(x_1, \ldots, x_l)$ does not belong to G. This implies that there are functions $h_i(x)$, $i = 1, \ldots, l$, in H such that $f(h_1(x), \ldots, h_l(x))$ is not contained in H. Obviously, H contains less than n^n elements. Hence, for any $l \geqq n^n$, some of the functions $h_i(x)$ are equal. If the corresponding variables are identified in f the resulting diagonalization depends on less than n^n variables and does not belong to G. This proves the lemma in the case (ii).

Assume we are dealing with the case (i). We note first that if a function $g(x_1, \ldots, x_k)$ assumes some value b, for some assignment of values for its variables, then there is a diagonalization of g assuming the value b and depending on at most n variables. This is due to the fact that at most n distinct values may occur in any assignment of values for the variables x_i. By an easy inductive argument we infer that if g assumes some values $b_1, \dots, b_p$ there is a diagonalization of g assuming the values $b_1, \dots, b_p$ and depending on at most n^p variables. Let now $f(x_1, \dots, x_l)$ be any function which does not belong to G. Then f depends on at least two variables and assumes all the values $1, 2, \dots, n$. These conditions may be expressed by giving the value of f for n suitably chosen assignments of values for the variables of f. Thus, we have completed the proof of our lemma.

Denote

$$d(n) = (n^n)^{2^{n^n}}.$$

We claim that no simple basis of E_n contains a function of more than $d(n)$ variables.

It is known (cf. [1]) that a subset F of E_n is complete if, and only if, F is not contained in any precomplete set. Let f be any member of a basis B and let $G_1, \dots, G_s$ be exactly those precomplete sets which do not contain f. Since B is a basis and the number of all precomplete sets does not exceed the number of all subsets of the set of 1-place functions, we have

$$1 \leqq s \leqq 2^{n^n}.$$

Replace f in B by a function f_1 which does not belong to any of the sets G_i, $i = 1, \dots, s$. The resulting set B_1 is complete. Let u_i, $i = 1, \dots, s$, be numbers corresponding to the sets G_i, according to our lemma. By the lemma and an obvious inductive argument, we infer that there is a diagonalization of f which does not belong to any of the sets G_i and depends on at most $\prod_{i=1}^{s} u_i$ variables. Using our upper bounds for the numbers s and u_i, we see that if B is simple it does not contain any function depending on more than $d(n)$ variables.

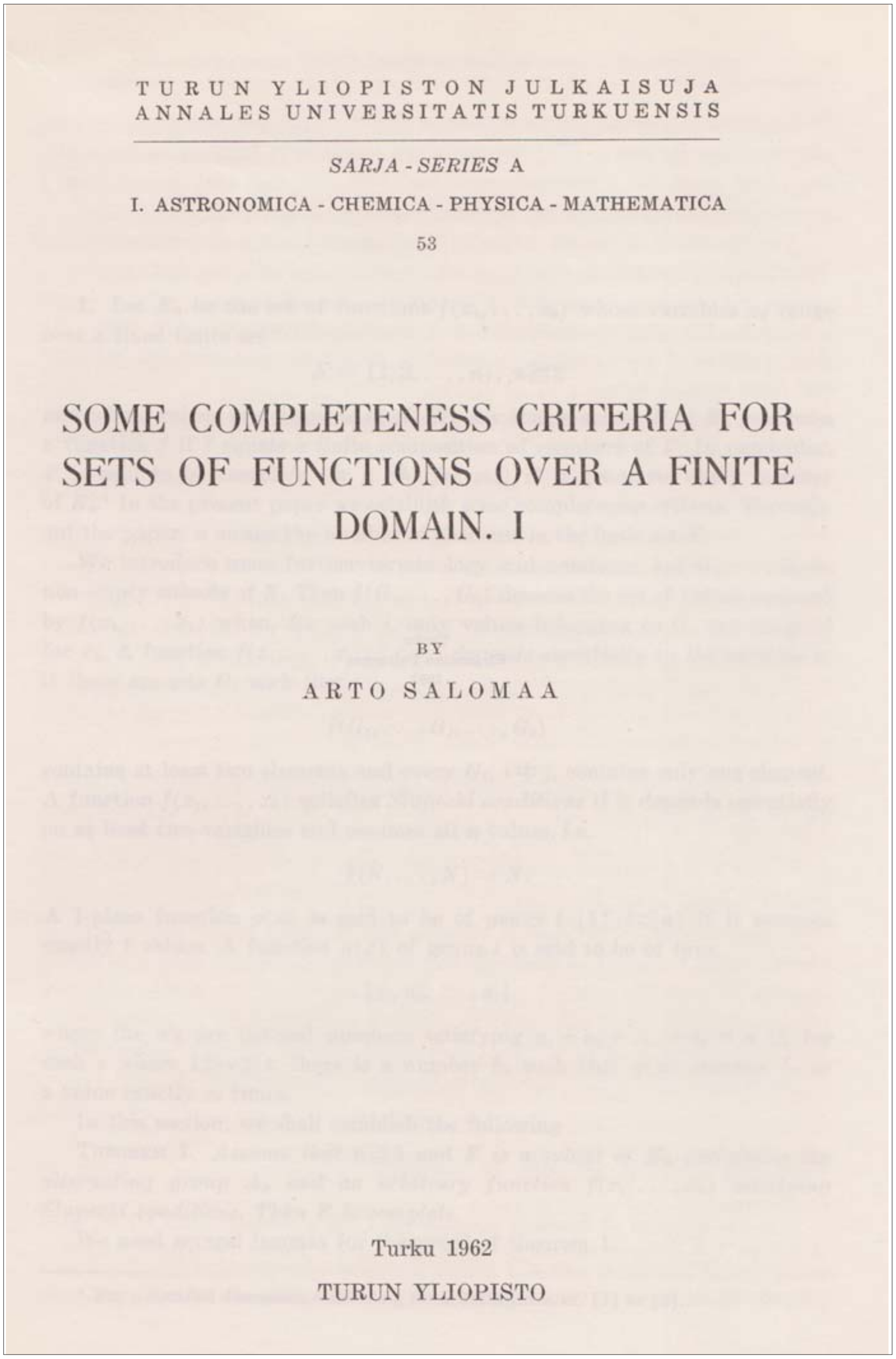
Hence, the number of all simple bases does not exceed the number of all subsets of the set of functions of $d(n)$ variables, i.e. $2^{n^{n^{d(n)}}}$. Thus, we have established the following

THEOREM. *The number of all simple bases of E_n, $n \geqq 3$, is finite.*

REFERENCES

[1] С. В. ЯБЛОНСКИЙ, Функциональные построения в k-значной логике. — Тр. Матем. инст. им. В. А. Стеклова, 51, 5 (1958), 5-142.

[2] Г. А. ШЕСТОПАЛ, О числе простых базисов булевых функций.-ДАН, 140, № 2 (1961), 314-317.



TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

SARJA - SERIES A

I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA

53

SOME COMPLETENESS CRITERIA FOR SETS OF FUNCTIONS OVER A FINITE DOMAIN. I

BY

ARTO SALOMAA

Turku 1962

TURUN YLIOPISTO

Turku
Kirjapaino Polytypos
1962

1. Let E_n be the set of functions $f(x_1, \dots, x_k)$ whose variables x_i range over a fixed finite set

$$N = \{1, 2, \dots, n\},\ n \geqq 2$$

and whose values are elements of N. We say that a subset F of E_n *generates* a function f if f equals a finite composition of members of F. In particular, F is said to be *complete* (or a *Sheffer set*) if it generates every member of E_n.[1] In the present paper we establish some completeness criteria. Throughout the paper, n means the number of elements in the basic set N.

We introduce some further terminology and notations. Let $G_1, \dots, G_k$ be non-empty subsets of N. Then $f(G_1, \dots, G_k)$ denotes the set of values assumed by $f(x_1, \dots, x_k)$ when, for each i, only values belonging to G_i are assigned for x_i. A function $f(x_1, \dots, x_j, \dots, x_k)$ *depends essentially on the variable* x_j if there are sets G_i such that

$$f(G_1, \dots, G_j, \dots, G_k)$$

contains at least two elements and every G_i, $i \neq j$, contains only one element. A function $f(x_1, \dots, x_k)$ satisfies *Słupecki conditions* if it depends essentially on at least two variables and assumes all n values, i.e.

$$f(N, \dots, N) = N.$$

A 1-place function $g(x)$ is said to be of *genus* t $(1 \leqq t \leqq n)$ if it assumes exactly t values. A function $g(x)$ of genus t is said to be of *type*

$$[a_1, a_2, \dots, a_t]$$

where the a's are natural numbers satisfying $a_1 + a_2 + \dots + a_t = n$ if, for each ν where $1 \leqq \nu \leqq t$, there is a number b_ν such that $g(x)$ assumes b_ν as a value exactly a_ν times.

In this section, we shall establish the following

THEOREM 1. *Assume that $n \geqq 5$ and F is a subset of E_n containing the alternating group A_n and an arbitrary function $f(x_1, \dots, x_k)$ satisfying Słupecki conditions. Then F is complete.*

We need several lemmas for the proof of theorem 1.

[1] For a detailed discussion concerning these definitions, cf. [1] or [2].

LEMMA 1.1. *Assume that* $n \geqq 3$[1] *and* $f(x_1, \ldots, x_k)$ *satisfies Słupecki conditions. Then for any* j, $3 \leqq j \leqq n$, *there are sets* G_i, $i = 1, \ldots, k$, *each consisting of at most* $j-1$ *elements such that* $f(G_1, \ldots, G_k)$ *contains at least* j *elements.*

For the proof of lemma 1.1, cf. [1]. (Lemma 1.1 is a consequence of the "fundamental lemma" in [1].)

LEMMA 1.2. *Assume that* $n \geqq 4$ *and* $h(x)$ *is of genus* $\leqq n-1$. *Then the set consisting of* $h(x)$ *and of the members of* A_n *generates every function of the same type as* $h(x)$.

Proof. Let $h'(x)$ be an arbitrary function of the same type as $h(x)$. Then it follows from our definition of the type of a function that

$$h'(x) = s_1 h s_2(x) \tag{1}$$

where s_1 and s_2 are permutations. We have to show that (1) holds for some even permutations s_1 and s_2. This is the case if $h(x)$ is of genus $\leqq n-2$ because A_n is $(n-2)$-ply transitive.

Therefore, we may assume that $h(x)$ is of genus $n-1$. We show first that if in (1) s_2 is odd it may be replaced by an even permutation.

There are distinct numbers a_1 and a_2 such that $h(a_1) = h(a_2)$. Denote $a_3 = s_2^{-1}(a_1)$ and $a_4 = s_2^{-1}(a_2)$. Obviously, $a_3 \neq a_4$. Consider the permutation s_2' defined as follows:

$$s_2'(a_3) = a_2,\ s_2'(a_4) = a_1,\ s_2'(x) = s_2(x) \text{ for } x \neq a_3, a_4.$$

Then also

$$h'(x) = s_1 h s_2'(x).$$

Clearly, either s_2 or s_2' is even.

Hence, it suffices to consider the case that in (1) s_1 is odd and s_2 is even. Denote $h_1(x) = hs_2(x)$. Choose distinct numbers a_5 and a_6 such that $h_1(x)$ assumes both of the values $h_1(a_5)$ and $h_1(a_6)$ only once. The choice is always possible because $n \geqq 4$ and $h_1(x)$ is of genus $n-1$. Clearly, $h_1(a_3) = h_1(a_4)$. Therefore, both $a_5 \neq a_3, a_4$ and $a_6 \neq a_3, a_4$. Let s_3 be the transposition $(h_1(a_5)\,h_1(a_6))$ and s_4 the product $(a_3a_4)(a_5a_6)$. Furthermore, define

$$s_5(x) = s_3 s_1(x) \text{ and } s_6(x) = s_2 s_4(x).$$

Then both s_5 and s_6 are even. In addition,

[1] In the statement of theorem 1 the condition $n \geqq 5$ is necessary. Thus for the proof of theorem 1, it obviously suffices to assume that $n \geqq 5$. A sharper formulation is given to lemma 1.1 and also to the following lemmas because we shall use these lemmas for other purposes, too.

$$h'(x) = s_5 h s_6(x).$$

This proves lemma 1.2.

LEMMA 1.3. *The set of all functions of type* $[b_1, b_2, \ldots, b_t]$ *where* $1 < t < n$ *generates every function of type* $[b_1 + b_2, b_3, \ldots, b_t]$.

Proof. Let $g(x)$ be an arbitrary function of type $[b_1 + b_2, b_3, \ldots, b_t]$. Suppose $g(x)$ assumes the value c_1 exactly $b_1 + b_2$ times and does not assume the value c_2 at all. Such numbers c_1 and c_2 certainly exist. Consider any function $g_1(x)$ defined as follows: $g_1(x) = g(x)$, except for b_2 values x such that $g(x) = c_1$, $g_1(x) = c_2$. Clearly, $g_1(x)$ is of type $[b_1, b_2, \ldots, b_t]$. We now choose such a function $g_2(x)$ of the type mentioned which maps the values assumed by $g(x)$ the themselves and c_2 to c_1. The choice is always possible. Then

$$g(x) = g_2 g_1(x).$$

Hence, lemma 1.3 follows.

LEMMA 1.4. *Assume that* $n \geqq 4$ *and* F *is a set of functions as in the statement of theorem* 1. *Then* F *generates a function of genus smaller than* n. *If* $n \geqq 5$ *then* F *generates a function whose genus* t *satisfies* $1 < t < n$.

Proof. By lemma 1.1, there are numbers $\alpha_1, \ldots, \alpha_k$ such that

$$f(S_1, \ldots, S_k) = N$$

where $S_i = N - \{\alpha_i\}$, for $i = 1, \ldots, k$. Denote $f(\alpha_1, \ldots, \alpha_k) = \alpha$. There are numbers α'_i, $i = 1, \ldots, k$, such that $f(\alpha'_1, \ldots, \alpha'_k) = \alpha$ and $\alpha'_i \neq \alpha_i$, for $i = 1, \ldots, k$. Choose k even permutations $p_i(x)$, $i = 1, \ldots, k$, such that $p_i(1) = \alpha_i$ and $p_i(2) = \alpha'_i$. The choice is possible because $n \geqq 4$ and A_n is $(n-2)$-ply transitive. Then $f(p_1(x), \ldots, p_k(x))$ is of genus smaller than n.

To complete the proof of the lemma, it suffices to consider the case where $n \geqq 5$ and $f(p_1(x), \ldots, p_k(x))$ is of genus 1. Hence, F generates all constants. Using lemma 1.1, we choose sets G_i, $i = 1, \ldots, k$, such that each G_i consists of two (not necessarily distinct) elements β_i and β'_i and $f(G_1, \ldots, G_k)$ contains at least three distinct elements β, β' and β''. By a suitable renumbering of the variables, this choice can be made in such a way that

$$f(\beta_1, \beta_2, \ldots, \beta_k) = \beta,$$
$$f(\beta'_1, \beta_2, \ldots, \beta_k) = \beta'$$

and

$$f(\beta'_1, \beta'_2, \ldots, \beta'_k) = \beta''.$$

Clearly, F generates the 1-place function $f(x, \beta_2, \ldots, \beta_k)$. If this function does not assume the value β'' we have completed the proof of the lemma.

Suppose

$$f(\gamma_1, \beta_2, \dots, \beta_k) = \beta''.$$

Then necessarily $\gamma_1 \neq \beta_1, \beta'_1$. Choose numbers γ_2 and $\gamma_{3,i}$, $i = 2, \dots, k$, such that $\gamma_2 \neq \beta_1, \beta'_1, \gamma_1$ and $\gamma_{3,i} \neq \beta_i, \beta'_i$ if $\beta_i \neq \beta'_i$ but $\gamma_{3,i} = \beta_i$ if $\beta_i = \beta'_i$. Assume that

$$f(\gamma_2, \gamma_{3,2}, \dots, \gamma_{3,k}) = \beta''.$$

Let $q_1(x)$ be any even permutation such that $q_1(1) = \gamma_2$, $q_1(2) = \beta_1$ and $q_1(3) = \beta'_1$. Let $q_i(x)$, $i = 2, \dots, k$, be any even permutations or constants such that $q_i(1) = \gamma_{3,i}$, $q_i(2) = \beta_i$ and $q_i(3) = \beta'_i$. (I.e. if $\beta_i \neq \beta'_i$ then $q_i(x)$ is an even permutation but if $\beta_i = \beta'_i$ then $q_i(x) = \beta_i$.) Then $f(q_1(x), \dots, q_k(x))$ is of genus t with $1 < t < n$. Finally, assume that

$$f(\gamma_2, \gamma_{3,2}, \dots, \gamma_{3,k}) \neq \beta''.$$

Let $q'_1(x)$ be any even permutation such that $q'_1(1) = \gamma_2$, $q'_1(2) = \gamma_1$ and $q'_1(3) = \beta'_1$. Then $f(q'_1(x), q_2(x), \dots, q_k(x))$ is of genus t with $1 < t < n$. This proves lemma 1.4. We note that the latter part of the proof remains valid also for $n = 4$, provided F contains all permutations. The numbers β and γ and the functions q are defined exactly as above but, in this case, some of the permutations q may be odd.

The proof of lemma 1.4 is essentially the same as the proof of lemma 11.3 in [2], with two modifications due to lemma 1.1 above and the fact that A_n is $(n-2)$-ply transitive. Similar modifications in the proofs of lemmas 11.6 and 11.7 in [2] yield the following

LEMMA 1.5. *Assume that $n \geqq 4$ and F_1 is a set of functions satisfying the hypothesis of theorem 1 and, in addition, containing a function of type $[n-a, a]$ where $1 \leqq a < n$ and not both $n = 4$ and $a = 2$. Then F_1 generates a function of genus $n-1$.*

We are now in the position to establish theorem 1. By lemmas 1.4, 1.2 and 1.3, F generates a function of genus 2. Hence, by lemma 1.5, F generates a function of genus $n-1$. Using lemmas 1.2 and 1.3 we see that F generates all 1-place functions which assume at most $n-1$ values. According to a completeness criterion in [1], if $n \geqq 3$ then a set containing all 1-place functions which assume at most $n-1$ values and, in addition, some function satisfying Słupecki conditions is complete. Hence, theorem 1 follows.

2. We shall now apply theorem 1 to the proof of a conjecture presented in [2].

We say that a function is a *Sheffer function* if its unit set is complete. Conjecture 1 presented in [2] is a special case ($k = 2$) of the following

THEOREM 2. *A function $f(x_1, \ldots, x_k)$ which generates the alternating group A_n is a Sheffer function, provided $n \geqq 4$.*

Theorem 2 is a consequence of theorem 1 if $n \geqq 5$. For if a function generates A_n then it obviously satisfies Słupecki conditions. Theorem 1 is not valid if $n = 4$. Hence, in this case, we have to use a different method in order to complete the proof of theorem 2. (The condition $n \geqq 4$ in the statement of theorem 2 is essential because, for $n < 4$, A_n is cyclic.)

We say that a function $g(x_1, \ldots, x_l)$ is *self-conjugate* under a permutation $p(x)$ if

$$p(g(x_1, \ldots, x_l)) = g(p(x_1), \ldots, p(x_l)).$$

It is easy to see that a function self-conjugate under $p(x)$ can generate only functions self-conjugate under $p(x)$. (Cf. [1] or [2].)

We prove first the following

LEMMA 2.1. *Assume that $n = 4$ and $g(x_1, \ldots, x_l)$ has both of the following properties:*

(i) *$g(x, \ldots, x) = p(x)$ is a non-identical permutation belonging to the four group.*

(ii) *Denote by H_4 the set consisting of all even permutations and of all constants. Then $g(h_1(x), \ldots, h_l(x))$ belongs to H_4 whenever each $h_i(x)$, $i = 1, \ldots, l$, belongs to H_4.*

Under these assumptions, $g(x_1, \ldots, x_l)$ is self-conjugate under $p(x)$.

Proof. It is readily seen that the lemma holds true for $l = 2$. In this case, namely, there are only 12 functions satisfying (i) and (ii). It is easily checked that each of these functions satisfies also the conclusion of the lemma.

Suppose that $l = 3$ and $g(x_1, x_2, x_3)$ satisfies (i) and (ii) but is not self-conjugate under $p(x)$. Hence, there are numbers a_1, a_2, a_3 such that

$$p(g(a_1, a_2, a_3)) \neq g(p(a_1), p(a_2), p(a_3)). \tag{2}$$

We may assume that the numbers a_i are distinct because, otherwise, we could conclude by identifying some variables in g that the lemma does not hold for $l = 2$. By a suitable renumbering of the variables, we obtain the equation $p(a_1) = a_2$. Since p belongs to the four group, the numbers $a_1, a_2, a_3, p(a_3)$ are the numbers $1, 2, 3, 4$ in some order. Let $c_1(x)$ be the 3-cycle $(a_2 a_3 p(a_3))$ and $c_2(x)$ the 3-cycle $(a_1 a_3 a_2)$. According to (ii), the following functions $c_3(x)$ and $c_4(x)$ belong to H_4:

$$c_3(x) = g(a_1, x, c_1(x))$$

and

$$c_4(x) = g(x, c_2(x), p(a_3)).$$

Using our hypothesis (i) and the definitions of the functions $c_i(x)$, we obtain the following equations:

$$c_3(a_1) = a_2,$$
$$c_3(a_2) = g(a_1, a_2, a_3),$$
$$c_3(a_3) = c_4(a_1),$$
$$c_4(p(a_3)) = a_3$$

and

$$c_4(a_2) = g(p(a_1), p(a_2), p(a_3)).$$

There are only four possibilities for the number $g(a_1, a_2, a_3)$. In each case it is easy to verify that (2) is false, provided c_3 and c_4 belong to H_4. This is a contradiction which proves our lemma for $l = 3$. The proof for the case $l = 4$ is similar.

We now make the following inductive hypothesis: the lemma holds true for $l < m$ where $m \geqq 5$. Let $g(x_1, \ldots, x_m)$ be an arbitrary function satisfying (i) and (ii). Suppose there are numbers $b_1, \ldots, b_m$ such that

$$p(g(b_1, \ldots, b_m)) \neq g(p(b_1), \ldots, p(b_m)).$$

At least two of the numbers b_i are equal because $m \geqq 5$. By identifying the corresponding variables in g, we obtain a function g_1 of at most $m-1$ variables. Obviously, g_1 satisfies (i) and (ii) but is not self-conjugate under p. This is impossible by the inductive hypothesis and, therefore, we have completed the proof of lemma 2.1.

We now prove theorem 2 for the case $n = 4$. By lemma 1.4, $f(x_1, \ldots, x_k)$ generates a function of genus smaller than n. Since f generates the alternating group, we obtain the inequality

$$f(x, \ldots, x) \neq x, \text{ for any } x. \tag{3}$$

We claim that f generates a function of one of the types $[3, 1]$, $[2, 2]$ or $[2, 1, 1]$. Assume the contrary, i.e. that f generates only permutations and constants. Then by (3), the function $f_1(x) = f(x, \ldots, x)$ is either a 4-cycle or a non-identical permutation belonging to the four group. In the former case, f generates all permutations and, therefore, by the remark made at the end of the proof of lemma 1.4, it generates also a function of genus 2 or 3, i.e. a function of one of the types mentioned. In the latter case, f is self-conjugate under f_1 by lemma 2.1 and, hence, cannot generate A_4.

If f generates a function of type $[3, 1]$ or $[2, 1, 1]$ then theorem 2 follows, by lemmas 1.5, 1.2 and 1.3 and by the completeness criterion mentioned at the end of section 1.

There remains the possibility that f generates a function of type $[2, 2]$. Hence, by lemmas 1.2 and 1.3, it generates all functions of this type and all constants. By lemma 1.1, there are numbers a_i^j where $i = 1, \dots, k$ and $j = 1, 2, 3$ such that

$$f(a_1^1, \dots, a_k^1),\ f(a_1^2, \dots, a_k^2) \text{ and } f(a_1^3, \dots, a_k^3)$$

are distinct but, for any i, at most two of the numbers a_i^j are distinct. It is possible to choose 1-place functions $u_i(x)$, $i = 1, \dots, k$, of type $[2, 2]$ or $[4]$ such that

$$u_i(j) = a_i^j\,, \text{ for } j = 1, 2, 3.$$

Hence, f generates the function

$$u(x) = f(u_1(x), \dots, u_k(x)).$$

The function $u(x)$ assumes at least three distinct values. If it is not a permutation we have completed the proof. If $u(x)$ is a permutation we may conclude that f generates all permutations. For if $u(x)$ is even we obtain an odd permutation by interchanging in the definition of each $u_i(x)$ the values $u_i(1)$ and $u_i(2)$.

Suppose f does not generate any 1-place functions other than the functions of types $[1, 1, 1, 1]$, $[2, 2]$ and $[4]$. This implies that $f(x, \dots, x)$ is self-conjugate under a non-identical permutation $p(x)$ belonging to the four group. Choose an arbitrary assignment of values $(y_1, \dots, y_k)$ for the variables of f. Define functions $v_i(x)$, $i = 1, \dots, k$, as follows:

$$v_i(1) = y_1,\ v_i(2) = p(y_1),\ v_i(3) = y_i,\ v_i(4) = p(y_i).$$

The functions $v_i(x)$ are of type $[1, 1, 1, 1]$ or $[2, 2]$. Therefore, according to our supposition, the function

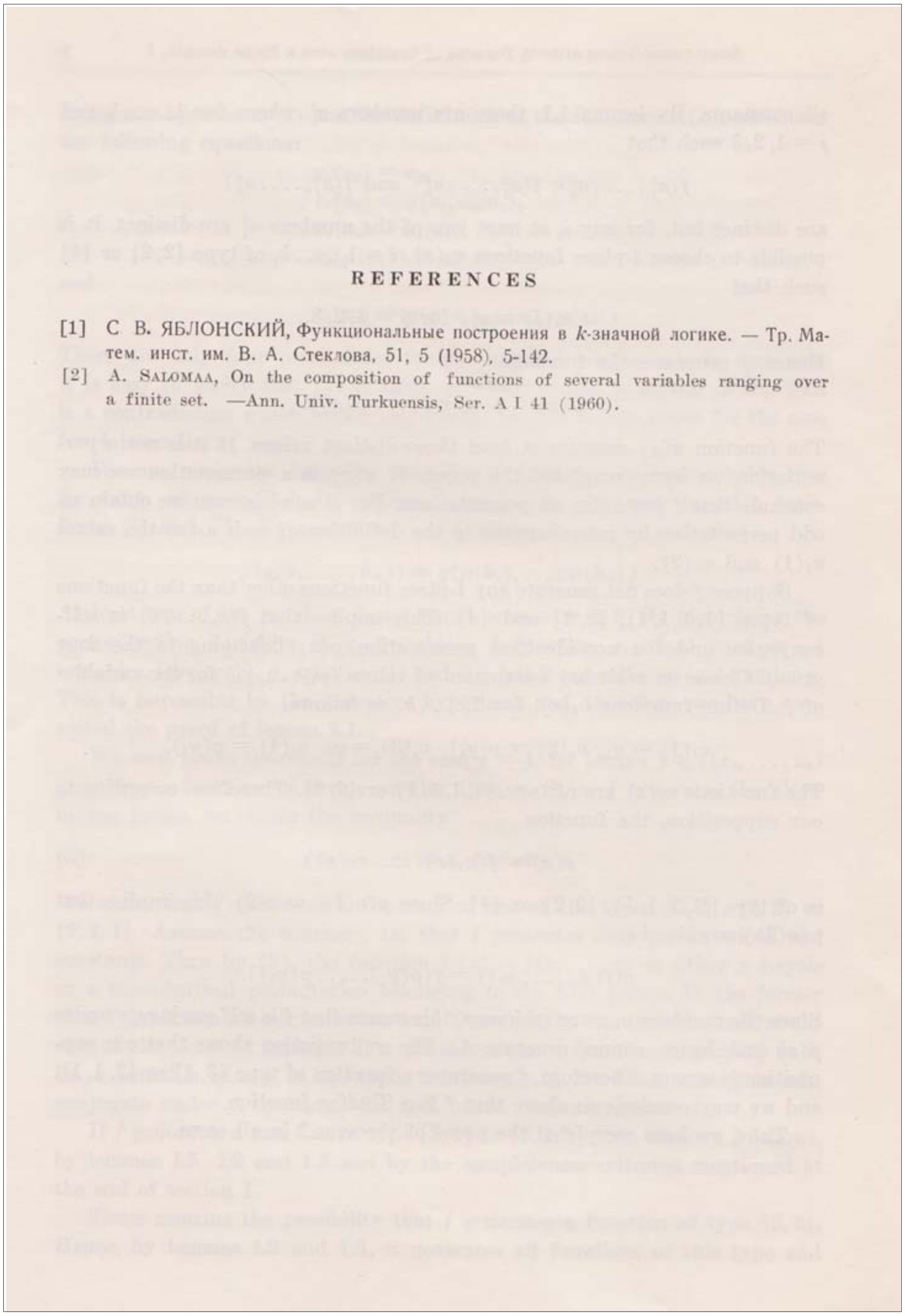
$$v(x) = f(v_1(x), \dots, v_k(x))$$

is of type $[1, 1, 1, 1]$, $[2, 2]$ or $[4]$. Since $p(v(1)) = v(2)$, this implies that $p(v(3)) = v(4)$, i.e.

$$p(f(y_1, \dots, y_k)) = f(p(y_1), \dots, p(y_k)).$$

Since the numbers y_i were arbitrary, this means that f is self-conjugate under $p(x)$ and, hence, cannot generate A_4. The contradiction shows that our supposition is wrong. Therefore, f generates a function of type $[3, 1]$ or $[2, 1, 1]$, and we may conclude as above that f is a Sheffer function.

Thus, we have completed the proof of theorem 2 in all cases.



REFERENCES

[1] С В. ЯБЛОНСКИЙ, Функциональные построения в *k*-значной логике. — Тр. Матем. инст. им. В. А. Стеклова, 51, 5 (1958), 5-142.

[2] A. Salomaa, On the composition of functions of several variables ranging over a finite set. —Ann. Univ. Turkuensis, Ser. A I 41 (1960).

Some Analogues of Sheffer Functions in Infinite-Valued Logics

Arto Salomaa

1. Let E_ω be the set of functions mapping some finite Cartesian power of the set of natural numbers into the set of natural numbers. Let E_n, $n \geqq 2$, be the set of functions mapping some finite Cartesian power of the set

$$N(n) = \{1, \ldots, n\}$$

into $N(n)$. Each of the sets E is closed under composition. We may generate new functions from some given functions by composing our original functions in various ways. A function belonging to the set E_n is termed a *Sheffer function* if it generates all functions in E_n.[1] It is well-known that there are Sheffer functions in each of the sets E_n. Since E_ω is non-denumerable, it is also clear that there are no Sheffer functions in the set E_ω. In fact, no denumerable subset of E_ω generates all functions in E_ω.

Consider an arbitrary finite or denumerable subset S of E_ω. A function $f \in E_\omega$ is termed a *Sheffer function of the set S* if f generates all functions in S. In this paper, we are first going to show how one can construct a 2-place Sheffer function $f_S(x, y)$ of an arbitrary preassigned S. The method of construction yields, for any S, a continuum of 2-place Sheffer functions $f_S(x, y)$.[2] We shall then prove a theorem concerning the infinite-valued logic of Łukasiewicz. Finally, we shall discuss some decision procedures for the property of being a Sheffer function.

[1] For a more detailed account, cf. [5].

[2] A 3-place Sheffer function of S, for any S, has been constructed in [1]. It is also mentioned in [1] that the number of variables can be reduced to two. The latter result is credited to O. B. Lupanov.

2. We shall establish a 1-to-1 correspondence between 2-place and 1-place functions belonging to E_ω. Let $\varphi(x, y) \in E_\omega$ be defined as follows:

$$\varphi(x, y) = \frac{(x + y - 1)\ (x + y - 2)}{2} + x.$$

It is seen that $\varphi(x, y)$ assumes every natural number as a value exactly once. Therefore, the equation

$$f_2(x, y) = f_1(\varphi(x, y))$$

defines a 1-to-1 correspondence between 2-place functions f_2 and 1-place functions f_1.

Consider the following compositions of φ:

$$\varphi_2(x_1, x_2) = \varphi(x_1, x_2),$$
$$\varphi_i(x_1, \ldots, x_i) = \varphi(\varphi_{i-1}(x_1, \ldots, x_{i-1}), x_i) \text{ for } i \geqq 3.$$

Every function φ_i assumes all natural numbers as values and each value exactly once. Therefore, a 1-to-1 correspondence between i-place and 1-place functions in E_ω can be established by using the function φ_i.

We shall now prove the following

THEOREM 1. *For any two functions*

$$g(x_1, \ldots, x_k),\ h(x_1, \ldots, x_l) \in E_\omega,$$

there is a single 2-place function $f(x, y) \in E_\omega$ which generates both g and h.

Proof. Let $g_1(x)$ and $h_1(x)$ be the 1-place functions corresponding to the functions g and h. By the definition of this correspondence, the functions g_1, h_1 and φ generate our original functions g and h. Hence, to prove theorem 1, it suffices to construct a 2-place function $f(x, y)$ which generates the three functions g_1, h_1 and φ. Such a function $f(x, y)$ can be defined as follows:

$$f(x, x) = x + 1 \qquad \text{for } 1 \leqq x \leqq 4,$$
$$f(x, x) = 1 \qquad \text{for } x \geqq 5;$$
$$f(x, f_1(x)) = g_1(x) \qquad \text{where } f_1(x) = f(x, x),$$

$$\begin{aligned}
&f(x, f_1^2(x)) = h_1(x),\\
&f(x, f_1^3(x)) = 2x + 5,\\
&f(x, f_1^4(x)) = 2x + 4;\\
&f(2x + 5, 2y + 4) = \varphi(x, y);\\
&f(x, y) = 1 \quad \text{otherwise.}
\end{aligned}$$

No contradiction arises in this definition, i.e. there is no argument (x, y) such that the value of $f(x, y)$ has been given twice. This is seen as follows. For any x, the numbers x, $f_1(x)$, $f_1^2(x)$, $f_1^3(x)$ and $f_1^4(x)$ are distinct. This implies that all arguments of f appearing on the first six lines of the definition are distinct. Since always $f_1(x) \leqq 5$, we may conclude that the pair $(2x + 5, 2y + 4)$ is distinct from all pairs of the form $(z, f_1^i(z))$, $i = 1, \ldots, 4$. Finally, because $2x + 5$ is always odd and $2y + 4$ is always even we see that the pair $(2x + 5, 2y + 4)$ is also distinct from all pairs (z, z).

It is an immediate consequence of the definition of the function f that f generates the functions g_1, h_1 and φ. This completes the proof of theorem 1.

Consider the matrix of the function $f(x, y)$. The functions g_1 and h_1, as well as the auxiliary functions $2x + 5$ and $2x + 4$ are obtained from the first five columns of the matrix. If we use other parts of the matrix in order to generate the required 1-place functions, we obtain alternative methods to construct 2-place functions generating g_1, h_1 and φ. For instance, also the following function $f'(x, y)$ generates the functions g_1, h_1 and φ:

$$\begin{aligned}
&f'(x, x) = x + 1,\\
&f'(x, x + 1) = g_1(x),\\
&f'(x + 1, x) = h_1(x),\\
&f'(x, x + 2) = 6x,\\
&f'(x + 2, x) = 6x + 3,\\
&f'(6x, 6y + 3) = \varphi(x, y),\\
&f'(x, y) = 1 \ \text{otherwise.}
\end{aligned}$$

As an illustration, we choose

$$g(x, y) = x + y$$

and

$$h(x, y) = xy.$$

Then, for $x, y \leqq 15$, the values of the function $f'(x, y)$ are as follows:

y x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	2	6												
2	1	3	3	12											
3	9	2	4	3	18										
4		15	2	5	4	24									
5			21	3	6	4	30								
6				27	4	7	4	36	1						2
7					33	3	8	5	42						
8						39	4	9	5	48					
9							45	6	10	5	54				
10								51	6	11	5	60			
11									57	4	12	6	66		
12									3	63	5	13	6	72	5
13											69	8	14	6	78
14												75	9	15	6
15													81	8	16

According to the definition of $f'(x, y)$, number 1 occurs in the blank entries. However, the values in these entries may be chosen arbitrarily. They are not needed for the construction of the functions g_1, h_1 and φ.

The existence of 2-place Sheffer functions of any preassigned at most denumerable subset of E_ω is guaranteed by the following

Theorem 2. *Assume S is an at most denumerable subset of E_ω. Then there is a continuum of 2-place Sheffer functions $f_S(x, y)$ of S.*

Proof. Let

$$g_i(x),\ i = 1, 2, \ldots$$

be the 1-place functions corresponding to the functions in S. By the definition of this correspondence, every function in S is generated by the functions $g_i(x)$ and $\varphi(x, y)$. Thus, every function $f_S(x, y)$ which generates the functions $g_i(x)$ and $\varphi(x, y)$ is a Sheffer function of S.

Denote by $h(x, y)$ any function in E_ω such that

$$h(x, x) = x + 1,$$
$$h(x, x + i) = g_i(x) \text{ for } i = 1, 2, \ldots.$$

There is a continuum of such functions $h(x, y)$. Each function $h(x, y)$ generates all functions $g_i(x)$. Hence, every function $f_S(x, y)$ which generates $\varphi(x, y)$ and some $h(x, y)$ is a Sheffer function of S.

For any function h, the existence of a function $f_S(x, y)$ which generates both φ and h is guaranteed by theorem 1. Clearly, for different functions h, the corresponding functions f_S may be chosen to be different. Hence, theorem 2 follows.

If we use a result of Sierpiński we may simplify the definition of the functions h. According to [6], any sequence of 1-place functions in E_ω can be generated by two 1-place functions in E_ω. Hence, we may generate all functions $g_i(x)$ by two functions $g'(x)$ and $g''(x)$. Then we may choose $h(x, y)$ to be any function such that

$$\begin{aligned} h(x, x) &= x + 1, \\ h(x, x+1) &= g'(x), \\ h(x+1, x) &= g''(x). \end{aligned}$$

According to theorem 2, there is a 1-to-1 correspondence between the whole set E_ω and the set of Sheffer functions $f_S(x, y)$. If one studies Sheffer functions of the set E_n one is likely to agree that there are surprisingly many Sheffer functions. Theorem 2 corresponds to this fact in connection with the set E_ω.

3. It is natural in view of the results obtained in [1] and [2] that, for some sets S, no Sheffer function of S is contained in S itself. This is the case if S is the set of truth-functions in the infinite-valued logic of Łukasiewicz.

Theorem 3. *Let S_L be the (denumerable) set generated by the truth-functions $t_N(x)$ and $t_C(x, y)$ corresponding to negation N and implication C in the infinite-valued logic of Łukasiewicz. Then no function in S_L is a Sheffer function of S_L.*

Proof. Let $f(x_1, \ldots, x_k)$ be a Sheffer function of S_L. Then the function

$$f_1(x) = f(x, \ldots, x),$$

called the *main diagonal* of f, has no fixed-points. Fixed-points are preserved under compositions. And there is no number x such that

$$t_N(x) = t_C(x, x) = x.$$

Let $g(x_1, \ldots, x_l)$ be an arbitrary function in the set S_L. Then the main diagonal of g possesses at least one fixed-point.[1] Thus, we have completed the proof of theorem 3.

[1] For the proof of this result, cf. [7]. In connection with this proof it is convenient to change our notation in such a manner that (instead of natural numbers) rational numbers in the closed interval (0,1) are considered as truth-values.

For the finitely many-valued logics of Łukasiewicz, the statement corresponding to theorem 3 is not valid. Let $S_L^{(n)}$ be the set generated by the truth-functions corresponding to implication and negation in the many-valued logic of Łukasiewicz with n truth-values. It is a result due to McKINSEY [4] that there is a function in $S_L^{(n)}$ which generates all functions in $S_L^{(n)}$.

4. We shall finally discuss some algorithms for finding out whether a given function is a Sheffer function. Consider the following decision problem: given an arbitrary at most denumerable subset S of E_ω and an arbitrary function $f \in E_\omega$, is there a method of deciding whether f is a Sheffer function of S?[1] The answer is negative. In fact, this problem is unsolvable even in the following most simple form:

(D). To decide of two given 1-place functions belonging to E_ω whether one of them generates the other.

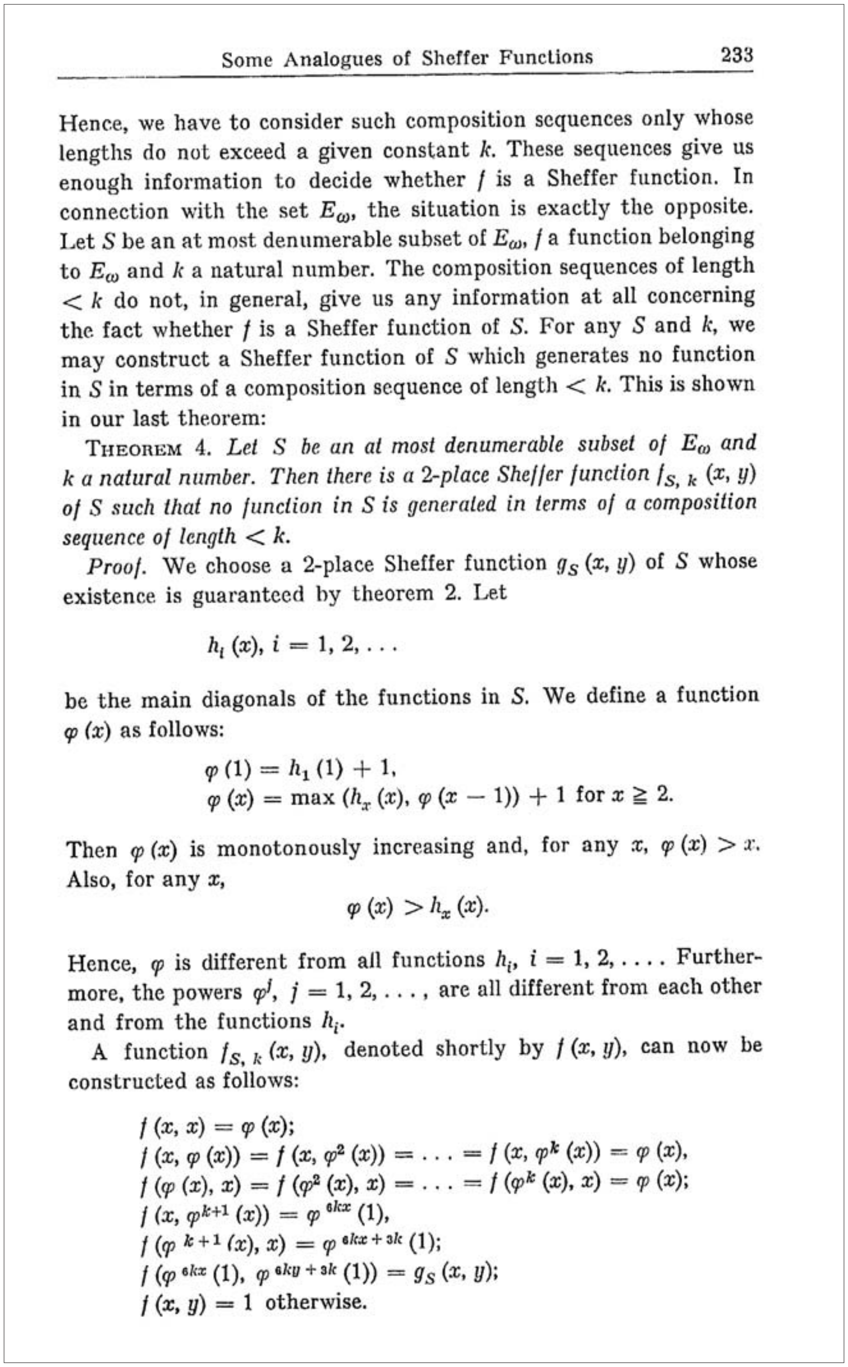
(D) is easily reduced to some unsolvable case of the word problem. Consider an arbitrary Thue system T over a finite alphabet. Enumerate the equations of T, beginning with the number 2. Given two words α and β, we define a function $\psi_1(x) \in E_\omega$ as follows: $\psi_1(x) = 1$ if x is not the number of the equation $\alpha = \beta$. If x is the number of this equation then $\psi_1(x) = x$. Let $\psi_2(x)$ be the function assuming the value 1, for all x. Then ψ_1 generates ψ_2 if and only if the equation $\alpha = \beta$ does not hold. Hence, if (D) is solvable then also the word problem of T possesses a solution. However, T may be chosen in such a manner that its word problem is unsolvable.[2] Therefore, (D) is unsolvable.

The corresponding decision problem for sets E_n possesses a solution. Assume $f \in E_n$. To decide whether f is a Sheffer function, we form all composition sequences with only one variable and with length $\leqq n^n$. The function f is a Sheffer function if and only if all 1-place functions in E_n are among these composition sequences.[3]

[1] We use the expression »a function is given» to mean that, for any argument, the value of the function can be computed in finitely many steps.

[2] We may choose the Thue system of the universal Turing machine. Cf. [3, pp. 147—157]. Similarly, (D) can be reduced to the word problem for groups.

[3] For a more detailed account, cf. [5]. The notion of the length of a composition sequence in terms of f is defined as follows: A variable alone constitutes a composition sequence of length 0. If f is applied to composition sequences which are of length $\leqq i$ and one of which is of length i, the resulting composition sequence is of length $i + 1$.



Hence, we have to consider such composition sequences only whose lengths do not exceed a given constant k. These sequences give us enough information to decide whether f is a Sheffer function. In connection with the set E_ω, the situation is exactly the opposite. Let S be an at most denumerable subset of E_ω, f a function belonging to E_ω and k a natural number. The composition sequences of length $< k$ do not, in general, give us any information at all concerning the fact whether f is a Sheffer function of S. For any S and k, we may construct a Sheffer function of S which generates no function in S in terms of a composition sequence of length $< k$. This is shown in our last theorem:

Theorem 4. *Let S be an at most denumerable subset of E_ω and k a natural number. Then there is a 2-place Sheffer function $f_{S,\,k}(x, y)$ of S such that no function in S is generated in terms of a composition sequence of length $< k$.*

Proof. We choose a 2-place Sheffer function $g_S(x, y)$ of S whose existence is guaranteed by theorem 2. Let

$$h_i(x),\ i = 1, 2, \dots$$

be the main diagonals of the functions in S. We define a function $\varphi(x)$ as follows:

$$\begin{aligned}&\varphi(1) = h_1(1) + 1,\\ &\varphi(x) = \max(h_x(x), \varphi(x-1)) + 1 \text{ for } x \geqq 2.\end{aligned}$$

Then $\varphi(x)$ is monotonously increasing and, for any x, $\varphi(x) > x$. Also, for any x,

$$\varphi(x) > h_x(x).$$

Hence, φ is different from all functions h_i, $i = 1, 2, \dots$. Furthermore, the powers φ^j, $j = 1, 2, \dots$, are all different from each other and from the functions h_i.

A function $f_{S,\,k}(x, y)$, denoted shortly by $f(x, y)$, can now be constructed as follows:

$$\begin{aligned}&f(x, x) = \varphi(x);\\ &f(x, \varphi(x)) = f(x, \varphi^2(x)) = \dots = f(x, \varphi^k(x)) = \varphi(x),\\ &f(\varphi(x), x) = f(\varphi^2(x), x) = \dots = f(\varphi^k(x), x) = \varphi(x);\\ &f(x, \varphi^{k+1}(x)) = \varphi^{6kx}(1),\\ &f(\varphi^{k+1}(x), x) = \varphi^{6kx+3k}(1);\\ &f(\varphi^{6kx}(1), \varphi^{6ky+3k}(1)) = g_S(x, y);\\ &f(x, y) = 1 \text{ otherwise.}\end{aligned}$$

We have to show, first, that there is no pair (x, y) such that the value of $f(x, y)$ has been given twice. For the first five lines of the definition, this is an immediate consequence of the properties of the function φ. Assume that, for some x, y and z,

$$(\varphi^{6kx}(1),\ \varphi^{6ky+3k}(1)) = (\varphi^{i}(z), z)$$

where $0 \leqq i \leqq k+1$. We obtain first

$$\varphi^{6kx+i}(1) = \varphi^{6ky+3k}(1)$$

and hence, by the definition of the function φ,

$$6\,kx + i = 6\,ky + 3\,k$$

or

$$i = 3\,k + 6\,k\,(y - x).$$

This is impossible because $0 \leqq i \leqq k+1$. Similarly, we can show that the equation

$$(\varphi^{6kx}(1),\ \varphi^{6ky+3k}(1)) = (z,\ \varphi^{i}(z))$$

is impossible for $0 \leqq i \leqq k+1$. Hence, the value of $f(x, y)$ has not been given twice for any pair (x, y).

The function $f(x, y)$ is a Sheffer function of S because it generates the function $g_S(x, y)$. Assume some composition sequence of f which is of length $< k$ is a function belonging to the set S. Then its main diagonal is one of the functions h_i. But according to the definition of f, its main diagonal is a power of the function φ. This is impossible. Hence, $f(x, y)$ satisfies all requirements and we have completed the proof of theorem 4. It is easy to see that a continuum of functions $f_{S,\,k}(x, y)$ can be obtained.

Theorem 4 gives an example of the rich possibilities of functional constructions in the set E_ω.

University of Turku.

References

[1] S. V. Áblonskij. *O nékotoryh svojstvah sčétnyh zamknutyh klassov iz $P_{\aleph_0}$.* **Doklady Akademii Nauk SSSR,** vol. 124 (1959), pp. 990—993.

[2] Ú. I. Ánov and A. A. Mučnik. *O suščéstvovanii k-značnyh zamknutyh klassov né iméúščih konéčnogo bazisa.* **Ibid.,** vol. 127 (1959), pp. 44—46.

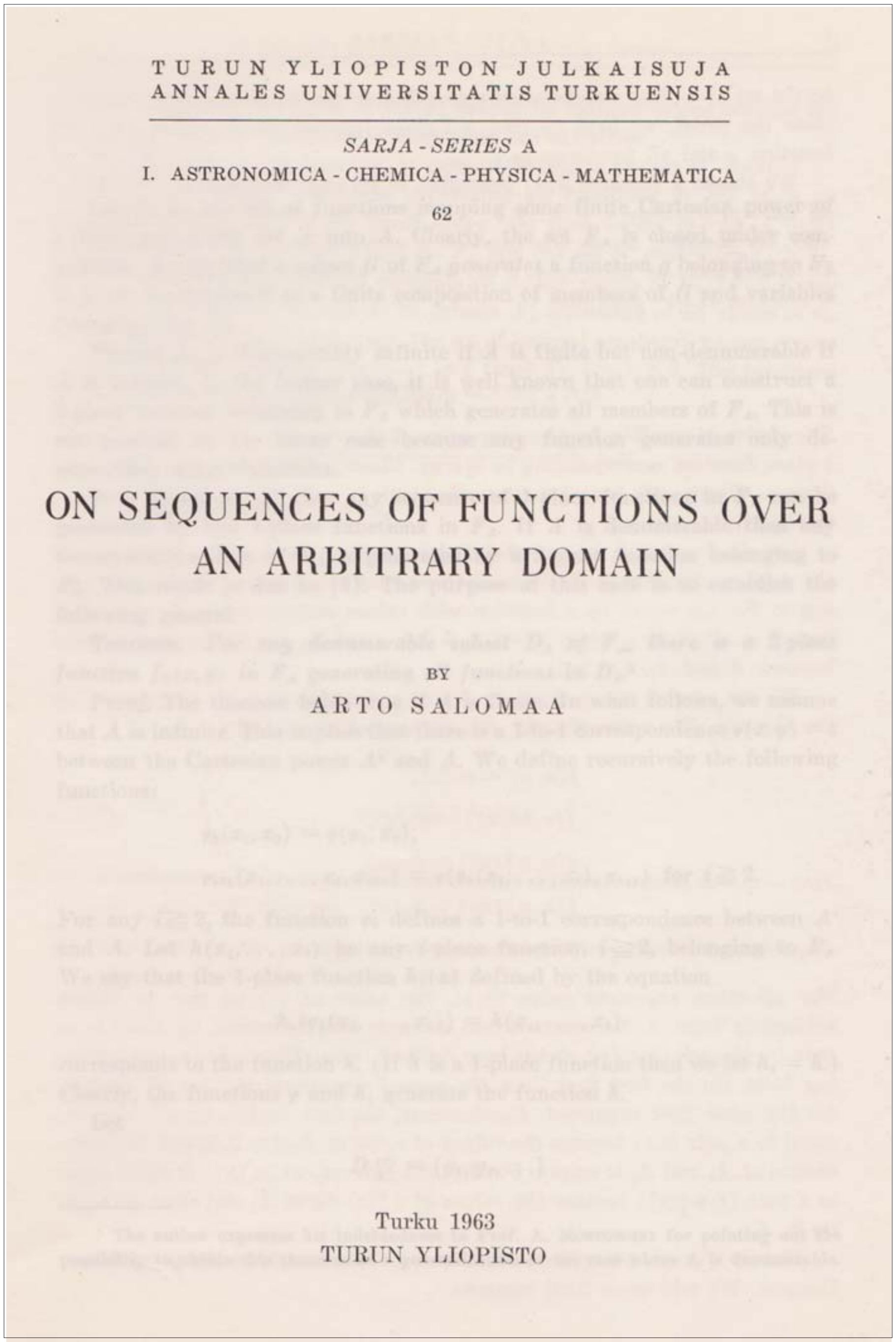
[3] H. Hermes. **Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit.** Springer, Berlin 1961, x + 246 pp.

[4] J. C. C. McKinsey. *On the generation of the functions Cpq and Np of Łukasiewicz and Tarski by means of a single binary operation.* **Bulletin of the American Mathematical Society,** vol. 42 (1936), pp. 849—851.

[5] Arto Salomaa. *On the composition of functions of several variables ranging over a finite set.* **Annales Universitatis Turkuensis,** Series AI, vol. 41, Turun Yliopisto, Turku 1960, 48 pp.

[6] W. Sierpiński. *Sur les suites infinies de fonctions définies dans les ensembles quelconques.* **Fundamenta mathematicae,** vol. 24 (1935), pp. 209—212.

[7] Thoralf Skolem. *Bemerkungen zum Komprehensionsaxiom.* **Zeitschrift für mathematische Logik und Grundlagen der Mathematik,** vol. 3 (1957), pp. 1—17.



TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

SARJA - SERIES A
I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA
62

ON SEQUENCES OF FUNCTIONS OVER AN ARBITRARY DOMAIN

BY
ARTO SALOMAA

Turku 1963
TURUN YLIOPISTO

Let F_A be the set of functions mapping some finite Cartesian power of a fixed non-empty set A into A. Clearly, the set F_A is closed under composition. We say that a subset G of F_A *generates* a function g belonging to F_A if g can be expressed as a finite composition of members of G and variables (ranging over A).

The set F_A is denumerably infinite if A is finite but non-denumerable if A is infinite. In the former case, it is well known that one can construct a 2-place function belonging to F_A which generates all members of F_A. This is not possible in the latter case because any function generates only denumerably many functions.

It is shown in [2] that any sequence of 1-place functions in F_A can be generated by two 1-place functions in F_A. If A is denumerable then any denumerable subset of F_A is generated by a 3-place function belonging to F_A. This result is due to [1]. The purpose of this note is to establish the following general

THEOREM. *For any denumerable subset D_A of F_A, there is a 2-place function $f_D(x,y)$ in F_A generating all functions in D_A.*[1]

Proof. The theorem holds true if A is finite. In what follows, we assume that A is infinite. This implies that there is a 1-to-1 correspondence $\varphi(x,y) = z$ between the Cartesian power A^2 and A. We define recursively the following functions:

$$\varphi_2(x_1, x_2) = \varphi(x_1, x_2),$$

$$\varphi_{i+1}(x_1, \dots, x_i, x_{i+1}) = \varphi(\varphi_i(x_1, \dots, x_i), x_{i+1}) \text{ for } i \geqq 2.$$

For any $i \geqq 2$, the function φ_i defines a 1-to-1 correspondence between A^i and A. Let $h(x_1, \dots, x_i)$ be any i-place function, $i \geqq 2$, belonging to F_A. We say that the 1-place function $h_1(x)$ defined by the equation

$$h_1(\varphi_i(x_1, \dots, x_i)) = h(x_1, \dots, x_i)$$

corresponds to the function h. (If h is a 1-place function then we let $h_1 = h$.) Clearly, the functions φ and h_1 generate the function h.

Let

$$D_A^{(1)} = \{g_1, g_2, \dots\}$$

[1] The author expresses his indebtedness to Prof. A. MOSTOWSKI for pointing out the possibility to obtain this theorem as a generalization of the case where A is denumerable.

be the set of 1-place functions corresponding to the functions in D_A. To complete the proof, we have to find a 2-place function in F_A, generating the function φ and all functions g_i.

We choose a function $\psi(x)$ belonging to F_A such that, for all x in A and all natural numbers i, $\psi^i(x) \neq x$. (If "$<$" is an ordering relation then we may, for instance, choose any function ψ such that $x < \psi(x)$, for all x in A.) It follows that, for all x in A, $\psi^i(x) \neq \psi^j(x)$ whenever $i \neq j$. We choose next a function $k(x,y)$ such that

$$k(x,x) = \psi(x),$$
$$k(x, \psi^i(x)) = g_i(x), \quad i = 1, 2, \ldots .$$

The choice is possible, by the properties of the function ψ. Let $k_1(x)$ be the 1-place function corresponding to $k(x,y)$. Clearly, $k(x,y)$ generates all functions g_i. Hence, any function generating both k_1 and φ generates all functions in D_A.

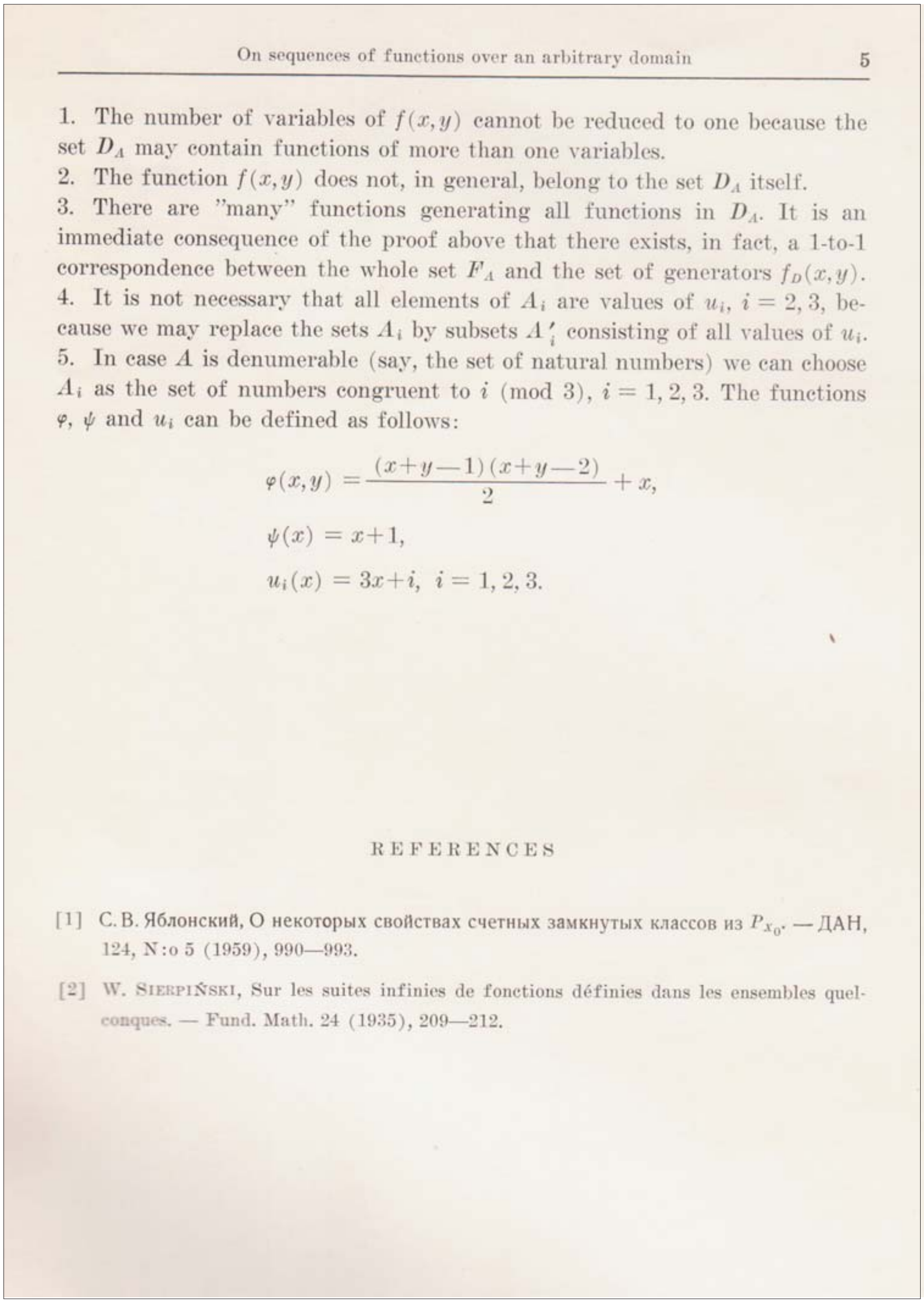
Let A_i, $i = 1, 2, 3$, be pairwise disjoint subsets of A, each of which is of the same cardinality as A. We need three auxiliary 1-place functions belonging to F_A. Let $u_1(x)$ be a function with values exclusively in A_1 such that, for all x, $u_1^i(x) \neq x$ where $i = 1, 2, 3$. Let $u_i(x)$ be a 1-to-1 correspondence between A and A_i, $i = 2, 3$.

We are now in the position to define a function $f_D(x,y)$ as required in the theorem. We write, shortly, $f(x,y)$ instead of $f_D(x,y)$:

$$\begin{aligned} f(x,x) &= u_1(x), \\ f(x, u_1(x)) &= u_2(x), \\ f(x, u_1^2(x)) &= u_3(x), \\ f(x, u_1^3(x)) &= k_1(x), \\ f(u_2(x), u_3(y)) &= \varphi(x,y). \end{aligned}$$

For all other argument pairs (x,y), the value of $f(x,y)$ may be chosen arbitrarily from A. No contradiction arises in this definition, i.e. there is no pair (x,y) such that $f(x,y)$ has been defined twice. This is due to the following facts. On the first four lines, the second arguments of f are all distinct, for the same first argument. Furthermore, the pair $(u_2(x), u_3(y))$ is never equal to a pair (z,z) because the values of u_i lie in A_i, $i = 2, 3$, and the intersection of A_2 and A_3 is empty. Finally, the pair $(u_2(x), u_3(y))$ is never equal to a pair $(z, u_1^i(z))$ because the values of $u_1^i(z)$ lie in A_1 and those of $u_3(y)$ lie in A_3.

Clearly, $f(x,y)$ generates both k_1 and φ. This completes the proof of our theorem. We add some final remarks.



1. The number of variables of $f(x,y)$ cannot be reduced to one because the set D_A may contain functions of more than one variables.
2. The function $f(x,y)$ does not, in general, belong to the set D_A itself.
3. There are "many" functions generating all functions in D_A. It is an immediate consequence of the proof above that there exists, in fact, a 1-to-1 correspondence between the whole set F_A and the set of generators $f_D(x,y)$.
4. It is not necessary that all elements of A_i are values of u_i, $i=2,3$, because we may replace the sets A_i by subsets A'_i consisting of all values of u_i.
5. In case A is denumerable (say, the set of natural numbers) we can choose A_i as the set of numbers congruent to i (mod 3), $i=1,2,3$. The functions φ, ψ and u_i can be defined as follows:

$$\varphi(x,y) = \frac{(x+y-1)(x+y-2)}{2} + x,$$

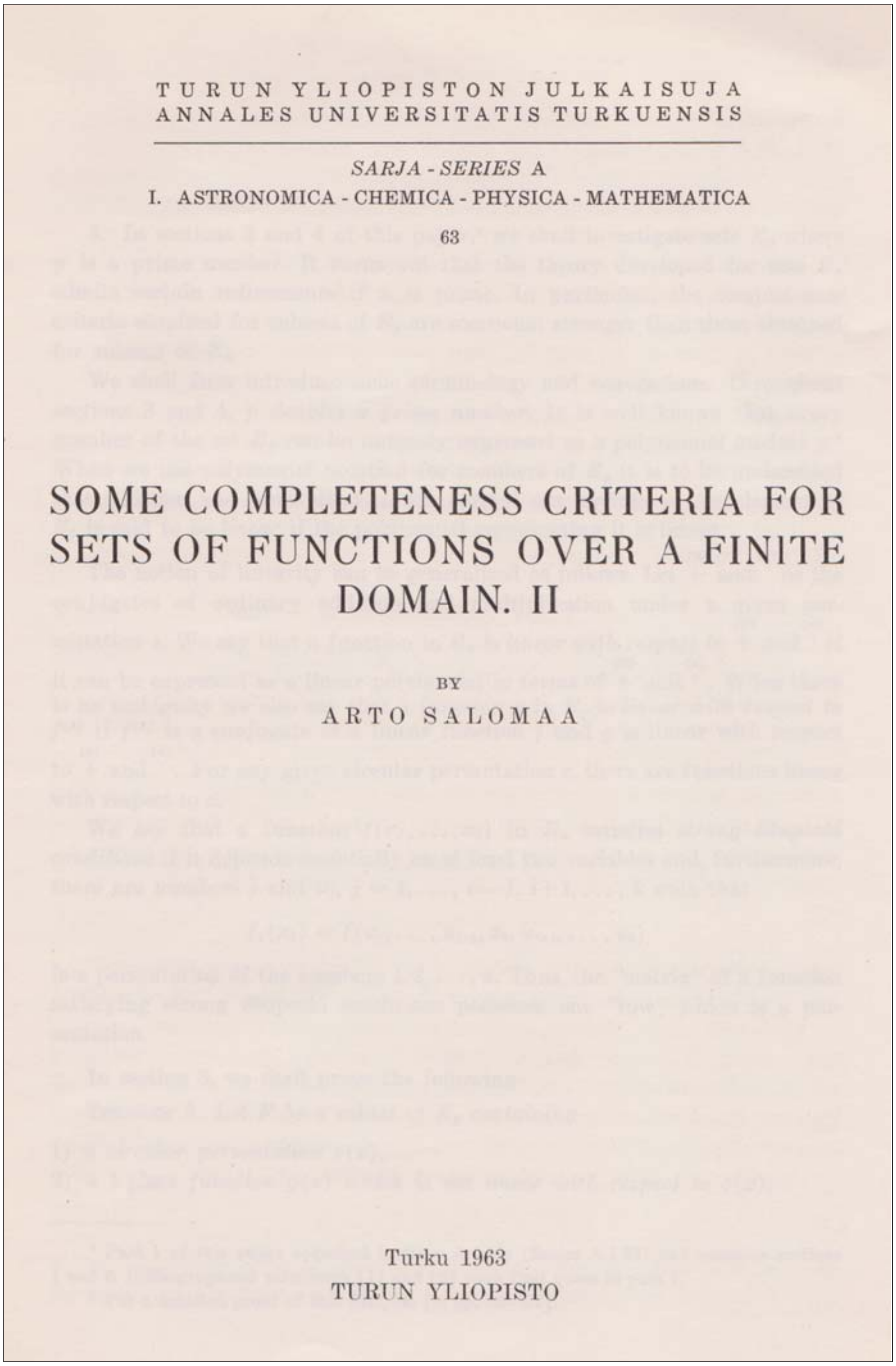
$$\psi(x) = x+1,$$

$$u_i(x) = 3x+i, \;\; i = 1,2,3.$$

REFERENCES

[1] С. В. Яблонский, О некоторых свойствах счетных замкнутых классов из P_{X_0}. — ДАН, 124, N:o 5 (1959), 990—993.

[2] W. Sierpiński, Sur les suites infinies de fonctions définies dans les ensembles quelconques. — Fund. Math. 24 (1935), 209—212.



TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

SARJA - SERIES A
I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA
63

SOME COMPLETENESS CRITERIA FOR SETS OF FUNCTIONS OVER A FINITE DOMAIN. II

BY
ARTO SALOMAA

Turku 1963
TURUN YLIOPISTO

3. In sections 3 and 4 of this paper,[1] we shall investigate sets E_p where p is a prime number. It turns out that the theory developed for sets E_n admits certain refinements if n is prime. In particular, the completeness criteria obtained for subsets of E_p are somewhat stronger than those obtained for subsets of E_n.

We shall first introduce some terminology and conventions. Throughout sections 3 and 4, *p denotes a prime number*. It is well known that every member of the set E_p can be uniquely expressed as a polynomial modulo p.[2] When we use polynomial notation for members of E_p it is to be understood that addition and multiplication are carried out modulo p. An element of E_p is said to be *linear* if the polynomial representing it is linear.

The notion of linearity can be generalized as follows. Let $\overset{(s)}{+}$ and $\overset{(s)}{\cdot}$ be the conjugates of ordinary addition and multiplication under a given permutation s. We say that a function in E_p is *linear with respect to* $\overset{(s)}{+}$ *and* $\overset{(s)}{\cdot}$ if it can be expressed as a linear polynomial in terms of $\overset{(s)}{+}$ and $\overset{(s)}{\cdot}$. When there is no ambiguity we also say that a function g in E_p is *linear with respect to* $f^{(s)}$ if $f^{(s)}$ is a conjugate of a linear function f and g is linear with respect to $\overset{(s)}{+}$ and $\overset{(s)}{\cdot}$. For any given circular permutation c, there are functions linear with respect to c.

We say that a function $f(x_1, \ldots, x_k)$ in E_n satisfies *strong Słupecki conditions* if it depends essentially on at least two variables and, furthermore, there are numbers i and u_j, $j = 1, \ldots, i—1, i+1, \ldots, k$ such that

$$f_1(x_i) = f(u_1, \ldots, u_{i-1}, x_i, u_{i+1}, \ldots, u_k)$$

is a permutation of the numbers $1, 2, \ldots, n$. Thus, the "matrix" of a function satisfying strong Słupecki conditions possesses one "row" which is a permutation.

In section 3, we shall prove the following

Theorem 3. *Let F be a subset of E_p containing*

1) *a circular permutation $c(x)$,*
2) *a 1-place function $g(x)$ which is not linear with respect to $c(x)$,*

[1] Part I of this paper appeared in these Annals (Series A I 53) and contains sections 1 and 2. Bibliographical references [1] and [2] were first given in part I.

[2] For a detailed proof of this fact, cf. [1, pp. 95—97].

3) *a function* $f(x_1, \dots, x_k)$ *satisfying strong Słupecki conditions.*

Then F *is complete.*

We shall first present five lemmas needed for the proof of theorem 3. Lemma 3.1, due to JABLONSKIĬ, is purely combinatorial. Lemma 3.2 deals with permutation groups of prime degree.

LEMMA 3.1. *Assume a set* B *of* p *elements is divided into* l *non-empty and mutually disjoint subsets* A_i, $i = 1, \dots, l$, *where* $1 < l < p$. *Let* $c(x)$ *be a circular permutation on the elements of* B. *Let* L *contain exactly one element of each of the sets* A_i. *Then there are numbers* r *and* j *such that the set* $c^r(L)$ *contains at least two elements belonging to the set* A_j.

For the proof of lemma 3.1, cf. [1, pp. 105—106].

LEMMA 3.2. *Let* G *be a permutation group of degree* p, *generated by* $c(x)$ *and* $c_1(x)$ *where* $c(x)$ *is a circular permutation and* $c_1(x)$ *is not linear with respect to* $c(x)$. *Then* G *is doubly transitive. Furthermore,* G *contains a non-identical permutation possessing at least two fixed-points.*

Proof. We may assume that

$$c(x) = x + 1$$

and $c_1(x)$ is not linear. For, by forming conjugates, it is immediately seen that if our lemma is true in this case then it is true for any G.

We shall first prove the latter part of the lemma. The permutation

$$c_2(x) = c_1 c c_1^{-1}(x)$$

is circular and not a power of $c(x)$ because $c_1(x)$ is not linear. This implies that one permutation of the form $c_2 c^i(x)$, $i = 1, \dots, p$, possesses at least two fixed-points. For every element $1, 2, \dots, p$ is a fixed-point in some permutation of this form, and there are no fixed-points in the permutation

$$c_2 c^p(x) = c_2(x).$$

On the other hand, all permutations of the form $c_2 c^i(x)$ are different from the identity. Hence, the latter part of the lemma follows.

By a well known theorem of BURNSIDE, because G is a transitive group of prime degree it is either doubly transitive or solvable. To complete the proof of the lemma, we show that G is not solvable. According to a theorem of BRAUER, [3, p. 64], the commutator subgroup G' of G is simple. Hence, if G is solvable then G' is cyclic of prime order or consists of the identity alone.

Consider the following permutations belonging to G':

$$c_2^{-1} c^i c_2 c^{-i}(x), \quad i = 1, \dots, p. \tag{1}$$

Because an element of order p commutes with its own powers only, it is easy to see that all permutations (1) are distinct. Clearly, G' cannot be of prime order $> p$. Hence, if G' satisfies one of the conditions given above then it has to be cyclic of order p. This implies that all elements of G', except for the identity, are circular permutations. Obviously, there are distinct numbers r and s such that

$$c_1(r+1)—c_1(r) = c_1(s+1)—c_1(s).$$

(According to our convention, operations are carried out modulo p.) If we choose in (1)

$$i = c_1(s)—c_1(r)$$

then the resulting permutation is not the identity and has the value $c_1(s)$ as a fixed-point. Hence, it is not circular. This completes the proof of lemma 3. 2.

We shall give an alternative proof for the first part of the lemma in which we do not use the theorems of Burnside and Brauer. Because $c_1(x)$ is not linear, the difference

$$d(x) = c_1(x)—c_1(x—1)$$

assumes at least two distinct values. Let

$$D_k = \{d_1, \ldots, d_k\}$$

be the set defined as follows: for each ν, $1 \leqq \nu \leqq k$, there is a permutation g in G such that, for some i,

$$g(i)—g(i—1) = d_\nu,$$

whereas if d_l does not belong to D_k then, for all g in G and for all x,

$$g(x)—g(x—1) \neq d_l.$$

I.e. D_k is the set of all differences of consecutive elements appearing in the permutations of G. Clearly, $k > 1$. If

$$D_k = \{1, 2, \ldots, p—1\} \tag{2}$$

then G is doubly transitive. For if (2) holds then G contains a permutation mapping the ordered pair $(1, 2)$ into an arbitrary preassigned ordered pair (a, b). Such a permutation can be expressed in the form $c^\alpha g_1 c^\beta$ where g_1 satisfies, for some i, the equation

$$g_1(i)—g_1(i—1) = b—a.$$

We now assume that $k < p—1$ and derive a contradiction. For any permutation g belonging to G and any x, the numbers

$$g(x+d_i),\ i = 1, \dots, k \tag{3}$$

form a permutation of the numbers

$$g(x)+d_i,\ i = 1, \dots, k. \tag{4}$$

Assume the contrary, and let g_2 be a permutation belonging to G such that

$$g_2(x_1+d_i) = g_2(x_1)+d_l,$$

for some x_1, i and l where $1 \leqq i \leqq k$ and $l > k$. Choose a permutation g_3 in G such that, for some x_2,

$$g_3(x_2) - g_3(x_2 - 1) = d_i.$$

Then, for some suitably chosen γ and δ, the permutation $g_4 = c^{\gamma} g_3 c^{\delta}$ satisfies the equations

$$g_4(x_1) = x_1,\ g_4(x_1+1) = x_1+d_i.$$

This implies that

$$g_2 g_4(x_1+1) - g_2 g_4(x_1) = d_l.$$

But because the permutation $g_2 g_4$ belongs to G, this contradicts the definition of the set D_k. Therefore, the numbers (3) form a permutation of the numbers (4). This implies that, for any g in G and any x, the numbers

$$g(x+d_i),\ i = 1, \dots, k$$

form a permutation of the numbers

$$g(x+1+d_i)+d_{\mu(x)},\ i = 1, \dots, k$$

where $1 \leqq \mu(x) \leqq k$. This property is possessed by some linear permutations only. This is a contradiction, and we may conclude that (2) holds. Hence, the first part of lemma 3.2 follows.

The condition of $c_1(x)$ being non-linear with respect to $c(x)$ is essential. If $c_1(x)$ is linear with respect to $c(x)$ then the latter statement in the lemma is always false. The first statement is true in some cases. If $c(x) = x+1$ and $c_1(x) = ax+b$ then G is doubly transitive if and only if a is a primitive root modulo p. We note finally that the hypothesis of lemma 3.2 is never satisfied for $p = 2$ or $p = 3$.

The proofs of the following three lemmas are merely parts of the proof of theorem 3.

LEMMA 3.3. *Let H be a subset of E_p containing a circular permutation $c(x)$, a function $g(x)$ which is not linear with respect to $c(x)$ and a function $h(x_1, \dots, x_k)$ which satisfies Słupecki conditions. Then H generates all constants.*

Proof. Since $c(x)$ is a circular permutation, it suffices to show that H generates some constant. We shall show first that H generates a function of genus smaller than p. This is obvious if $g(x)$ is not a permutation. If $g(x)$ is a permutation then, according to lemma 3.2, H contains a doubly transitive group G. By lemma 1.1 (in part I), there are numbers α_i and α'_i, $\alpha_i \neq \alpha'_i$, $i = 1, \dots, k$, such that

$$h(\alpha_1, \dots, \alpha_k) = h(\alpha'_1, \dots, \alpha'_k).$$

Whe choose from G k permutations $g_i(x)$, $i = 1, \dots, k$, such that $g_i(1) = \alpha_i$ and $g_i(2) = \alpha'_i$. Then the function $h(g_1(x), \dots, g_k(x))$ is of genus smaller than p.

Let $a(x)$ be of genus γ where $1 < \gamma < p$. We shall show that $c(x)$ and $a(x)$ generate a function of genus $\gamma_1 < \gamma$. By repeating the same argument we see that $c(x)$ and $a(x)$ generate a function of genus 1, i.e. a constant. Thus, the proof of lemma 3.3 will be completed.

Let the values assumed by $a(x)$ be $a_1, \dots, a_\gamma$ and let $A_1, \dots, A_\gamma$ be maximal subsets of the set $\{1, \dots, p\}$ defined by the condition $a(A_i) = a_i$, $i = 1, \dots, \gamma$. If $a^2(x)$ is of genus smaller than γ then we have completed the proof. If $a^2(x)$ is of genus γ then the numbers a_i are in different sets A_i. We denote

$$L = \{a_1, \dots, a_\gamma\}.$$

By lemma 3.1, there are numbers r and j such that $c^r(L)$ contains at least two elements belonging to A_j. This implies that the function $ac^r a(x)$ is of genus smaller than γ.

We mention without proof that lemma 3.3 remains valid if $g(x)$ is replaced by any 1-place function which is not a power of $c(x)$. As regards the function h, it suffices to assume that it depends essentially on at least two variables. (Cf. the proof of lemma 4.3 below.)

Lemma 3.4. *Let H be as in lemma 3.3, with the additional assumption that $g(x)$ is a permutation (which is not linear with respect to $c(x)$). Then H generates a function $g_1(x)$ of genus γ where $1 < \gamma < p$.*

Proof. By lemma 3.3, H generates all constants. On the other hand, the function $h(x_1, \dots, x_k)$ and all constants generate a function $h_1(x,y)$ depending essentially on both of its variables. This is easily established by induction on the number k.

Consider the matrix of $h_1(x,y)$. If the rows and columns are regarded as 1-place functions belonging to E_p then H generates all of these 1-place functions. We may assume that each row and column is either constant or a permutation because, otherwise, the proof is completed. Under this assumption, either each row and column is a permutation or exactly one row and one column are constants and other rows and columns are permutations. This is due to the fact that h_1 depends essentially on both of its variables. If we are dealing with the latter alternative then some function of the form $h_1(x, c^\alpha(x))$ can be chosen as $g_1(x)$.

We may, therefore, assume that we are dealing with the first alternative, i.e. each row and column in the matrix of $h_1(x,y)$ is a permutation. Consider the functions

$$h_1(x, c^i(x)),\ i = 1, \ldots, p. \tag{5}$$

If one of these functions is of genus γ with $1 < \gamma < p$, the proof of lemma 3.4 has been completed. Under our assumptions, it is not possible that some functions (5) are constants and some other functions (5) are permutations.

Assume that all functions (5) are constants. Clearly, they have to be different constants, for $i = 1, \ldots, p$. By lemma 3.2, H contains a non-identical permutation $g_2(x)$ possessing at least two fixed-points. We may choose

$$g_1(x) = h_1(x, g_2(x)).$$

Assume, finally, that all functions (5) are permutations. There are distinct numbers y_1 and y_2 such that

$$h_1(1, y_1) = h_1(2, y_2) = 1.$$

By lemma 3.2, H contains a doubly transitive group. We choose from this group a permutation $g_3(x)$ such that $g_3(1) = y_1$ and $g_3(2) = y_2$. If the function $h_1(x, g_3(x))$ assumes some value other than 1 then this function may be chosen as $g_1(x)$. If

$$h_1(x, g_3(x)) = 1,$$

for all x, then the function

$$h_2(x,y) = h_1(x, g_3(y))$$

belongs to some case we have already considered. Hence, lemma 3.4 follows. We note that the lemma is valid also without the additional assumption concerning $g(x)$. If $g(x)$ is not a permutation then the conclusion is trivial.

In the following lemma we are dealing with double transitivity concerning functions other than permutations.

LEMMA 3.5. *Let H be subset of E_p containing a circular permutation $c(x)$, a constant $c'(x) = c'$ and a function $h(x_1, \ldots, x_k)$ satisfying strong Slupecki conditions. Then, for any numbers x_1, x_2, y_1, y_2 where $x_1 \neq x_2$, H generates a function $g(x)$ such that $g(x_1) = y_1$ and $g(x_2) = y_2$.*

Proof. It obviously suffices to prove the lemma for the case $c(x) = x + 1$.

Any other case can be reduced to this case by considering conjugate sets of functions.

Clearly, H generates all constants. The function $h(x_1, \ldots, x_k)$ and all constants generate a 2-place function $h_1(x,y)$ satisfying strong Słupecki conditions. This can be shown by induction on the number k.

Let μ' be a number such that $h_1(\mu',y)$ is a permutation. (Such a number μ' exists because h_1 satisfies strong Słupecki conditions. We may assume that μ' is assigned for x because, otherwise, we change the notation for the variables.) All powers of this permutation are generated by H. Hence, H generates a function $h_2(x,y)$ depending essentially on both x and y and satisfying the equation

$$(6) \qquad h_2(\mu',y) = y, \quad \text{for any } y.$$

Let u be an arbitrary but fixed number satisfying $1 \leqq u \leqq p-1$. Because $h_2(x,y)$ depends essentially on the variable x, (6) implies that there numbers μ and ν such that

$$(7) \qquad h_2(\mu,y) = y, \text{ for any } y,$$

and

$$(8) \qquad a = h_2(\mu - u, \nu) \neq h_2(\mu, \nu) = \nu.$$

This is due to the fact that p is prime and, hence, any number x can be expressed in the form

$$x = \mu' - \xi u.$$

Let H_1 be the set of 1-place functions generated by H. We define the set

$$D_l = \{d_1, \ldots, d_l\}$$

as follows: for each i, $1 \leqq i \leqq l$, there is a function $e(x)$ in H_1 such that, for some x,

$$e(x+u) - e(x) = d_i,$$

whereas if d' does not belong to D_l then, for all e in H_1 and for all x,

$$e(x+u) - e(x) \neq d'.$$

Clearly, the numbers u and p (which is reduced to 0) belong to D_l. If

$$(9) \qquad D_l = \{1, 2, \ldots, p\}$$

then lemma 3.5 follows. In this case, we let $u = x_2 - x_1$ and choose from H_1 a function $e(x)$ such that, for some x',

$$e(x'+u)-e(x') = y_2 - y_1.$$

Then we may choose

$$g(x) = c^{\alpha} e c^{\beta}(x)$$

where $\alpha = y_1 - e(x')$ and $\beta = x' - x_1$.

We assume that (9) does not hold, i.e. $l < p$, and derive a contradiction. We choose from H_1 functions $g_i(x)$, $i = 1, \ldots, l$, such that $g_i(1) = \nu$, $g_i(1+u) = \nu + d_i$, and a function $g'(x)$ such that $g'(1) = \mu - u, g'(1+u) = \mu$. Then the functions

$$h'_i(x) = h_2(g'(x), g_i(x)), i = 1, \ldots, l$$

belong to H_1. Clearly, $h'_i(1) = a$ and $h'_i(1+u) = \nu + d_i$, by (7) and (8). Hence, by the definition of the set D_l, the numbers $\nu + d_i - a$ form a permutation of the numbers d_i, i.e.

$$\nu + d_i - a = d_{s_i}, \ i = 1, \ldots, l.$$

Summation gives us the equation

$$l(\nu - a) = 0.$$

But because of (8), this contradicts the primality of p. Thus, the proof of lemma 3.5 has been completed.

We note that if one has to show that some group is doubly transitive then it suffices to show that the ordered pair $(1,2)$ can be mapped into an arbitrary ordered pair by permutations belonging to this group. A similar argument is not sufficient for the proof of lemma 3.5 because we cannot, in general, form inverses of functions belonging to H_1.

We shall now present the following

Proof of theorem 3. Because any function satisfying strong Słupecki conditions satisfies Słupecki conditions it follows from lemma 3.3 that F generates all constants. Clearly, the function $g(x)$ given in hypothesis 2) cannot be constant. If $g(x)$ is not a permutation we conclude that F generates a function of genus γ where $1 < \gamma < p$. By lemma 3.4, the same conclusion holds true also if $g(x)$ is a permutation.

We shall now use lemma 3.5 in order to show that if F generates a function $a(x)$ of genus γ where $2 < \gamma < p$ then F generates a function $a'(x)$ of genus γ' where $2 \leqq \gamma' < \gamma$. This assertion, together with the result obtained above, implies that F generates a function of genus 2. To simplify the notation, we prove the assertion for $\gamma = 3$. The proof in the general case is similar.

Assume that F generates a function $a(x)$ of genus 3. Let the values assumed by $a(x)$ be α_i, $i = 1, 2, 3$, and let A_i consist of those numbers x which satisfy the equation $a(x) = \alpha_i$. It suffices to consider the case that α_i belongs to A_i, for $i = 1, 2, 3$. For if the numbers α belong to different sets A then the function $a^6(x)$ always possesses this property. If two of the numbers α belong to the same set A_j whereas the third of these numbers belongs to a set A'_j different from A_j then the function $a^2(x)$ is of genus 2 which proves our assertion. Finally, if all numbers α belong to the same set A then we replace $a(x)$ by a function of the form $c^i a(x)$. It is easy to see that at least one function of this form belongs to one of the two cases we have already considered.

The sum of the cardinalities of the sets A_i is a prime number. Hence, we may assume that the cardinality of A_1 is greater than the cardinality of A_3. Choose an arbitrary element a_2 belonging to A_2. By lemma 3.5, given any element a_1 of A_1, F generates a function $e(x)$ such that $e(\alpha_1) = a_1$ and $e(\alpha_2) = a_2$. If some of these functions $e(x)$ has the property that $e(\alpha_3)$ belongs to A_1 or A_2 then the function $aea(x)$ is of genus 2. Therefore, we may assume that all functions $e(x)$ have the property that $e(\alpha_3)$ belongs to A_3.

There are two distinct elements a_1 and a'_1 of A_1, an element a_3 of A_3 and two functions $e'(x)$ and $e''(x)$ such that

$$e'(\alpha_1) = a_1,\ e''(\alpha_1) = a'_1,\ e'(\alpha_2) = e''(\alpha_2) = a_2,\ e'(\alpha_3) = e''(\alpha_3) = a_3.$$

This follows from the fact that the cardinality of A_1 is greater than that of A_3. By lemma 3.5, F generates a function $e_1(x)$ such that $e_1(a_1) = \alpha_1$ and $e_1(a'_1) = \alpha_2$. Consider the values

$$e_1(a_2) \text{ and } e_1(a_3). \tag{10}$$

The function $ae_1e'a(x)$ is of genus 2, provided it is not the case that the numbers (10) both belong to A_1 or one of them belongs to A_2 and the other to A_3. The function $ae_1e''a(x)$ is of genus 2, provided it is not the case that the numbers (10) both belong to A_2 or one of them belongs to A_1 and the other to A_3. (Note that we have not assumed that the numbers (10) are distinct. In fact, they may be equal.) Hence, in every case F generates a function of genus 2. Thus, the assertion is correct.

Let $b(x)$ be a function of genus 2 generated by F. The next step in the proof of theorem 3 is to show that F generates a function of type $[p-1, 1]$. Assume $b(x)$ is of type $[p-\beta, \beta]$ where $2 \leqq \beta < p-\beta$. We shall prove that F generates a function $b_1(x)$ of type

$$[p-\beta_1, \beta_1] \text{ where } 1 \leqq \beta_1 < \beta. \tag{11}$$

Since we may repeat the same argument, this implies that F generates a function of type $[p-1, 1]$.

We denote by B_1 and B_2 maximal subsets of the set $\{1, \ldots, p\}$ such that $b(x)$ assumes a constant value in both B_1 and B_2. Then we may assume that the cardinality of B_1 equals β and the cardinality of B_2 equals $p-\beta$. Given any i and j, F generates a function $b_{i,j}(x)$ assuming the value i in the set B_1 and the value j in the set B_2. This is a consequence of lemma 3.5.

The function $f(x_1, \ldots, x_k)$ given in hypothesis 3) of theorem 3 and all constants generate a 2-place function $f_1(x,y)$ satisfying strong Słupecki conditions. We shall now prove that F generates a function $f_1'(x,y)$ such that, for some values x_1, x_2, y_1, y_2,

$$f_1'(x_1,y_1) \neq f_1'(x_1,y_2) = f_1'(x_2,y_1) = f_1'(x_2,y_2). \tag{12}$$

Because $f_1(x,y)$ satisfies strong Słupecki conditions and p is a prime number there are sets X_1 and Y_1, containing exactly two elements each, such that the set $f_1(X_1, Y_1)$ contains exactly three numbers ξ, ξ' and ξ''. We suppose ξ is assumed by f_1 for two variable assignments in the sets X_1 and Y_1, whereas ξ' and ξ'' are each assumed for one variable assignment in these sets. If ξ' and ξ'' are in different sets B then the function $b_{\xi,\xi'} f_1(x,y)$ satisfies (12). The case where ξ' and ξ'' are in the same set B is easily reduced to this case by considering functions of the form $c^i f_1(x,y)$.

We now choose a number δ such that $c^\delta(x)$ maps some element of B_1 into some other element of B_1. Then we obtain the following inequalities for the cardinality of the intersection of B_1 and $c^\delta(B_1)$:

$$1 \leqq \text{card}\,(B_1 \cap c^\delta(B_1)) < \text{card}\,(B_1) = \beta. \tag{13}$$

The lower limitation is obvious, by the choice of δ. The upper limitation is a consequence of the fact that c^δ does not map every element of B_1 into an element of B_1. Otherwise, the group generated by c^δ would not be transitive which is impossible because c^δ is a circular permutation.

We may now choose

$$b_1(x) = f_1'(b_{x_1,x_2}(x), b_{y_1,y_2}c^{-\delta}(x)).$$

By (12), $b_1(x)$ assumes two values. One of them is assumed for the values of x belonging to the intersection of the two sets B_1 and $c^\delta(B_1)$, the other for all remaining values of x. It follows from (13) that $b_1(x)$ is of type (11).

Thus, we have shown that F generates a function $b'(x)$ of type $[p-1,1]$. This implies, by lemma 3.5, that all functions of this type are generated by F. For any function of this type is of the form $b''b'c^i(x)$ where the function $b''(x)$ maps the values of $b'(x)$ into some preassigned ordered pair.

We shall now make the following hypothesis of induction: F generates all functions of type

$$[p-m, \underbrace{1, \ldots, 1}_{m \text{ terms}}] \quad \text{where } 1 \leqq m < p-2. \tag{14}$$

We shall prove that this implies that F generates all functions of type

$$[\underbrace{p—m—1, 1, \ldots, 1}_{m+1 \text{ terms}}]. \tag{15}$$

Consequently, F generates all functions of genus $p—1$. Hence, by lemma 1.3 (in part I), F generates all 1-place functions which are not permutations. According to a well known completeness criterion, [1, p. 72], this implies that F is complete.

To show that all functions of type (15) are generated by F, we proceed as follows. It is easy to prove that F generates a 2-place function $\varphi(x,y)$ such that, for some μ and ν,

$$\varphi(\mu, y) = y, \text{ for any } y, \tag{16}$$

and

$$\rho = \varphi(\mu—1, \nu) \neq \varphi(\mu, \nu) = \nu. \tag{17}$$

The argument is similar to the one presented in the proof of lemma 3.5.

We denote by $\varphi_1(x)$ any function assuming the value μ $p—1$ times and the value $\mu—1$ once, and by $\varphi_2(x)$ any function assuming the value ν $p—m$ times. Clearly, F generates all functions $\varphi_1(x)$. By our inductive hypothesis and lemma 1.3, F generates also all functions $\varphi_2(x)$. Consider compositions of the form

$$\varphi(\varphi_1(x), \varphi_2(x)). \tag{18}$$

By (16) and (17), any function $\varphi_3(x)$ of type (15), assuming the value ρ once and the value ν $p—m—1$ times, is among the functions (18). By composing functions $\varphi_3(x)$, we obtain any function $\varphi_4(x)$ of type (15) which assumes the values ρ and ν. Let ω be a natural number such that $c^{\omega}(\rho) = \nu$. Any function $\varphi_5(x)$ of type (15) which, for some η and η', satisfies the equation

$$\varphi_5(\eta') = c^{\omega}\varphi_5(\eta)$$

can be expressed in the form $c^{i}\varphi_4(x)$. Thus, F generates all functions $\varphi_5(x)$.

We shall now assume that F generates all functions $\varphi_6(x)$ of type (15) which, for some η_1 and η'_1, satisfy the equation

$$\varphi_6(\eta'_1) = c^{r\omega}\varphi_6(\eta_1) \tag{19}$$

where r is a fixed integer $\geqq 1$. We denote by $\varphi_7(x)$ any function assuming the value ν once and the value $c^{r\omega}(\nu)$ $p—m—1$ times. By our assumption and lemma 1.3, F generates all functions of the form

$$\varphi(\varphi_1(x), \varphi_7(x)). \tag{20}$$

By composing functions (20) and multiplying by powers of $c(x)$, we obtain all functions $\varphi_8(x)$ of type (15) which, for some η_2 and η'_2, satisfy the equation

$$\varphi_8(\eta'_2) = c^{(r+1)\omega}\varphi_8(\eta_2).$$

We conclude, by induction on the number r, that F generates all functions of type (15) which, for some natural r, satisfy (19). Because p is prime and $\omega \neq 0$, any power of $c(x)$ can be expressed in the form $c^{r\omega}(x)$. This implies that F generates all functions of type (15).

Thus, our induction has been completed. Hence, theorem 3 follows.

We shall make some final remarks concerning the necessity of the assumptions made in theorem 3. The theorem is not valid for subsets of E_n if n is composite. In this case, our F may be contained in some class T or in some class U. (For the notation, cf. [1, pp. 85—93].)

It is well known (cf. [1, p. 80]) that a subset of E_n is complete if and only if it is not contained in any precomplete subset of E_n. In general, very little is known about the precomplete subset of E_n. The most powerful instrument in the proof of theorem 3 is the circular permutation $c(x)$. As it turns out, very few precomplete subsets of E_p contain circular permutations. The function $g(x)$ is needed because, otherwise, F may contain only functions linear with respect to $c(x)$. If we do not assume that g is a 1-place function then F may contain only functions self-conjugate under $c(x)$. Finally, we need a function satisfying Słupecki conditions because, otherwise, F may be contained in the precomplete subset of E_p consisting of all 1-place functions and of those functions of more than one variables which do not assume all p values. (In [1], this precomplete set is denoted by $T_{N,\,p-1}$.)

Although we need a function satisfying Słupecki conditions, it seems most likely that we do not need a function satisfying strong Słupecki conditions. Our original intention was to prove a stronger theorem where in hypothesis 3) it is assumed only that f satisfies Słupecki conditions. However, we have not been able to carry out the proof of this stronger theorem. It can be shown that, under these weaker assumptions, F generates all constants and a function of genus 2. We leave the proof of this fact to the reader. For this purpose, we have formulated lemmas 3.3 and 3.4 in somewhat stronger way than is necessary for the proof of theorem 3.

The hypothesis of theorem 3 is never satisfied for $p = 2$. If $p = 3$ then also the stronger formulation of theorem 3 is valid. This follows because all precomplete subsets of E_3 are known. (They are 18 in number and were first listed in [4]. For a detailed account, cf. [1, pp. 109—140].) It is easy to check that F is not contained in any of them.

The stronger formulation of theorem 3 has some direct implications to the theory of precomplete sets. Of these we mention the following. For any circular permutation $c(x)$, there are exactly three precomplete subsets of E_p containing $c(x)$.

4. We shall now apply theorem 3 to the theory of Sheffer functions of E_p. We shall prove the following

THEOREM 4. *A function $f(x_1, \ldots, x_k)$ belonging to E_p is a Sheffer function if (and only if) it generates a circular permutation $c(x)$ and a function $g(x)$ which is not a power of $c(x)$.*

Apparently, the "only if"-part of the theorem is trivial. Theorem 4 can be stated also in the following form:

THEOREM 4'. *A function $f(x_1, \ldots, x_k)$ belonging to E_p is a Sheffer function if (and only if) it generates a circular permutation $c(x)$ and is not self-conjugate under $c(x)$.*

It is easy to see that the hypotheses of theorems 4 and 4' are equivalent. Conjecture 2 presented in [2, p. 47] is a special case ($k = 2$) of theorem 4. We need three lemmas in order to reduce theorem 4 to theorem 3.

LEMMA 4.1. *A non-linear function and all constants belonging to E_p, $p \geqq 3$, generate a non-linear 1-place function.*

A proof of lemma 4.1 can be found in [1, p. 98]. The lemma holds true also with respect to the generalized notion of linearity.

LEMMA 4.2. *A function $f(x_1, \ldots, x_k)$ satisfying the hypothesis of theorem 4' is non-linear.*

Proof. Assume the contrary, i.e. the polynomial representation of f is as follows:

$$f(x_1, \ldots, x_k) = a_1 x_1 + \ldots + a_k x_k + a_{k+1}.$$

The necessarily

$$(21) \qquad a_1 + \ldots + a_k = 1$$

because, otherwise, the function

$$f_1(x) = f(x, \ldots, x)$$

possesses one fixed-point which is impossible since f generates a circular permutation $c(x)$. But (21) implies that f is self-conjugate under the circular permutation $x + 1$. Hence, f generates only functions self-conjugate under $x + 1$. This implies that $c(x)$ is a power of $x + 1$ and f is self-conjugate under $c(x)$. This is a contradiction. Hence, f is non-linear.

The given proof of lemma 4.2 is in terms of ordinary addition and multiplication modulo p. However, it can be formulated in terms of arbitrary conjugates of addition and multiplication. Hence, f is non-linear in the general sense.

Lemma 4.3. *Let $p \geqq 3$. Then there is no function $h(x_1, \ldots, x_l)$ in E_p which depends essentially on all of its l variables, $l \geqq 2$, and satisfies the following condition: the subset H of E_p consisting of h and the linear permutations $x+1$ and rx, $r>1$, generates no 1-place functions other than linear permutations.*

Proof. It suffices to prove the lemma for $l=2$. The general case can be reduced to this case by considering functions obtained by identifying some variables. We assume that $h(x,y)$ depends essentially on both x and y and, furthermore, that $h(x,y)$, $x+1$ and rx, $r>1$, generate no 1-place functions other than linear permutations. We shall derive a contradiction.

Let H_1 be the set of 1-place functions generated by our three functions. By the assumptions,

$$h(rx+\nu, x+\nu) = d_\nu x + b_\nu, \ \nu = 0, 1, \ldots, p-1, \tag{22}$$

because each of these functions is in H_1. Consider the function

$$h'(x) = h(x+r, x+1).$$

Because h' is in H_1 it is a linear permutation. This fact and (22) imply that the difference

$$(d_\nu + b_\nu) - (d_{\nu-1} + b_{\nu-1})$$

assumes a constant value, for $\nu = 0, 1, \ldots, p-1$. The function $h_1(x) = h(x,x)$ is in H_1 and, hence, is a linear permutation. This implies, by (22), that the difference $b_\nu - b_{\nu-1}$ assumes a constant value. Hence, also the difference $d_\nu - d_{\nu-1}$ assumes a constant value.

There is no number x_1 such that

$$d_0 x_1 + b_0 = d_1 x_1 + b_1$$

because, otherwise, the function $h_2(x) = h(x+rx_1, x+x_1)$ is not a permutation, contrary to our assumptions. This implies that $d_0 = d_1$ and $b_0 \neq b_1$. Hence,

$$h(rx+\nu, x+\nu) = d_0 x + b_0 + \nu b, \ \nu = 0, 1, \ldots, p-1,$$

where $b = b_1 - b_0 \neq 0$. By easy computations, we obtain the result that $h(x,y)$ is linear:

$$h(x,y) = Ax + By + C, \ A \neq 0, \ B \neq 0. \tag{23}$$

Furthermore, $A + B \neq 0$ because, otherwise, the function $h(x,x)$ is not a permutation.

It follows from our assumptions that H_1 does not contain all linear permutations. For it is well known that all linear permutations form a doubly transitive group. Hence, if H_1 contains all linear permutations then H_1 and h generate, by lemma 1.1, a 1-place function which is not a permutation, contrary to our assumptions.

We may, therefore, assume that H_1 contains exactly the following functions:

$$a_i x + j, \ 0 \leqq i \leqq u, \ 0 \leqq j \leqq p-1,$$

where $u < p-1$, $a_0 = 1$ and $a_1 = r$. (Clearly, the set consisting of the numbers a_i has to be closed under multiplication (mod p).) The set H_1 contains the functions $h(a_i x, x)$ and $h(a_i x, a_i x)$, for $i = 0, 1, \ldots, u$. Because $A + B \neq 0$ and $A \neq 0$ this implies, by (23), that the numbers $Aa_i + B$ form a permutation of the numbers $(A+B)a_i$. Since $B \neq 0$, we obtain the equation

$$(24) \qquad a_0 + \ldots + a_u = u + 1.$$

By considering functions $h(a_1 a_i x, x)$ and $h(a_1 a_i x, a_1 a_i x)$, we obtain similarly the equation

$$(u+1)B = Ba_1(a_0 + \ldots + a_u).$$

Hence, by (24), $a_1 = 1$ because $u + 1 < p$ and $B \neq 0$. But this contradicts the fact that $a_1 = r > 1$. Therefore, lemma 4.3 follows. We note finally that the proof remains unaltered if the permutations $x + 1$ and rx are replaced by $c(x)$ and $c'(x)$ where $c(x)$ is a circular permutation and $c'(x)$ is a permutation linear with respect to $c(x)$ but not a power of $c(x)$.

We are now in the position to establish theorem 4 (and theorem 4′). By known results (cf. [1, pp. 18—20]) the theorem is valid if $p = 2$. We may, therefore, assume that $p \geqq 3$. By lemma 4.3, it cannot be the case that f generates no 1-place functions other than permutations linear with respect to $c(x)$. Hence, f has to generate either some constant (and, therefore, all constants) or some 1-place function not linear with respect to $c(x)$. In the latter case we may conclude, by lemma 3.3, that f generates all constants. Hence, it is an immediate consequence of lemmas 4.1 and 4.2 that f generates a 1-place function not linear with respect to $c(x)$. By considering composition sequences of $c(x)$ in terms of f and constants, we see that f generates a function satisfying strong Słupecki conditions. This means that f generates a set F satisfying the hypotheses of theorem 3. Thus, by theorem 3, theorem 4 follows.

We add some further discussion concerning the applications of theorem 4. Given a function $f(x_1, \ldots, x_k)$, we call the function

$$f_1(x) = f(x, \ldots, x)$$

the *main diagonal* of f. The following theorem is an immediate consequence of theorem 4′:

THEOREM 5. *Let $Shd(p,k)$ be the number of such k-place Sheffer functions in E_p whose main diagonal is a circular permutation. Then*

$$Shd(p,k) = (p-1)\,!\,(p^{p^k-p} - p^{p^{k-1}-1}). \tag{25}$$

The equation (25) is easily obtained by computing first the number of functions self-conjugate under a circular permutation. For $p = 2$, (25) obviously gives the number of all k-place Sheffer functions.

The number $Shd(p,k)$ (which expresses the exact number of k-place Sheffer functions of a special form) is greater than any known lower limitation on the number of all k-place Sheffer functions. In case $p = 5$ we obtain, by (25), 2.288.818.359.360.000 2-place Sheffer functions. A better lower limitation on the number of all k-place Sheffer functions in E_p is obtained by adding to $Shd(p,k)$ the number of all such k-place functions $f(x_1, \ldots, x_k)$ which generate a circular permutation in terms of a composition sequence of "second order", eg.

$$c(x) = f(f(x, \ldots, x), x, \ldots, x)$$

where $c(x)$ is a circular permutation.

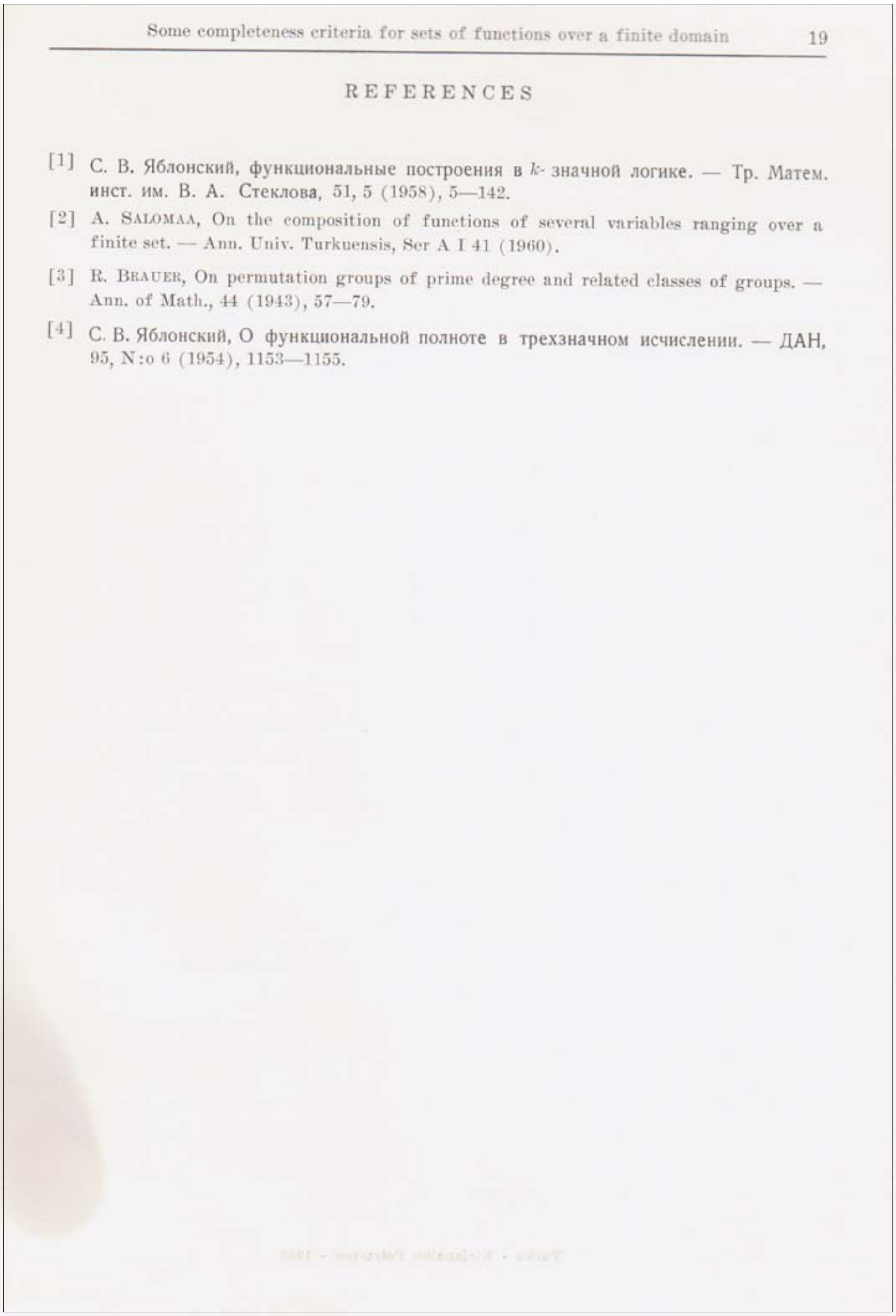
The equation (25) expresses the fact that almost every function in E_p whose main diagonal is a circular permutation is a Sheffer function. (One may consider limits when either p or k approaches infinity.)

We shall, finally, consider the following problem. It is clear that one value of a function f in E_n may cause f not to be a Sheffer function, no matter what the other values of f are. Any fixed-point of the main diagonal is such a value. The question arises: what is the minimum number a of values of a k-place function f which have to be fixed in order to be sure that f always is a Sheffer function, no matter how the remaining $n^k - a$ values of f are defined? It is easy to prove that $a \geqq n + 2$. According to theorem 4, $a = n + 2$ when n is prime. For instance, any function $f(x_1, \ldots, x_k)$ (in E_p) satisfying the following conditions is a Sheffer function:

$$f(x, \ldots, x) = x + 1,$$

$$f(2, 1, \ldots, 1) = f(3, 2, \ldots, 2) = 1.$$

For composite values of n, $a > n + 2$.



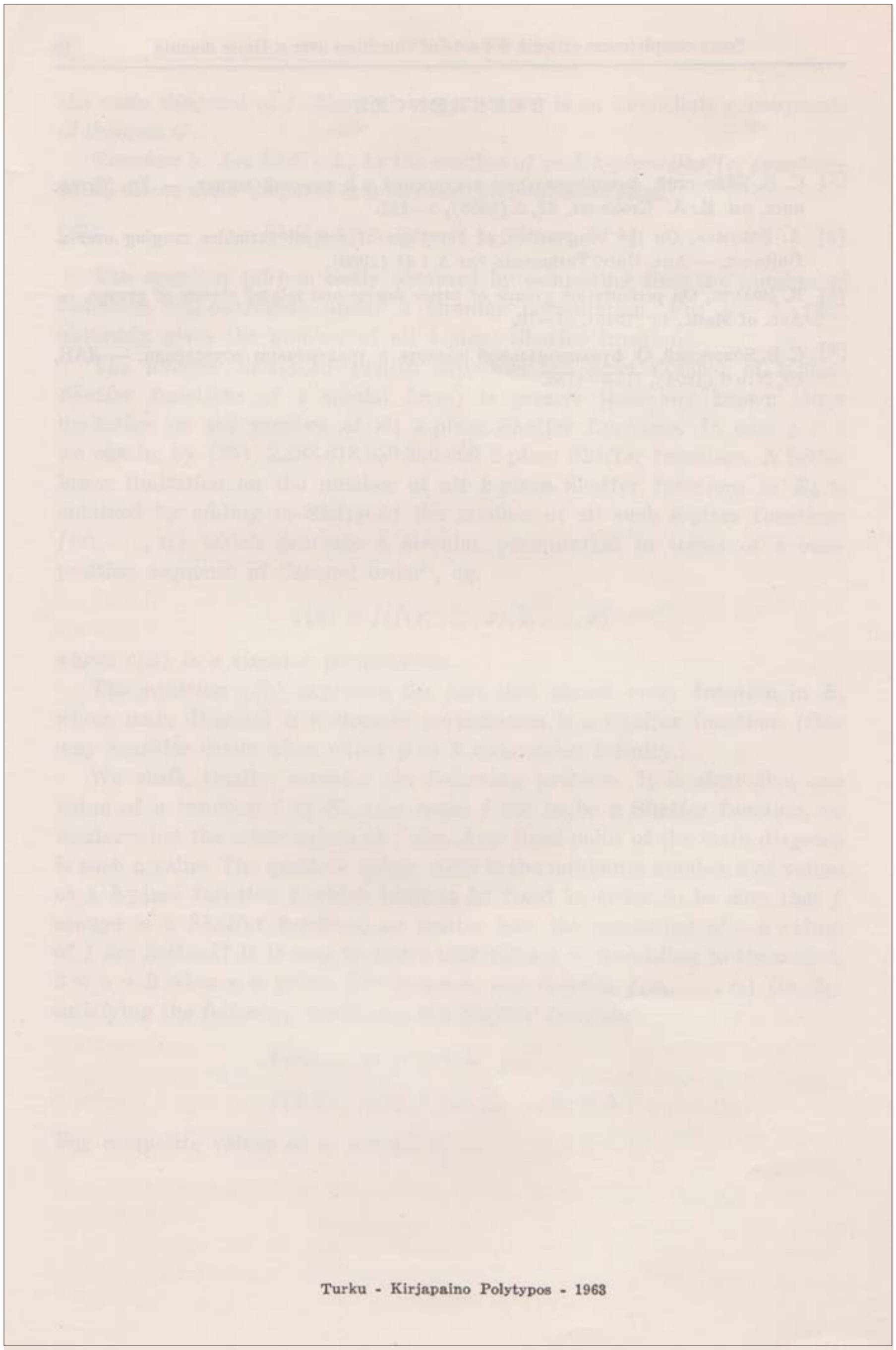
REFERENCES

[1] С. В. Яблонский, функциональные построения в k- значной логике. — Тр. Матем. инст. им. В. А. Стеклова, 51, 5 (1958), 5—142.

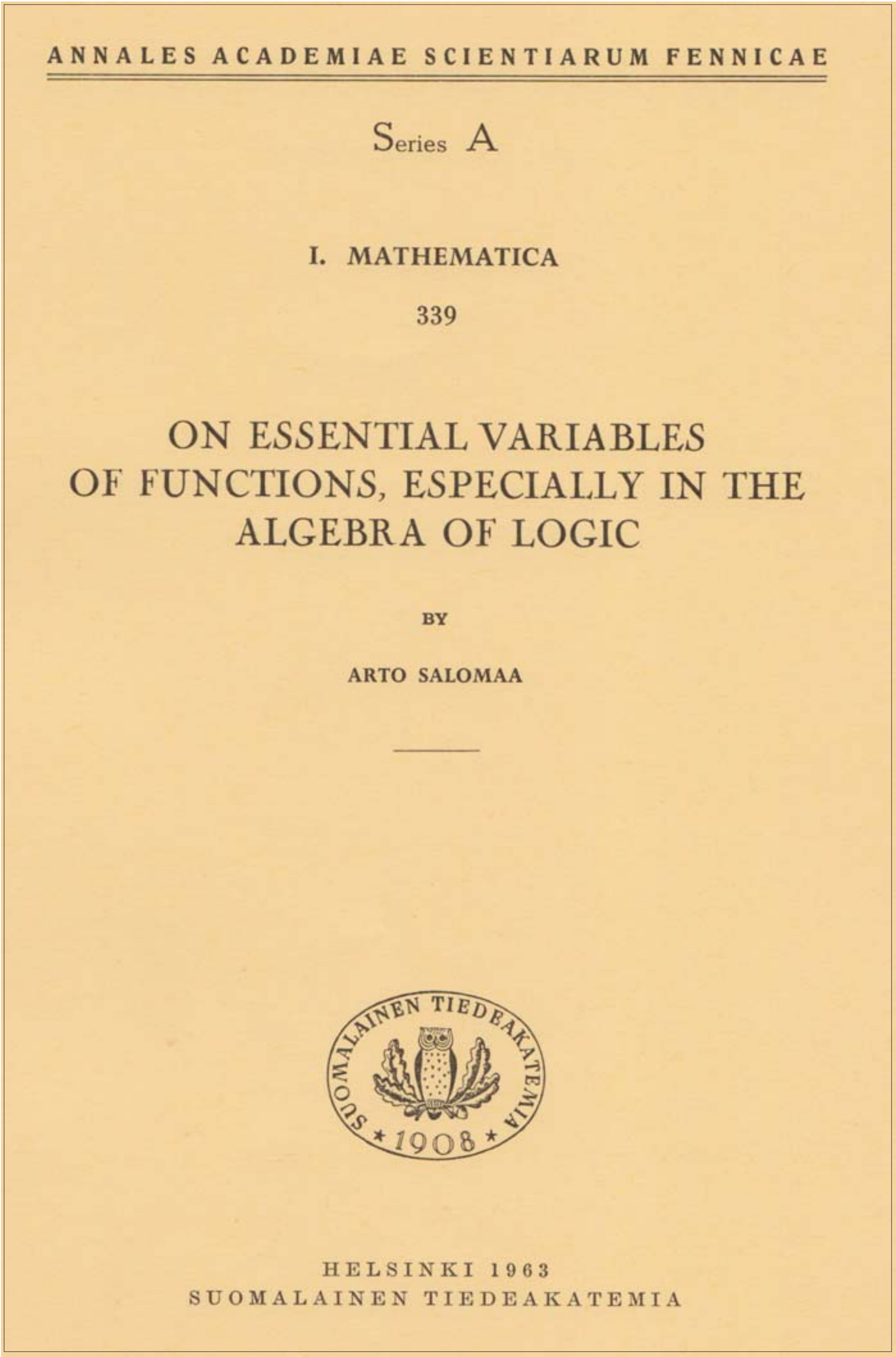
[2] A. Salomaa, On the composition of functions of several variables ranging over a finite set. — Ann. Univ. Turkuensis, Ser A I 41 (1960).

[3] R. Brauer, On permutation groups of prime degree and related classes of groups. — Ann. of Math., 44 (1943), 57—79.

[4] С. В. Яблонский, О функциональной полноте в трехзначном исчислении. — ДАН, 95, N:o 6 (1954), 1153—1155.



Turku - Kirjapaino Polytypos - 1963



ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

339

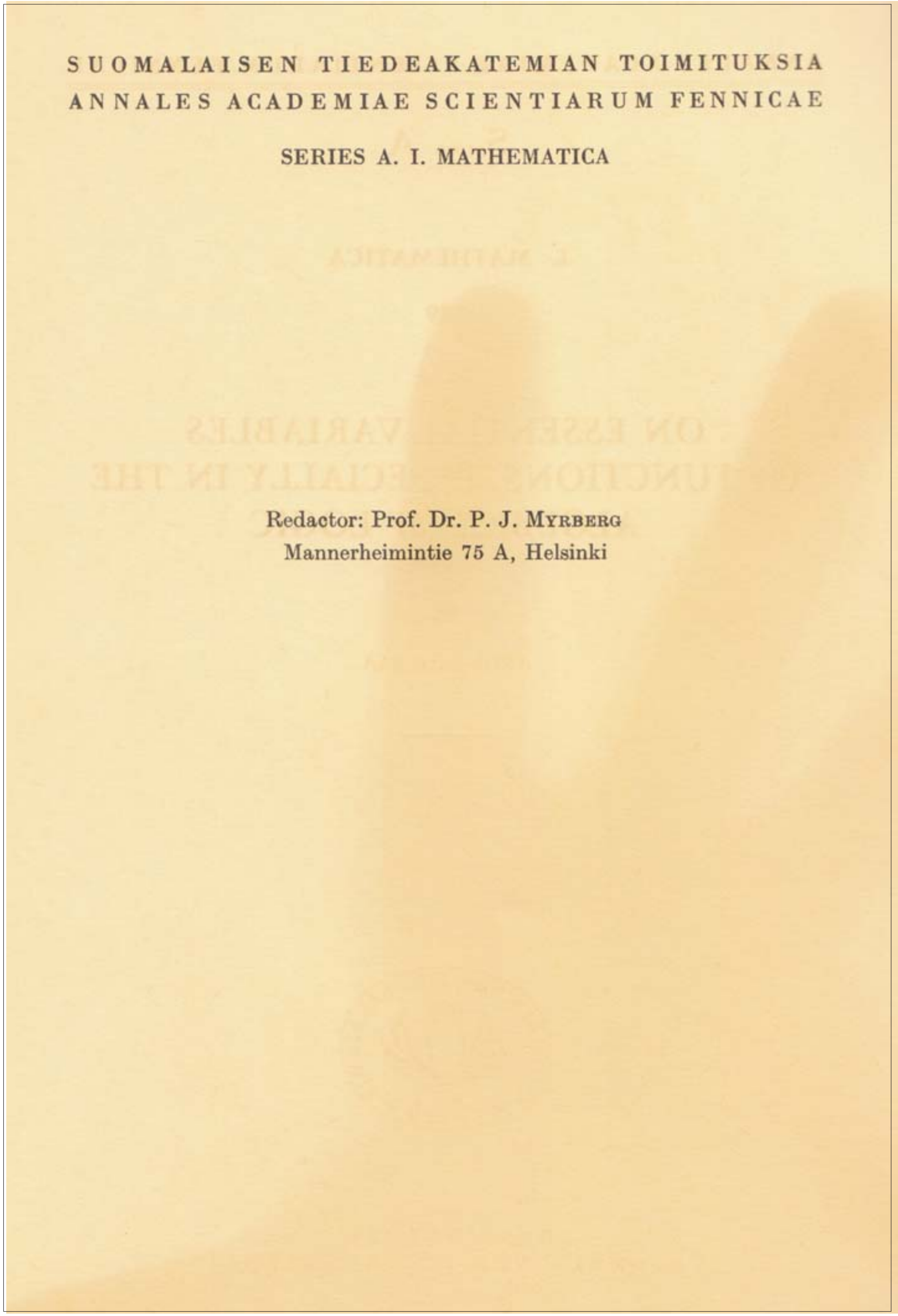
ON ESSENTIAL VARIABLES OF FUNCTIONS, ESPECIALLY IN THE ALGEBRA OF LOGIC

BY

ARTO SALOMAA

SUOMALAINEN TIEDEAKATEMIA
* 1908 *

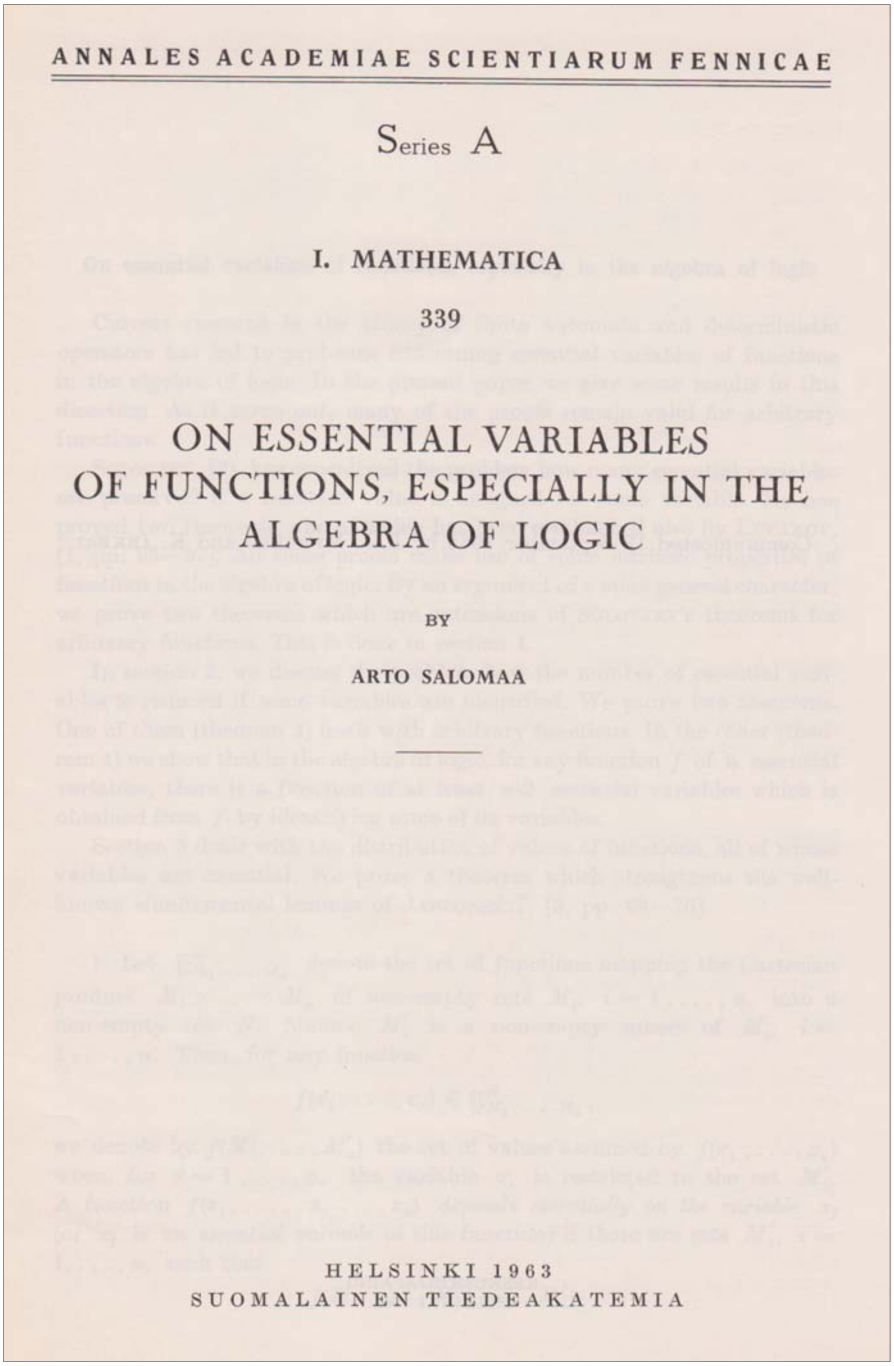
HELSINKI 1963
SUOMALAINEN TIEDEAKATEMIA



SUOMALAISEN TIEDEAKATEMIAN TOIMITUKSIA
ANNALES ACADEMIAE SCIENTIARUM FENNICAE

SERIES A. I. MATHEMATICA

Redactor: Prof. Dr. P. J. Myrberg
Mannerheimintie 75 A, Helsinki



ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

339

ON ESSENTIAL VARIABLES OF FUNCTIONS, ESPECIALLY IN THE ALGEBRA OF LOGIC

BY

ARTO SALOMAA

HELSINKI 1963
SUOMALAINEN TIEDEAKATEMIA

Communicated 13 September 1963 by P. J. Myrberg and K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1963

On essential variables of functions, especially in the algebra of logic

Current research in the theory of finite automata and deterministic operators has led to problems concerning essential variables of functions in the algebra of logic. In the present paper we give some results in this direction. As it turns out, many of the proofs remain valid for arbitrary functions.

SOLOVJEV, [2], has considered the problem how many essential variables are preserved if a constant value is assigned for some variable. He has proved two theorems, one of which has been established also by LUPANOV, [1, pp. 95—97]. All these proofs make use of some intrinsic properties of functions in the algebra of logic. By an argument of a more general character, we prove two theorems which are extensions of SOLOVJEV's theorems for arbitrary functions. This is done in section 1.

In section 2, we discuss the problem how the number of essential variables is reduced if some variables are identified. We prove two theorems. One of them (theorem 3) deals with arbitrary functions. In the other (theorem 4) we show that in the algebra of logic, for any function f of n essential variables, there is a function of at least n-2 essential variables which is obtained from f by identifying some of its variables.

Section 3 deals with the distribution of values of functions, all of whose variables are essential. We prove a theorem which strengthens the well-known »fundamental lemma» of JABLONSKIĬ, [3, pp. 68—70].

1. Let $\mathfrak{F}^N_{M_1,\dots,M_n}$ denote the set of functions mapping the Cartesian product $M_1 \times \dots \times M_n$ of non-empty sets M_i, $i = 1, \dots, n$, into a non-empty set N. Assume M'_i is a non-empty subset of M_i, $i = 1, \dots, n$. Then, for any function

$$f(x_1, \dots, x_n) \in \mathfrak{F}^N_{M_1,\dots,M_n},$$

we denote by $f(M'_1, \dots, M'_n)$ the set of values assumed by $f(x_1, \dots, x_n)$ when, for $i = 1, \dots, n$, the variable x_i is restricted to the set M'_i. A function $f(x_1, \dots, x_j, \dots, x_n)$ *depends essentially on the variable* x_j (or x_j is an *essential variable* of this function) if there are sets M'_i, $i = 1, \dots, n$, such that

$$f(M'_1, \dots, M'_j, \dots, M'_n)$$

contains at least two elements and every M'_i, $i \neq j$, contains only one element.

Theorem 1. *Let the function* $f(x_1, \ldots, x_n) \in \mathfrak{F}^N_{M_1, \ldots, M_n}$ *depend essentially on all of its* n *variables,* $n \geqq 2$. *Then there is an index* j *and an element* $c \in M_j$ *such that the function*

$$f(x_1, \ldots, x_{j-1}, c, x_{j+1}, \ldots, x_n)$$

depends essentially on all of its $n-1$ *variables.*

Proof. For $n = 2$, the assertion follows by the definition of essential variables. (In fact, we may choose $j = 1$ or $j = 2$.) We, therefore, assume that $n > 2$.

Because f depends essentially on the variable x_1, we have

$$f(a_1, a_2, \ldots, a_n) \neq f(a_1', a_2, \ldots, a_n),$$

for some $a_1' \in M_1$, and $a_i \in M_i$, $i = 1, \ldots, n$. Hence, the function $f(x_1, a_2, \ldots, a_n)$ depends essentially on the variable x_1. I.e., we have replaced $n-1$ variables of f by constants (elements of the sets M_i) in such a way that f depends essentially on the remaining variable.

We shall now make the following hypothesis of induction: we have replaced $n-k$ variables of f, $1 \leqq k < n-1$, by constants b_i in such a way that f depends essentially on the remaining k variables. By a suitable renumbering of the variables, we may assume that they are the first k variables, i.e. the function

$$f_1(x_1, \ldots, x_k) = f(x_1, \ldots, x_k, b_{k+1}, \ldots, b_n)$$

depends essentially on all of its k variables.

Let l, $k+1 \leqq l \leqq n$, be the number defined as follows: for some elements $c_i \in M_i$, $k+1 \leqq i \leqq l$,

$$(1) \quad f(x_1, \ldots, x_k, c_{k+1}, \ldots, c_{l-1}, c_l, b_{l+1}, \ldots, b_n) \neq f_1(x_1, \ldots, x_k)$$

whereas, for all elements $y_i \in M_i$, $k+1 \leqq i \leqq l-1$,

$$(2) \quad f(x_1, \ldots, x_k, y_{k+1}, \ldots, y_{l-1}, b_l, \ldots, b_n) = f_1(x_1, \ldots, x_k).$$

Such a number l exists because, otherwise, f would depend essentially on the variables $x_1, \ldots, x_k$ only. The function

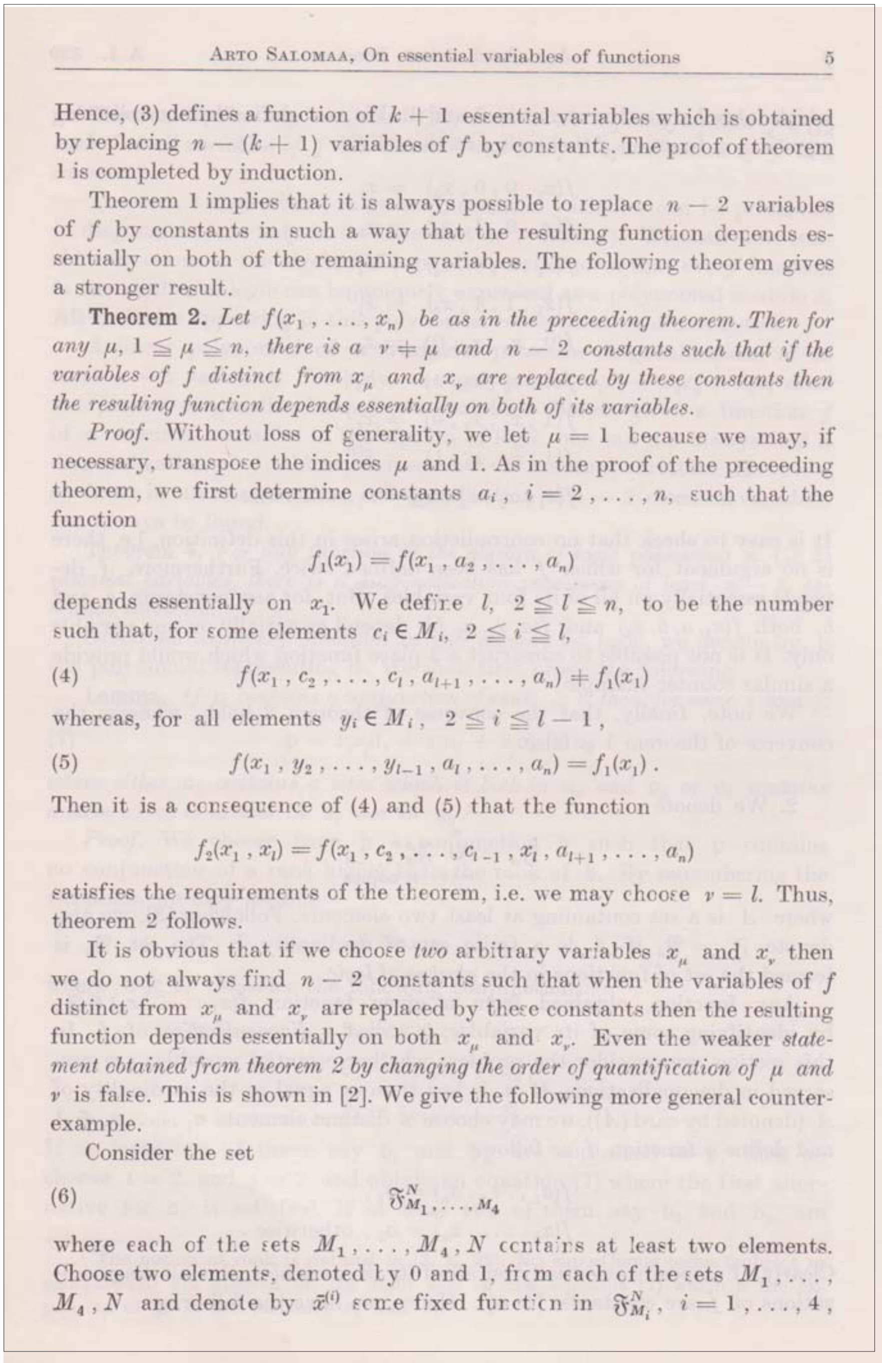
$$(3) \quad f_2(x_1, \ldots, x_k, x_l) = f(x_1, \ldots, x_k, c_{k+1}, \ldots, c_{l-1}, x_l, b_{l+1}, \ldots, b_n)$$

depends essentially on all of its $k+1$ variables. In fact, by (2) and (1),

$$f_2(x_1, \ldots, x_k, b_l) = f_1(x_1, \ldots, x_k)$$

and

$$f_2(x_1, \ldots, x_k, c_l) \neq f_1(x_1, \ldots, x_k).$$



Hence, (3) defines a function of $k+1$ essential variables which is obtained by replacing $n-(k+1)$ variables of f by constants. The proof of theorem 1 is completed by induction.

Theorem 1 implies that it is always possible to replace $n-2$ variables of f by constants in such a way that the resulting function depends essentially on both of the remaining variables. The following theorem gives a stronger result.

Theorem 2. *Let $f(x_1, \ldots, x_n)$ be as in the preceeding theorem. Then for any μ, $1 \leqq \mu \leqq n$, there is a $\nu \neq \mu$ and $n-2$ constants such that if the variables of f distinct from x_μ and x_ν are replaced by these constants then the resulting function depends essentially on both of its variables.*

Proof. Without loss of generality, we let $\mu = 1$ because we may, if necessary, transpose the indices μ and 1. As in the proof of the preceeding theorem, we first determine constants a_i, $i = 2, \ldots, n$, such that the function

$$f_1(x_1) = f(x_1, a_2, \ldots, a_n)$$

depends essentially on x_1. We define l, $2 \leqq l \leqq n$, to be the number such that, for some elements $c_i \in M_i$, $2 \leqq i \leqq l$,

$$f(x_1, c_2, \ldots, c_l, a_{l+1}, \ldots, a_n) \neq f_1(x_1) \tag{4}$$

whereas, for all elements $y_i \in M_i$, $2 \leqq i \leqq l-1$,

$$f(x_1, y_2, \ldots, y_{l-1}, a_l, \ldots, a_n) = f_1(x_1)\,. \tag{5}$$

Then it is a consequence of (4) and (5) that the function

$$f_2(x_1, x_l) = f(x_1, c_2, \ldots, c_{l-1}, x_l, a_{l+1}, \ldots, a_n)$$

satisfies the requirements of the theorem, i.e. we may choose $\nu = l$. Thus, theorem 2 follows.

It is obvious that if we choose *two* arbitrary variables x_μ and x_ν then we do not always find $n-2$ constants such that when the variables of f distinct from x_μ and x_ν are replaced by these constants then the resulting function depends essentially on both x_μ and x_ν. Even the weaker *statement obtained from theorem 2 by changing the order of quantification of μ and ν* is false. This is shown in [2]. We give the following more general counterexample.

Consider the set

$$\mathfrak{F}^N_{M_1, \ldots, M_4} \tag{6}$$

where each of the sets $M_1, \ldots, M_4, N$ contains at least two elements. Choose two elements, denoted by 0 and 1, from each of the sets $M_1, \ldots, M_4, N$ and denote by $\bar{x}^{(i)}$ some fixed function in $\mathfrak{F}^N_{M_i}$, $i = 1, \ldots, 4$, which interchanges the elements 0 and 1. We now define by the following equations a function f belonging to the set (6):

$$\begin{aligned} f(x_1\,,0\,,0\,,x_4) &= x_1\,, \\ f(x_1\,,0\,,1\,,x_4) &= x_4\,, \\ f(x_1\,,1\,,0\,,x_4) &= \bar{x}_4^{(4)}\,, \\ f(x_1\,,1\,,1\,,x_4) &= \bar{x}_1^{(1)}\,, \\ f(0\,,x_2\,,x_3\,,0) &= x_2\,, \\ f(0\,,x_2\,,x_3\,,1) &= x_3\,, \\ f(1\,,x_2\,,x_3\,,0) &= \bar{x}_3^{(3)}\,, \\ f(1\,,x_2\,,x_3\,,1) &= \bar{x}_2^{(2)}\,, \\ f(x_1\,,x_2\,,x_3\,,x_4) &= x_1\,, \text{ otherwise}\,. \end{aligned}$$

It is easy to check that no contradiction arises in this definition, i.e. there is no argument for which f has been defined twice. Furthermore, f depends essentially on all of its four variables. But, for any constants a and b, both $f(x_1, a, b, x_4)$ and $f(a, x_2, x_3, b)$ depend essentially on one variable only. It is not possible to construct a 3-place function which would provide a similar counter-example.

We note, finally, that the converse of theorem 2 holds, whereas the converse of theorem 1 is false.

2. We denote

$$\mathfrak{F}_A = \bigcup_{n=1}^{\infty} \mathfrak{F}^{A}_{\underbrace{A,\ldots,A}_{n \text{ copies}}}$$

where A is a set containing at least two elements. Following [3], we also denote $\mathfrak{F}_A = \mathfrak{P}_k$ if A is a finite set of cardinality k. The set $\mathfrak{P}_2$ is termed the set of functions in the *algebra of logic*.

Any function, obtained from a given function $f(x_1\,,\ldots,x_n) \in \mathfrak{F}_A$ by identifying some of its variables, is called a *diagonalization* of f. In this section, we consider the problem whether essential variables are preserved in diagonalizations. If n is less than or equal to the cardinality of A (denoted by card (A)), we may choose n distinct elements $a_1\,,\ldots,a_n \in A$ and define a function f as follows:

$$\begin{aligned} f(a_1\,,\ldots,a_n) &= a_1\,, \\ f(x_1\,,\ldots,x_n) &= a_2\,, \text{ otherwise}\,. \end{aligned}$$

Clearly, f depends essentially on all of its n variables. But all diagonalizations of f are constants $(= a_2)$. Hence, we have the following

Theorem 3. *For any $n \leqq$ card (A), there is an n-place function $f \in \mathfrak{F}_A$ such that all variables of f are essential and every diagonalization of f is a constant.*

Theorem 3 shows that, in general, essential variables can be preserved in diagonalizations only in the case that $n >$ card(A). We shall now consider functions in the algebra of logic. It is well-known that every function in the algebra of logic can be uniquely expressed as a polynomial modulo 2. All variables appearing in this polynomial representation are essential.

A linear polynomial of n variables possesses diagonalizations of at most $n-2$ variables. Similarly, the polynomial $x_1x_2 + x_2x_3 + x_3x_1$ does not possess diagonalizations of two variables. Hence, given a function f of n essential variables in the algebra of logic, one can not always find a diagonalization of f which possesses $n-1$ essential variables. However, as shown in our next theorem, a diagonalization of $n-2$ essential variables can always be found.

Theorem 4. *For any function in the algebra of logic possessing n $(\geqq 2)$ essential variables, there is a diagonalization possessing at least $n-2$ essential variables.*

Given an arbitrary function in the algebra of logic, we denote by $\mathfrak{p}$ the polynomial representing it. We shall first prove the following

Lemma. *If $\mathfrak{p}$ contains a conjunction of rank $\geqq 3$ then, for some i and j,*

$$\mathfrak{p} = x_ix_j\mathfrak{a}_1 + x_i\mathfrak{a}_2 + x_j\mathfrak{a}_3 + \mathfrak{a}_4 \tag{7}$$

where either $\mathfrak{a}_1$ contains a term which is both in $\mathfrak{a}_2$ and $\mathfrak{a}_3$ or $\mathfrak{a}_1$ contains a term which is neither in $\mathfrak{a}_2$ nor in $\mathfrak{a}_3$.[1]

Proof. We choose from $\mathfrak{p}$ a conjunction $\mathfrak{b}$ such that $\mathfrak{p}$ contains no conjunction of a rank higher than the rank of $\mathfrak{b}$. By renumbering the variables, we may assume

$$\mathfrak{b} = x_1x_2 \dots x_k$$

where $k \geqq 3$. Consider the following conjunctions:

$$\mathfrak{b}_1 = x_1x_2x_4 \dots x_k\,,$$

$$\mathfrak{b}_2 = x_1x_3x_4 \dots x_k\,,$$

$$\mathfrak{b}_3 = x_2x_3x_4 \dots x_k\,.$$

If at least two of them, say $\mathfrak{b}_1$ and $\mathfrak{b}_2$, are contained in $\mathfrak{p}$, then we choose $i = 2$ and $j = 3$ and obtain an equation (7) where the first alternative for $\mathfrak{a}_1$ is satisfied. If at least two of them, say $\mathfrak{b}_2$ and $\mathfrak{b}_3$, are

[1] The notion of rank is defined in [3, p. 22]. No superfluous terms (subject to cancellation) are allowed on the right side of the equation (7) which is the expansion of $\mathfrak{p}$ in the variables x_i and x_j.

missing from $\mathfrak{p}$, then we choose $i = 1$ and $j = 2$ and obtain an equation (7) where the second alternative for $\mathfrak{a}_1$ is satisfied. This proves our lemma.

Proof of the main theorem. The assertion is trivial for $n = 2$. We assume the assertion holds for $n < m\,(\geqq 3)$. Let $\mathfrak{p}$ be the polynomial representing an arbitrary given function of m essential variables. We separate two cases.

Case 1. $\mathfrak{p}$ contains at least one conjunction of rank $\geqq 3$. We choose variables x_i and x_j as in the lemma and write $\mathfrak{p}$ in the form (7). Next, we define polynomials $\mathfrak{c}_1, \ldots, \mathfrak{c}_7$ as follows:

$\mathfrak{c}_1$ consists of terms common to $\mathfrak{a}_1$, $\mathfrak{a}_2$ and $\mathfrak{a}_3$.

$\mathfrak{c}_i$, $i = 2, 3$, consists of those terms common to $\mathfrak{a}_1$ and $\mathfrak{a}_i$ which are not in $\mathfrak{c}_1$.

$\mathfrak{c}_4$ consists of those terms common to $\mathfrak{a}_2$ and $\mathfrak{a}_3$ which are not in $\mathfrak{c}_1$.

$\mathfrak{c}_{4+i}$, $i = 1, 2, 3$, consists of the remaining terms in $\mathfrak{a}_i$.

Hence,

$$\mathfrak{p} = x_i x_j(\mathfrak{c}_1 + \mathfrak{c}_2 + \mathfrak{c}_3 + \mathfrak{c}_5) + x_i(\mathfrak{c}_1 + \mathfrak{c}_2 + \mathfrak{c}_4 + \mathfrak{c}_6) + x_j(\mathfrak{c}_1 + \mathfrak{c}_3 + \mathfrak{c}_4 + \mathfrak{c}_7) + \mathfrak{a}_4\,. \tag{8}$$

According to the choice of x_i and x_j,

$$\mathfrak{c}_1 + \mathfrak{c}_5 \neq 0\,. \tag{9}$$

We now form a diagonalization $\mathfrak{p}'$ by identifying x_i and x_j. Clearly,

$$\mathfrak{p}' = x_i(\mathfrak{c}_1 + \mathfrak{c}_5 + \mathfrak{c}_6 + \mathfrak{c}_7) + \mathfrak{a}_4\,.$$

We denote

$$\mathfrak{c}' = \mathfrak{c}_2 + \mathfrak{c}_3 + \mathfrak{c}_4$$

and refer to the variables which appear in $\mathfrak{c}'$ but do not appear elsewhere in $\mathfrak{p}$ as *ζ-variables.* If r is the number of ζ-variables then, by the choice of the polynomials $\mathfrak{c}_i$, $\mathfrak{p}'$ possesses $m - (r + 1)$ essential variables. Hence, if $r = 0$ or $r = 1$ we obtain the required diagonalization by identifying x_i and x_j.

We, therefore, assume that $r \geqq 2$. (Clearly, $r \leqq m - 2$.) Our inductive assumption implies that we may identify some ζ-variables in such a way that, after the identification, the resulting polynomial contains at least $r - 2$ ζ-variables. (In this identification, some variables other than ζ-variables may vanish from $\mathfrak{c}'$.) This identification gives the required diagonalization because no variables other than ζ-variables vanish from $\mathfrak{p}$. In particular, by (8) and (9), x_i and x_j are preserved.

Case 2. $\mathfrak{p}$ contains only conjunctions of ranks 1 and 2. If $\mathfrak{p}$ is linear we may identify any two variables. Otherwise, we choose some non-linear term, say $x_1 x_2$, and write

$$\mathfrak{p} = x_1x_2 + x_1(\mathfrak{d}_1 + \mathfrak{d}_2) + x_2(\mathfrak{d}_1 + \mathfrak{d}_3) + \mathfrak{d}_4$$

where $\mathfrak{d}_1$, $\mathfrak{d}_2$, $\mathfrak{d}_3$ are linear and $\mathfrak{d}_2$ and $\mathfrak{d}_3$ do not contain common terms. We separate three subcases.

Subcase 2a. $\mathfrak{d}_1$ contains at least two variables which do not appear elsewhere in $\mathfrak{p}$. We may identify any two such variables.

Subcase 2b. Every variable of $\mathfrak{d}_1$ appears also elsewhere in $\mathfrak{p}$. In this case, we identify x_1 and x_2.

Subcase 2c. $\mathfrak{d}_1$ contains exactly one variable, say x_3, which does not appear elsewhere in $\mathfrak{p}$. We identify first x_1 and x_2. If the resulting polynomial depends on the variable identified we have finished the proof. Otherwise, $\mathfrak{p}$ is of one of the forms

$$\mathfrak{p} = x_1x_2 + x_1(x_3 + 1) + x_2x_3 + \mathfrak{d}_4$$

or

$$\mathfrak{p} = x_1x_2 + x_1x_3 + x_2(x_3 + 1) + \mathfrak{d}_4 .$$

In the former case, we identify x_2 and x_3, in the latter, x_1 and x_3.

We have, thus, completed the induction. (In fact, the inductive assumption was not used in case 2.) This proves theorem 4.

The proof is easier in some special cases as, for instance, if $\mathfrak{p}$ contains some conjunction of rank $\geqq n - 3$. It is also easy to see that the statement analogous to theorem 2 is false for diagonalizations of functions in the algebra of logic. In fact, if we choose some variable x_μ it may happen that, for any other variable x_ν, the diagonalization obtained by identifying x_μ and x_ν is a constant.

3. Jablonskiĭ has proved in [3, pp. 68—70] the following

Fundamental lemma. *Let $f(x_1, \ldots, x_n) \in \mathfrak{P}_k$ $(k \geqq 3)$ depend essentially on at least two variables and assume $l > 2$ values. Then there are sets G_i, $i = 1, \ldots, n$, each containing at most two elements such that the set $f(G_1, \ldots, G_n)$ contains at least three elements.*

This lemma is an efficient tool in establishing completeness criteria for sets of functions over a finite domain, and in some analogous problems. We shall now extend the lemma to arbitrary sets $\mathfrak{F}_A$ where $\mathrm{card}(A) \geqq 3$. Furthermore, we strengthen it by constructing the sets G_i in such a way that an arbitrary preassigned value of the function f is included in the set $f(G_1, \ldots, G_n)$.

Theorem 5. *Let $\mathrm{card}(A) \geqq 3$ and $f(x_1, \ldots, x_n) \in \mathfrak{F}_A$ depend essentially on at least two variables and assume at least three values and let a be one of these values. Then there are sets $G_i \subset A$, $i = 1, \ldots, n$, each consisting of at most two elements such that $f(G_1, \ldots, G_n)$ contains at least three elements, one of which is a.*

Proof. We first choose elements $a_1, \ldots, a_n \in A$ such that

$$f(a_1, \ldots, a_n) = a \,.$$

Let U be the set of n-tuples $(u_1, \ldots, u_n)$ where, for $n-1$ elements u_i, $u_i = a_i$ and the n^{th} element u_i is arbitrary $\in A$. Denote by $f(U)$ the set of values assumed by f when its argument is restricted to the elements of U. Clearly, $a \in f(U)$. We may assume that $f(U)$ contains an element $b \neq a$. For if all elements in U satisfy the equation

$$f(u_1, \ldots, u_n) = a$$

then our original n-tuple $(a_1, \ldots, a_n)$ may be replaced by any element in U. Then, for every n-tuple in U, we form the set of n-tuples differing by at most one coordinate from the given n-tuple and, if necessary, continue the process. Because f does not assume the constant value a we obtain an element b as required. By a suitable renumbering of the variables, we may assume that

$$a = f(a_1, \ldots, a_{n-1}, a_n) \neq f(a_1, \ldots, a_{n-1}, b_n) = b \,. \tag{10}$$

In what follows, we separate cases and subcases.

Case 1. There is an n-tuple $(c_1, \ldots, c_n)$ where $c_n = a_n$ or $c_n = b_n$ such that

$$f(c_1, \ldots, c_n) \neq a \,, b \,.$$

Then, by (10), we may choose $G_i = \{a_i, c_i\}$, for $i = 1, \ldots, n-1$, and $G_n = \{a_n, b_n\}$.

Case 2. For all n-tuples $(y_1, \ldots, y_n)$ where $y_n = a_n$ or $y_n = b_n$,

$$f(y_1, \ldots, y_n) = a \text{ or } f(y_1, \ldots, y_n) = b \,.$$

Subcase 2a. All values assumed by f can not be represented in the form

$$f(a_1, \ldots, a_{n-1}, x_n) \tag{11}$$

where x_n runs through the elements of A. This implies that there is a $d \in A$ such that, for some n-tuple $(d_1, \ldots, d_n)$,

$$f(d_1, \ldots, d_n) = d$$

and, for every n-tuple $(a_1, \ldots, a_{n-1}, x_n)$,

$$f(a_1, \ldots, a_{n-1}, x_n) \neq d \,.$$

Hence, by (10), $d \neq a$, b. By the assumption of case 2, $d_n \neq a_n \,.\, b_n$. Denote

$$e = f(a_1, \ldots, a_{n-1}, d_n) \,.$$

According to the definition of d, $e \neq d$.

If $e = a$ we choose $G_i = \{a_i , d_i\}$, for $i = 1, \ldots, n-1$, and $G_n = \{b_n , d_n\}$,

If $e \neq a$ we choose $G_i = \{a_i , d_i\}$, for $i = 1, \ldots, n$.

Subcase 2b. All values assumed by f can be represented in the form (11). Hence, there are at least three distinct values of the form (11).

There is an n-tuple $(h_1, \ldots, h_n)$ such that

$$h' = f(a_1, \ldots, a_{n-1}, h_n) \neq f(h_1, \ldots, h_{n-1}, h_n) = h \tag{12}$$

because, otherwise, f would depend essentially on the last variable only.

Suppose $a = h$ or $a = h'$. By the assumption of subcase 2b, there is an element $h_n' \in A$ such that

$$f(a_1, \ldots, a_{n-1}, h_n') \neq h, h' .$$

By (12), we may choose $G_i = \{a_i , h_i\}$, for $i = 1, \ldots, n-1$, and $G_n = \{h_n , h_n'\}$.

Suppose $a \neq h, h'$. Then we may choose $G_i = \{a_i, h_i\}$, for $i = 1, \ldots, n$.

Thus, we have completed the proof of theorem 5 in all cases.

In general, it is not possible to construct the sets G_i in such a way that *two* arbitrary preassigned values of the function f are included in the set $f(G_1, \ldots, G_n)$. Thus, a further strengthening of the fundamental lemma in this direction is not possible. We shall finally mention a consequence of theorem 5 which can be proved by an easy induction. (Cf. the proof of consequence 1 in [3, p. 70].)

Theorem 6. *Let* $\mathrm{card}(A) \geqq 3$ *and* $f(x_1, \ldots, x_n) \in \mathfrak{F}_A$ *depend essentially on at least two variables and assume at least* $r+2$ *values and let* $a_1, \ldots, a_r$ *be some of these values. Then there are sets* $G_i \subset A$, $i = 1, \ldots, n$, *each consisting of at most* $r+1$ *elements such that* $f(G_1, \ldots, G_n)$ *contains at least* $r+2$ *elements, including the elements* $a_1, \ldots, a_r$.

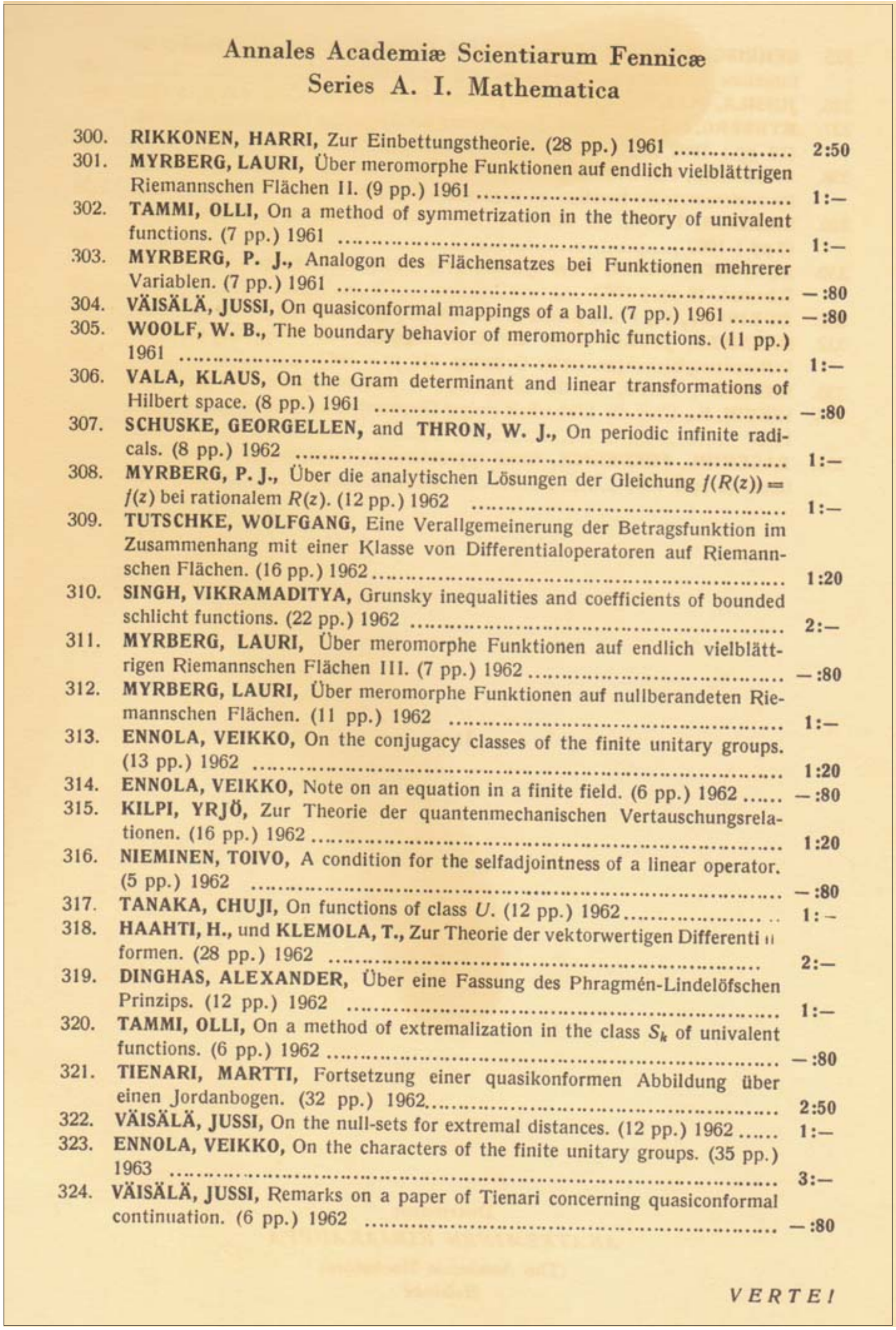
References

[1] Лупанов, О. Б.: Об одном классе схем из функциональных элементов. - Сб. »Проблемы кибернетики», 7 (1962), 61—114.

[2] Соловьев, Н. А.: К вопросу о существенной зависимости функций алгебры логики. - Сб. «Проблемы кибернетики», 9 (1963), 333—335.

[3] Яблонский, С. В.: Функциональные построения в κ-значной логике. - Тр. Матем. инст. им. В. А. Стеклова, 51 (1958), 5—142.

Printed November 1963.



Annales Academiæ Scientiarum Fennicæ
Series A. I. Mathematica

300. **RIKKONEN, HARRI,** Zur Einbettungstheorie. (28 pp.) 1961 **2:50**

301. **MYRBERG, LAURI,** Über meromorphe Funktionen auf endlich vielblättrigen Riemannschen Flächen II. (9 pp.) 1961 **1:—**

302. **TAMMI, OLLI,** On a method of symmetrization in the theory of univalent functions. (7 pp.) 1961 **1:—**

303. **MYRBERG, P. J.,** Analogon des Flächensatzes bei Funktionen mehrerer Variablen. (7 pp.) 1961 **—:80**

304. **VÄISÄLÄ, JUSSI,** On quasiconformal mappings of a ball. (7 pp.) 1961 **—:80**

305. **WOOLF, W. B.,** The boundary behavior of meromorphic functions. (11 pp.) 1961 **1:—**

306. **VALA, KLAUS,** On the Gram determinant and linear transformations of Hilbert space. (8 pp.) 1961 **—:80**

307. **SCHUSKE, GEORGELLEN,** and **THRON, W. J.,** On periodic infinite radicals. (8 pp.) 1962 **1:—**

308. **MYRBERG, P. J.,** Über die analytischen Lösungen der Gleichung $f(R(z)) = f(z)$ bei rationalem $R(z)$. (12 pp.) 1962 **1:—**

309. **TUTSCHKE, WOLFGANG,** Eine Verallgemeinerung der Betragsfunktion im Zusammenhang mit einer Klasse von Differentialoperatoren auf Riemannschen Flächen. (16 pp.) 1962 **1:20**

310. **SINGH, VIKRAMADITYA,** Grunsky inequalities and coefficients of bounded schlicht functions. (22 pp.) 1962 **2:—**

311. **MYRBERG, LAURI,** Über meromorphe Funktionen auf endlich vielblättrigen Riemannschen Flächen III. (7 pp.) 1962 **—:80**

312. **MYRBERG, LAURI,** Über meromorphe Funktionen auf nullberandeten Riemannschen Flächen. (11 pp.) 1962 **1:—**

313. **ENNOLA, VEIKKO,** On the conjugacy classes of the finite unitary groups. (13 pp.) 1962 **1:20**

314. **ENNOLA, VEIKKO,** Note on an equation in a finite field. (6 pp.) 1962 **—:80**

315. **KILPI, YRJÖ,** Zur Theorie der quantenmechanischen Vertauschungsrelationen. (16 pp.) 1962 **1:20**

316. **NIEMINEN, TOIVO,** A condition for the selfadjointness of a linear operator. (5 pp.) 1962 **—:80**

317. **TANAKA, CHUJI,** On functions of class U. (12 pp.) 1962 **1:—**

318. **HAAHTI, H.,** und **KLEMOLA, T.,** Zur Theorie der vektorwertigen Differentialformen. (28 pp.) 1962 **2:—**

319. **DINGHAS, ALEXANDER,** Über eine Fassung des Phragmén-Lindelöfschen Prinzips. (12 pp.) 1962 **1:—**

320. **TAMMI, OLLI,** On a method of extremalization in the class S_k of univalent functions. (6 pp.) 1962 **—:80**

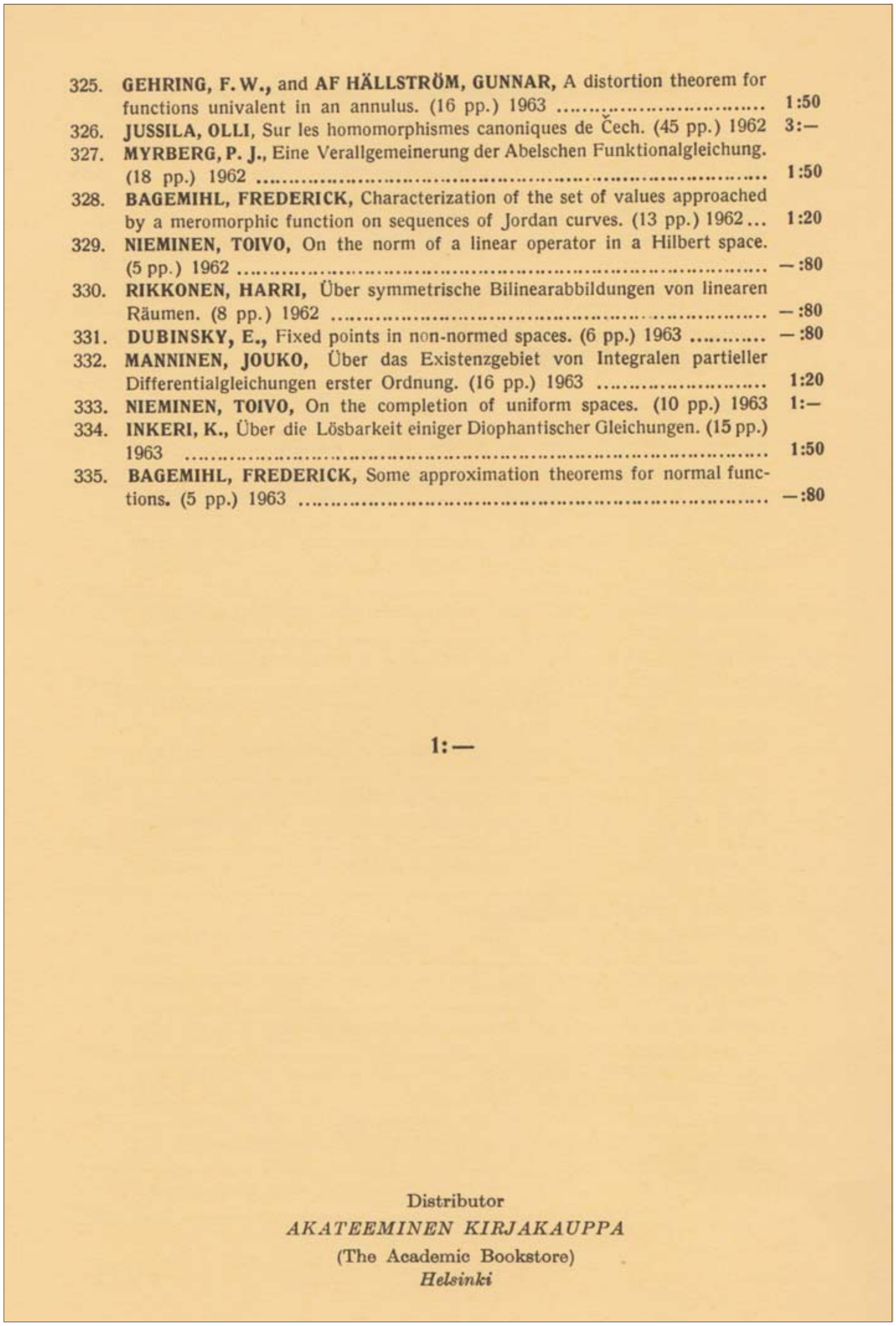
321. **TIENARI, MARTTI,** Fortsetzung einer quasikonformen Abbildung über einen Jordanbogen. (32 pp.) 1962 **2:50**

322. **VÄISÄLÄ, JUSSI,** On the null-sets for extremal distances. (12 pp.) 1962 **1:—**

323. **ENNOLA, VEIKKO,** On the characters of the finite unitary groups. (35 pp.) 1963 **3:—**

324. **VÄISÄLÄ, JUSSI,** Remarks on a paper of Tienari concerning quasiconformal continuation. (6 pp.) 1962 **—:80**

VERTE!



325. **GEHRING, F. W., and AF HÄLLSTRÖM, GUNNAR,** A distortion theorem for functions univalent in an annulus. (16 pp.) 1963 .... 1:50

326. **JUSSILA, OLLI,** Sur les homomorphismes canoniques de Čech. (45 pp.) 1962 3:—

327. **MYRBERG, P. J.,** Eine Verallgemeinerung der Abelschen Funktionalgleichung. (18 pp.) 1962 .... 1:50

328. **BAGEMIHL, FREDERICK,** Characterization of the set of values approached by a meromorphic function on sequences of Jordan curves. (13 pp.) 1962 ... 1:20

329. **NIEMINEN, TOIVO,** On the norm of a linear operator in a Hilbert space. (5 pp.) 1962 .... —:80

330. **RIKKONEN, HARRI,** Über symmetrische Bilinearabbildungen von linearen Räumen. (8 pp.) 1962 .... —:80

331. **DUBINSKY, E.,** Fixed points in non-normed spaces. (6 pp.) 1963 .... —:80

332. **MANNINEN, JOUKO,** Über das Existenzgebiet von Integralen partieller Differentialgleichungen erster Ordnung. (16 pp.) 1963 .... 1:20

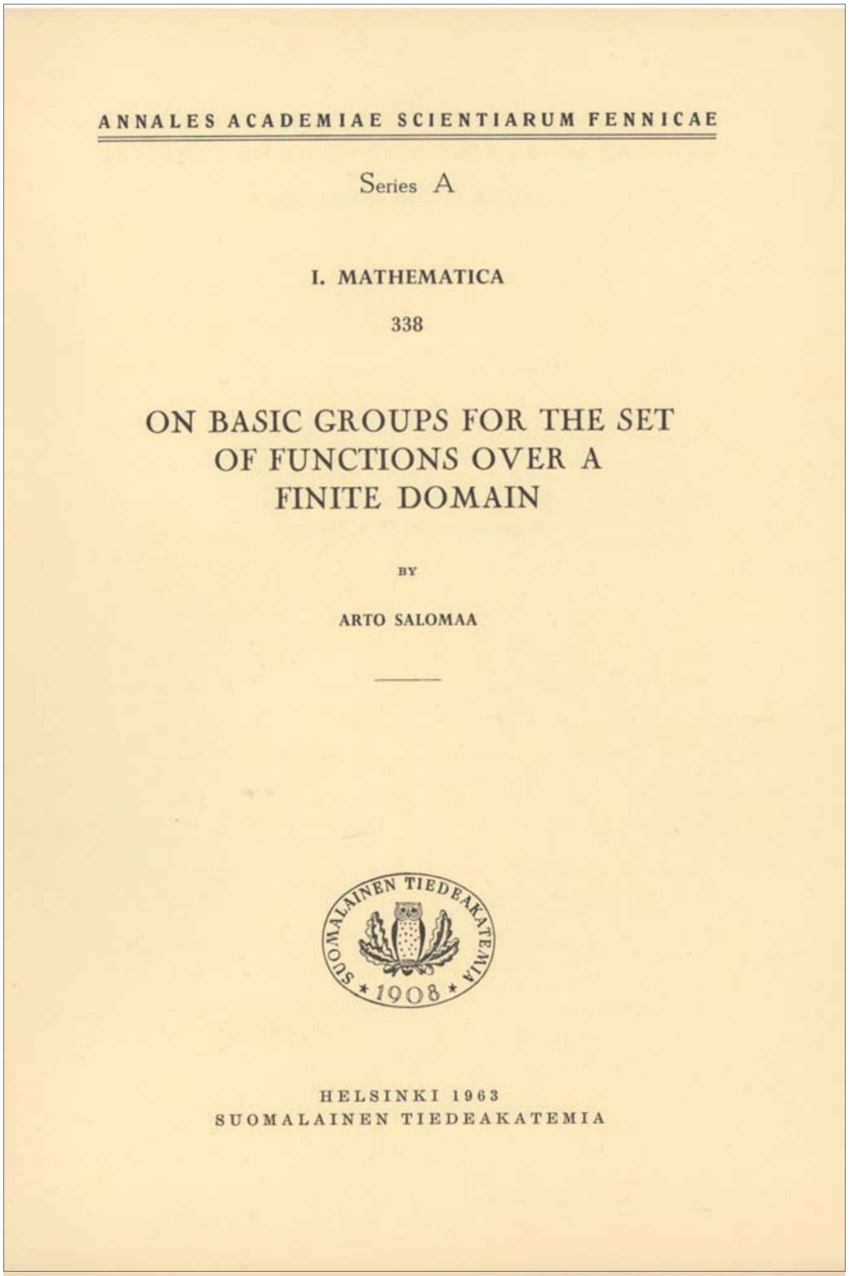
333. **NIEMINEN, TOIVO,** On the completion of uniform spaces. (10 pp.) 1963 1:—

334. **INKERI, K.,** Über die Lösbarkeit einiger Diophantischer Gleichungen. (15 pp.) 1963 .... 1:50

335. **BAGEMIHL, FREDERICK,** Some approximation theorems for normal functions. (5 pp.) 1963 .... —:80

1:—

Distributor
AKATEEMINEN KIRJAKAUPPA
(The Academic Bookstore)
Helsinki



ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

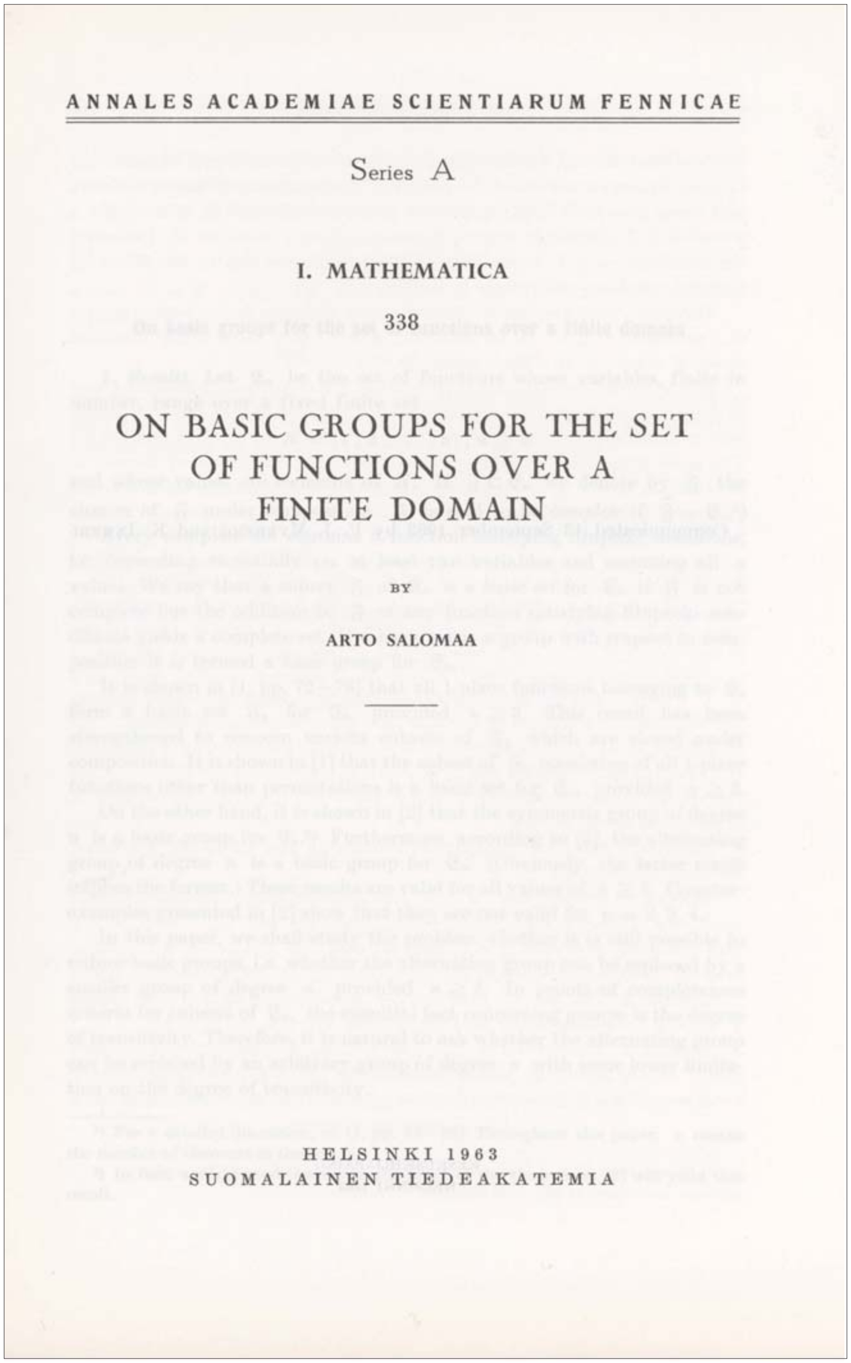
338

ON BASIC GROUPS FOR THE SET OF FUNCTIONS OVER A FINITE DOMAIN

BY

ARTO SALOMAA

HELSINKI 1963
SUOMALAINEN TIEDEAKATEMIA



ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

338

ON BASIC GROUPS FOR THE SET OF FUNCTIONS OVER A FINITE DOMAIN

BY

ARTO SALOMAA

HELSINKI 1963
SUOMALAINEN TIEDEAKATEMIA

Communicated 13 September 1963 by P. J. Myrberg and K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1963

On basic groups for the set of functions over a finite domain

1. *Results.* Let $\mathfrak{C}_n$ be the set of functions whose variables, finite in number, range over a fixed finite set

$$N = \{1, 2, \ldots, n\}, n \geqq 2$$

and whose values are elements of N. If $\mathfrak{F} \subset \mathfrak{C}_n$ we denote by $\overline{\mathfrak{F}}$ the closure of $\mathfrak{F}$ under composition. $\mathfrak{F}$ is said to be *complete* if $\overline{\mathfrak{F}} = \mathfrak{C}_n$.[1])

Every complete set contains a function satisfying *Słupecki conditions*, i.e. depending essentially on at least two variables and assuming all n values. We say that a subset $\mathfrak{F}$ of $\mathfrak{C}_n$ is a *basic set* for $\mathfrak{C}_n$ if $\mathfrak{F}$ is not complete but the addition to $\mathfrak{F}$ of any function satisfying Słupecki conditions yields a complete set. If a basic set is a group with respect to composition it is termed a *basic group* for $\mathfrak{C}_n$.

It is shown in [1, pp. 72—76] that all 1-place functions belonging to $\mathfrak{C}_n$ form a basic set $\mathfrak{F}_1$ for $\mathfrak{C}_n$, provided $n \geqq 3$. This result has been strengthened to concern various subsets of $\mathfrak{F}_1$ which are closed under composition. It is shown in [1] that the subset of $\mathfrak{F}_1$ consisting of all 1-place functions other than permutations is a basic set for $\mathfrak{C}_n$, provided $n \geqq 3$.

On the other hand, it is shown in [2] that the symmetric group of degree n is a basic group for $\mathfrak{C}_n$.[2]) Furthermore, according to [3], the alternating group of degree n is a basic group for $\mathfrak{C}_n$. (Obviously, the latter result implies the former.) These results are valid for all values of $n \geqq 5$. Counterexamples presented in [2] show that they are not valid for $n = 2, 3, 4$.

In this paper, we shall study the problem whether it is still possible to reduce basic groups, i.e. whether the alternating group can be replaced by a smaller group of degree n, provided $n \geqq 5$. In proofs of completeness criteria for subsets of $\mathfrak{C}_n$, the essential fact concerning groups is the degree of transitivity. Therefore, it is natural to ask whether the alternating group can be replaced by an arbitrary group of degree n with some lower limitation on the degree of transitivity.

[1]) For a detailed discussion, cf. [1, pp. 56—58]. Throughout this paper, n means the number of elements in the set N.

[2]) In fact, a slight modification in the proof of the theorem in [2] will yield this result.

It is clear that an arbitrary doubly transitive group is not basic for $\mathfrak{E}_n$. Counter-examples are found, for instance, by considering prime values of n and linear groups. A triply transitive group is basic for $\mathfrak{E}_n$ if n is not a power of 2. A quadruply transitive group is always basic for $\mathfrak{E}_n$ (provided the condition $n \geqq 5$ is satisfied). These results are due to the following theorem which we shall prove in section 2.

Theorem. *Every quadruply transitive group of degree n is a basic group for $\mathfrak{E}_n$, provided $n \geqq 5$. If, in addition, $n \neq 2^r$ then every triply transitive group of degree n is a basic group for $\mathfrak{E}_n$.*

It is a consequence of this theorem that if a quadruply transitive group of degree n is contained in the closure of a function $f \in \mathfrak{E}_n$ (i.e. if f *generates* a quadruply transitive group) then the unit set of f is complete.[1]) The same statement holds true for triply transitive groups of degree n, provided $n \neq 2^r, r \geqq 3$. It is very likely that the statement holds true for arbitrary triply transitive groups, perhaps even for arbitrary doubly transitive groups if $n \geqq 3$.

In section 3, we consider the exceptional cases in our theorem: $n = 2^r$, $r \geqq 3$. We construct a triply transitive group of degree 2^r which is not a basic group for $\mathfrak{E}_{2^r}$. Such a counter-example is provided by the holomorph of an Abelian group of order 2^r and type $(1, 1, \ldots, 1)$.

2. *Proofs.* To prove our theorem, we shall first establish several lemmas. We shall use the terms *genus* and *type* (of 1-place functions belonging to $\mathfrak{E}_n$) as defined in [3]. Assume that G_i, $i = 1, \ldots, k$, are non-empty subsets of N. Then, for any function $f(x_1, \ldots, x_k) \in \mathfrak{E}_n$, we denote by $f(G_1, \ldots, G_k)$ the set of values assumed by f when, for $i = 1, \ldots, k$, the variable x_i is restricted to the set G_i.

Lemmas 1 and 2 are the same as lemmas 1.1 and 1.3 in [3]. Therefore, we omit their proofs.

Lemma 1. *Assume that $n \geqq 3$ and $f(x_1, \ldots, x_k)$ satisfies Slupecki condiions. Then for any $j, 3 \leqq j \leqq n$, there are sets G_i, $i = 1, \ldots, k$, each consisting of a most $j - 1$ elements such that $f(G_1, \ldots, G_k)$ contains at least j elements.*

Lemma 2. *The set of functions of type $[b_1, b_2, b_3, \ldots, b_t]$ where $1 < t < n$ generates every function of type $[b_1 + b_2, b_3, \ldots, b_t]$.*

Lemma 3. *Assume that $n \geqq 4$ and $\mathfrak{F} \subset \mathfrak{E}_n$ contains a triply transitive group $\mathfrak{G}$ (of degree n) and a function $f(x_1, \ldots, x_k)$ satisfying Slupecki conditions. Then $\mathfrak{F}$ generates a function of genus 2 and all functions of genus 1.*

[1]) This means that f is a so-called *Sheffer function*. The result is valid for $n \geq 4$ because, according to [3], it is valid for $n = 4$.

Proof. I. We shall first prove that $\mathfrak{F}$ generates a function $g(x)$ whose genus γ satisfies $1 < \gamma < n$.

By lemma 1, there are numbers $a_1, \ldots, a_k$ such that

$$f(G_1, \ldots, G_k) = N \tag{1}$$

where $G_i = N - \{a_i\}$, for $i = 1, \ldots, k$. By (1), there are numbers a_i', $i = 1, \ldots, k$, such that

$$f(a_1', \ldots, a_k') = f(a_1, \ldots, a_k)$$

and $a_i' \neq a_i$, for $i = 1, \ldots, k$. We choose from $\mathfrak{G}$ k permutations $p_i(x)$, $i = 1, \ldots, k$, such that $p_i(1) = a_i$ and $p_i(2) = a_i'$. The choice is possible because $\mathfrak{G}$ is doubly transitive. Then the function

$$f(p_1(x), \ldots, p_k(x)) \tag{2}$$

is of genus smaller than n. If it is of genus greater than 1 we have found a function $g(x)$ as required.

We, therefore, assume that the function (2) is of genus 1. Hence, $\mathfrak{F}$ generates all functions of genus 1, i.e. all constants. Using lemma 1, we choose sets H_i, $i = 1, \ldots, k$, such that each H_i consists of two (not necessarily distinct) elements b_i and b_i' and $f(H_1, \ldots, H_k)$ contains at least three distinct elements b, b' and b''. By a suitable renumbering of the variables, this choice can be made in such a way that

$$f(b_1, b_2, \ldots, b_k) = b \tag{3}$$

$$f(b_1', b_2, \ldots, b_k) = b' \tag{4}$$

and

$$f(b_1', b_2', \ldots, b_k') = b'' . \tag{5}$$

Consider the 1-place function

$$g_1(x) = f(x, b_2, \ldots, b_k)$$

which is generated by $\mathfrak{F}$. If $g_1(x)$ does not assume the value b'' we may choose $g(x) = g_1(x)$. Suppose

$$g_1(c_1) = b'' . \tag{6}$$

Then necessarily $c_1 \neq b_1, b_1'$. Choose numbers c_2 and $c_{3,i}$, $i = 2, \ldots, k$, such that $c_2 \neq b_1, b_1', c_1$ and $c_{3,i} \neq b_i, b_i'$ if $b_i \neq b_i'$ but $c_{3,i} = b_i$ if $b_i = b_i'$. The choice is possible because $n \geq 4$.

Assume that

$$f(c_2, c_{3,2}, \ldots, c_{3,k}) = b'' . \tag{7}$$

Let $q_i(x)$, $i = 1, \ldots, k$, be constants in $\bar{\mathfrak{F}}$ or permutations in $\mathfrak{G}$, defined as follows. The function $q_1(x)$ is a permutation such that $q_1(1) = c_2$, $q_1(2) = b_1$ and $q_1(3) = b_1'$. Let $2 \leqq i \leqq k$ and $b_i \neq b_i'$. Then $q_i(x)$ is a permutation such that $q_i(1) = c_{3,i}$, $q_i(2) = b_i$ and $q_i(3) = b_i'$. Let $2 \leqq i \leqq k$ and $b_i = b_i'$. Then $q_i(x) = b_i$. By (3), (5) and (7), we may choose

$$g(x) = f(q_1(x), \ldots, q_k(x)).$$

Assume that

$$f(c_2, c_{3,2}, \ldots, c_{3,k}) \neq b''. \tag{8}$$

Let $q_1'(x)$ be a permutation in $\mathfrak{G}$ such that $q_1'(1) = c_2$, $q_1'(2) = c_1$ and $q_1'(3) = b_1'$. By (5), (6) and (8), we may choose

$$g(x) = f(q_1'(x), q_2(x), \ldots, q_k(x)).$$

Thus, in all cases, $\mathfrak{F}$ generates a function $g(x)$ whose genus γ satisfies $1 < \gamma < n$.

II. Assume that $\gamma > 2$. We shall now prove that $\mathfrak{F}$ generates a function $h(x)$ whose genus γ_1 satisfies $2 \leqq \gamma_1 < \gamma$. By repeating the argument, we may conclude that $\mathfrak{F}$ generates a function of genus 2.

Let u be a value assumed by $g(x)$ at least twice and let v and w be any other distinct values of $g(x)$. Hence, there are distinct numbers u_1, u_2 and v_1 such that

$$g(u_1) = g(u_2) = u \text{ and } g(v_1) = v.$$

Choose from $\mathfrak{G}$ a permutation $p(x)$ such that $p(u) = u_1$, $p(w) = u_2$ and $p(v) = v_1$. Then the function

$$h(x) = gpg(x)$$

is of genus γ_1 where $2 \leqq \gamma_1 < \gamma$.

We have, thus, shown that $\mathfrak{F}$ generates a function $h_1(x)$ of genus 2. Let $h_1(d_1) = h_1(d_2) = d$, $d_1 \neq d_2$, and $h_1(d_3) = d'$, $d' \neq d$. To complete the proof of lemma 3, we choose from $\mathfrak{G}$ a permutation $q(x)$ such that $q(d) = d_1$ and $q(d') = d_2$. Then $h_1qh_1(x) = d$. Thus, $\mathfrak{F}$ generates the constant d. Because $\mathfrak{F}$ contains a transitive group, we may conclude that $\mathfrak{F}$ generates all constants. Hence, lemma 3 follows.

Lemma 4. *Assume that* $n \geqq 3$[1]) *and* $\mathfrak{F} \subset \mathfrak{E}_n$ *contains a triply transitive group* $\mathfrak{G}$ *(of degree* n*), a function* $f(x_1, \ldots, x_k)$ *satisfying Słupecki conditions and a function* $g(x)$ *of type* $[n-1, 1]$. *Then* $\mathfrak{F}$ *is complete.*

[1]) For the proof of our theorem, it obviously suffices to consider the cases $n > 4$. A sharper formulation is given to some of the lemmas because their proofs remain unaltered. On the other hand, lemmas 4 and 5 may be considered as completeness criteria for subsets of $\mathfrak{E}_n$, $n \geqq 3$.

Proof. Obviously, any function of type $[n-1, 1]$ may be expressed in the form $p_1 g p_2(x)$ where $p_1(x)$ and $p_2(x)$ are permutations belonging to $\mathfrak{G}$. In fact, p_2 may be chosen from any transitive subgroup of $\mathfrak{G}$ and p_1 may be chosen from any doubly transitive subgroup of $\mathfrak{G}$. Thus, $\mathfrak{F}$ generates all functions of type $[n-1,1]$.

We shall now make the following hypothesis of induction: $\mathfrak{F}$ generates all functions of type

$$(9) \qquad [n-i\,, \underbrace{1\,, \dots\,, 1}_{i \text{ terms}}]$$

where $1 \leqq i < n-2$. We shall prove that this implies that $\mathfrak{F}$ generates all functions of type

$$(10) \qquad [n-(i+1)\,, \underbrace{1\,, \dots\,, 1}_{i+1 \text{ terms}}]\,.$$

We choose numbers b_i and b'_i, $i = 1\,, \dots\,, k$, as in the proof of lemma 3 such that the equations (3) — (5) hold, for some distinct numbers b, b' and b''.

Let $h(x)$ be an arbitrary function of type (10). We have to show that $h(x) \in \overline{\mathfrak{F}}$.

The function $h(x)$ assumes $i+2$ distinct values. Let α_1 be the value assumed by $h(x)$ $n-(i+1)$ times and let U consist of all numbers y such that $h(y) = \alpha_1$. Hence, the cardinality of U (denoted by card(U)) is at least 2. Finally, let the other values assumed by $h(x)$ be $\alpha_2\,, \dots\,, \alpha_{i+2}$ and let u_ν be numbers such that $h(u_\nu) = \alpha_\nu$, for $\nu = 2\,, \dots\,, i+2$.

We choose from $\mathfrak{G}$ a permutation $p(x)$ such that $p(b') = \alpha_1$, $p(b) = \alpha_2$ and $p(b'') = \alpha_3$ and denote

$$(11) \qquad f_1(x_1\,, \dots\,, x_k) = p(f(x_1\,, \dots\,, x_k))\,.$$

Clearly, $f_1(x_1\,, \dots\,, x_k)$ satisfies Słupecki conditions. Therefore, it is possible to choose numbers α^μ_ν, $\mu = 1\,, \dots\,, i-1$, $\nu = 1\,, \dots\,, k$, such that f_1 applied to the μ^{th} row vector of the matrix

$$\begin{Vmatrix} \alpha_1^1 & \dots & \alpha_k^1 \\ \vdots & & \vdots \\ \alpha_1^{i-1} & \dots & \alpha_k^{i-1} \end{Vmatrix}$$

yields the value $\alpha_{\mu+3}$, for any $\mu = 1\,, \dots\,, i-1$.

We now consider auxiliary functions $h_i(x)$, $i = 1\,, \dots\,, k$, defined by the following table:

	$h_1(x)$	$h_2(x)$	$\dots$	$h_k(x)$
$x \in U$	b_1'	b_2		b_k
$x = u_2$	b_1	b_2		b_k
$x = u_3$	b_1'	b_2'		b_k'
$x = u_4$	$\overset{1}{\alpha}_1$	$\overset{1}{\alpha}_2$		$\overset{1}{\alpha}_k$
.				
.				
.				
$x = u_{i+2}$	$\overset{i-1}{\alpha}_1$	$\overset{i-1}{\alpha}_2$		$\overset{i-1}{\alpha}_k$

It follows from our inductive assumption concerning functions of type (9) and lemma 2 that every function assuming some value at least $n - i$ times is generated by $\mathfrak{F}$. Because the functions $h_i(x)$ satisfy this condition, we may conclude that $h_i(x) \in \overline{\mathfrak{F}}$, for $i = 1, \dots, k$.

It is a consequence of (11) and the choice of the functions $h_i(x)$ that

$$h(x) = f_1(h_1(x), \dots, h_k(x)) .$$

Thus, we have shown that all functions of type (10) are generated by $\mathfrak{F}$.

We conclude, by induction, that all functions of type

$$(12) \qquad [2, \underbrace{1, \dots, 1}_{n-2 \text{ terms}}]$$

are generated by $\mathfrak{F}$. By lemma 2, the set of functions of type (12) generates the subset of $\mathfrak{E}_n$ consisting of all 1-place functions other than permutations. By the criterion mentioned in section 1, we may conclude that $\mathfrak{F}$ is complete.

Lemma 5. *Assume that* $n \geqq 3$ *and* $\mathfrak{F} \subset \mathfrak{E}_n$ *contains a triply transitive group* $\mathfrak{G}$ *(of degree* n*), a function* $f(x_1, \dots, x_k)$ *satisfying Slupecki conditions and a function* $g(x)$ *of type* $[n - a, a]$ *where* $a \neq \dfrac{n}{2}$. *Then* $\mathfrak{F}$ *is complete.*

Proof. If $n = 3$ or $n = 4$ the assumptions of lemmas 4 and 5 are equivalent. Therefore, we assume that $n \geqq 5$. We shall show that $\mathfrak{F}$ generates a function of type $[n - 1, 1]$. This implies, by lemma 4, that $\mathfrak{F}$ is complete.

By the hypothesis, $n - a \neq a$. We assume that the notation is chosen in such a way that $n - a > a$. If $a = 1$ the proof is completed. We, therefore, assume that $a \geqq 2$. We shall show that $\mathfrak{F}$ generates a function $g_1(x)$ of type $[n - a_1, a_1]$ where $1 \leqq a_1 < a$. By repeating the argument, we conclude that $\mathfrak{F}$ generates a function of type $[n - 1, 1]$.

Let E_1 and E_2 be disjoint subsets of N such that $\mathrm{card}(E_1) = n - a$, $\mathrm{card}(E_2) = a \geqq 2$ and $g(x)$ assumes a constant value both in E_1 and in E_2. Because $\mathfrak{F}$ contains a doubly transitive group it generates every function assuming a constant value both in E_1 and in E_2.

We choose from $\mathfrak{G}$ a permutation $p(x)$ mapping some element of E_2 into itself and some other element of E_2 into E_1. Consider the sets

$$\begin{aligned} V_1 &= E_1 \cap p(E_1)\,, \quad V_2 = E_2 \cap p(E_1)\,, \\ V_3 &= E_2 \cap p(E_2)\,, \quad V_4 = E_1 \cap p(E_2)\,. \end{aligned} \tag{13}$$

The union of the sets (13) equals N. On the other hand, by the choice of the permutation p,

$$1 \leqq \mathrm{card}\,(V_i) < \mathrm{card}\,(E_2) = a\,, \quad \text{for} \quad i = 2\,, 3\,, 4\,. \tag{14}$$

Furthermore, $1 \leqq \mathrm{card}\,(V_1)$. The sets (13) are not of the same cardinality. For if $\mathrm{card}\,(V_1) = \mathrm{card}\,(V_2)$ and $\mathrm{card}\,(V_3) = \mathrm{card}\,(V_4)$ we obtain

$$\mathrm{card}\,(V_1) = \tfrac{1}{2}\,\mathrm{card}\,(E_1) > \tfrac{1}{2}\,\mathrm{card}\,(E_2) = \mathrm{card}\,(V_3)\,.$$

Let b_i and b_i', $i = 1\,, \ldots\,, k$, be the same numbers as in the proof of lemma 3. Thus, equations (3) — (5) hold, for some distinct numbers b, b' and b''. Choose arbitrary elements $v_i \in V_i$, $i = 1, 2, 3$, and a permutation $p'(x) \in \mathfrak{G}$ such that $p'(b) = v_1$, $p'(b') = v_2$ and $p'(b'') = v_3$.

The following auxiliary functions $h_i(x)$ are generated by $\mathfrak{F}$:

$$h_i(E_1) = \{b_i\}\,, \; h_i(E_2) = \{b_i'\}\,, \quad i = 1\,, \ldots\,, k\,.$$

(Some of the functions $h_i(x)$ may be constants which are generated by $\mathfrak{F}$, according to lemma 3.) Let

$$\bar{g}(x) = p'(f(h_1(x)\,, h_2 p^{-1}(x)\,, \ldots\,, h_k p^{-1}(x)))\,.$$

It follows from the definitions of the functions involved that

$$\bar{g}(x) = v_i\,, \quad \text{for} \quad x \in V_i\,, \quad i = 1\,, 2\,, 3\,. \tag{15}$$

Furthermore, $\bar{g}(x)$ assumes a constant value v', for $x \in V_4$.

Suppose $v' \notin V_4$. Then $\bar{g}^2(x)$ is a function of genus 3 and type $[t_1, t_2, t_3]$ where at least one of the numbers t, say t_3, satisfies $1 \leqq t_3 < a$. This is due to (14) and the fact that $v' \in V_1 \cup V_2 \cup V_3$. Let the values assumed by $\bar{g}^2(x)$ be u_1, u_2 and u_3 where u_1 is assumed at least twice and u_3 exactly t_3 times. Choose numbers u_1^1, u_1^2 and u_3^1 such that $\bar{g}^2(u_1^1) = \bar{g}^2(u_1^2) = u_1$ and $\bar{g}^2(u_3^1) = u_3$. Furthermore, choose a permutation $p_1(x) \in \mathfrak{G}$ mapping the ordered triple (u_1, u_2, u_3) into the ordered triple (u_1^1, u_1^2, u_3^1). Then we may choose

$$g_1(x) = \bar{g}^2 p_1 \bar{g}^2(x)\,.$$

Clearly $g_1(x)$ is of type $[n - t_3, t_3]$ where $1 \leqq t_3 < a$.

Thus, we may assume that $v' = v_4 \in V_4$. The equations (15) may be written in the form

$$\bar{g}(x) = v_i\,, \quad \text{for} \quad x \in V_i\,, \quad i = 1\,,2\,,3\,,4\,. \tag{16}$$

We say that a quadruple $(\zeta_1, \zeta_2, \zeta_3, \zeta_4)$ is a *permissible set of representatives* for the numbers v_i if there is a permutation in $\mathfrak{G}$ mapping v_i into ζ_i, $i = 1, 2, 3, 4$. Assume that the elements of some permissible set of representatives are contained in exactly three sets V_i and let $p_\zeta(x)$ be the corresponding permutation. Then the function $\bar{g}p_\zeta\bar{g}(x)$ is of type $[t_1, t_2, t_3]$ where $1 \leqq t_3 < a$. Proceeding as above, we obtain a function $g_1(x)$ as required. We may, therefore, assume that there is no permissible set of representatives whose elements are contained in exactly three sets V_i.

We shall now make use of the fact established above that the sets (13) are not of the same cardinality. If $\alpha(i)$ is a permutation of the numbers 1, 2, 3, 4 such that

$$\text{card}\,(V_{\alpha(1)}) \geqq \text{card}\,(V_{\alpha(2)}) \geqq \text{card}\,(V_{\alpha(3)}) \geqq \text{card}\,(V_{\alpha(4)})$$

then necessarily

$$\text{card}\,(V_{\alpha(1)}) > \text{card}\,(V_{\alpha(4)})\,. \tag{17}$$

Furthermore, by (14),

$$1 \leqq \text{card}\,(V_{\alpha(i)}) < \text{card}\,(E_2) = a\,, \quad \text{for} \quad i = 2\,,3\,,4\,. \tag{18}$$

Let $V_{\alpha(1)} = \{v^1_{\alpha(1)}\,, \ldots, v^\beta_{\alpha(1)}\}$. Consider the numbers v_i in the equations (16). Choose from $\mathfrak{G}$ β permutations $q_i(x)$, $i = 1\,, \ldots, \beta$, such that

$$q_i(v_{\alpha(1)}) = v_{\alpha(2)}\,, q_i(v_{\alpha(2)}) = v^i_{\alpha(1)}\,, \quad q_i(v_{\alpha(3)}) = v_{\alpha(3)}\,.$$

Then, for all $i, q_i(v_{\alpha(4)}) \in V_{\alpha(4)}$ because, otherwise, we would obtain a permissible set of representatives whose elements are contained in exactly three sets V_i.

By (17), this implies that, for some μ and $\nu, \mu \neq \nu$,

$$q_\mu(v_{\alpha(4)}) = q_\nu(v_{\alpha(4)}) = v^*_{\alpha(4)} \in V_{\alpha(4)}\,.$$

We have, thus, constructed the following two permissible sets of representatives which differ by one element only

$$(v_{\alpha(2)}\,, v^\mu_{\alpha(1)}\,, v_{\alpha(3)}\,, v^*_{\alpha(4)})\,; (v_{\alpha(2)}\,, v^\nu_{\alpha(1)}\,, v_{\alpha(3)}\,, v^*_{\alpha(4)})\,. \tag{19}$$

We now choose from $\mathfrak{G}$ a permutation $q'(x)$ such that

$$q'(v^\mu_{\alpha(1)}) = v_{\alpha(2)}\,, q'(v^\nu_{\alpha(1)}) = v_{\alpha(3)}\,, q'(v_{\alpha(3)}) = v_{\alpha(1)}\,.$$

Consider the values

$$q'(v_{\alpha(2)}) \quad \text{and} \quad q'(v^*_{\alpha(4)})\,. \tag{20}$$

Because the sets (19) are permissible and q' obviously maps a permissible set into a permissible set, the values (20) are both contained in the set $V_{\alpha(1)}$. Otherwise, we would obtain a permissible set of representatives whose elements are contained in exactly three sets V_i.

We may now choose

$$g_1(x) = \bar{g}q'q_\mu\bar{g}(x) .$$

The function $g_1(x)$ assumes the value $v_{\alpha(2)}$, for $x \in V_{\alpha(2)}$, and the value $v_{\alpha(1)}$, otherwise. By (18), it is of type $[n - a_1, a_1]$ where $1 \leqq a_1 < a$. This completes the proof of lemma 5.

Proof of the theorem. We assume first that $n \geqq 5, n \neq 2^r$ and $\mathfrak{G}$ is a triply transitive group of degree n. Let $f(x_1, \ldots, x_k)$ be an arbitrary function satisfying Słupecki conditions. To show that $\mathfrak{G}$ is basic for $\mathfrak{E}_n$, we prove that the set $\mathfrak{F}$ consisting of $\mathfrak{G}$ and f is complete.

By lemma 3, $\mathfrak{F}$ generates a function $g(x)$ of genus 2. This implies, by lemma 5, that $\mathfrak{F}$ is complete, provided $g(x)$ is not of type

$$(21) \qquad [\tfrac{1}{2}n , \tfrac{1}{2}n] .$$

We assume that $g(x)$ is of type (21) and that E_1 and E_2 are disjoint subsets of N such that $\text{card}\,(E_1) = \text{card}\,(E_2) = \frac{1}{2}n$ and $g(x)$ assumes a constant value both in E_1 and in E_2. We shall now proceed as in the proof of lemma 5.

We form the sets V_i, $i = 1, 2, 3, 4,$ and obtain a function $\bar{g}(x)$ satisfying the equations (16). (Otherwise, we would obtain a function of genus 2 and not of type (21) which would complete the proof.) Furthermore, we may assume that the sets V_i are of the same cardinality because, otherwise, we could use the inequality (17) as in the proof of lemma 5. Thus, the set N is divided into subsets as follows:

N			
E_1		E_2	
V_1	V_4	V_2	V_3

We now form a new partition of N into V-sets by choosing from $\mathfrak{G}$ a permutation $\bar{p}(x)$ which maps some element of V_1 into itself and some other element of V_1 into V_3 and denoting

$$V_1^1 = E_1 \cap \bar{p}(E_1) , V_2^1 = E_2 \cap \bar{p}(E_1) , V_3^1 = E_2 \cap \bar{p}(E_2) , V_4^1 = E_1 \cap \bar{p}(E_2) .$$

Again, we may conclude that the sets V_i^1 are of the same cardinality. Furthermore, we may assume that the following equations hold:

$$
\begin{aligned}
(22)\quad \operatorname{card}(V_1 \cap V_1^1) &= \operatorname{card}(V_1 \cap V_4^1) = \operatorname{card}(V_4 \cap V_1^1) = \operatorname{card}(V_4 \cap V_4^1) \\
&= \operatorname{card}(V_2 \cap V_2^1) = \operatorname{card}(V_2 \cap V_3^1) = \operatorname{card}(V_3 \cap V_2^1) \\
&= \operatorname{card}(V_3 \cap V_3^1) = \tfrac{1}{2} \operatorname{card}(V_1) = \tfrac{1}{4} \operatorname{card}(E_1) \\
&= \tfrac{1}{8} \operatorname{card}(N) = \tfrac{1}{8}\, n\,.
\end{aligned}
$$

For if the equations (22) do not hold we may argue as follows. Assume that, for instance,

$$(23)\qquad \operatorname{card}(V_1 \cap V_1^1) > \operatorname{card}(V_1 \cap V_4^1)\,.$$

Let $V_1 \cap V_1^1 = \{\bar{v}_1, \ldots, \bar{v}_\gamma\}$. We choose from $\mathfrak{G}$ permutations $\pi_i(x)$, $i = 1, \ldots, \gamma$, such that $\pi_i(v_1) = \bar{v}_i$, $\pi_i(v_2)$ equals some fixed element in $V_4 \cap V_1^1$ and $\pi_i(v_3)$ equals some fixed element in $V_4 \cap V_4^1$. If, for some i, $\pi_i(v_4) \notin V_1 \cap V_4^1$ we obtain a function of genus 2 and not of type (21). If, for all i, $\pi_i(v_4) \in V_1 \cap V_4^1$ we obtain, by (23), two permissible sets of representatives differing by one element only. Then we may argue as in the proof of lemma 5.

Equations (22) express the fact that N is divided into subsets as follows:

(24)

N							
E_1				E_2			
V_1		V_4		V_2		V_3	
V_1^1	V_4^1	V_1^1	V_4^1	V_2^1	V_3^1	V_2^1	V_3^1

We continue the process by forming a new partition of N into sets V_i^2, $i = 1, 2, 3, 4$. If we do not obtain a function of genus 2 and of some type other than (21) we obtain equations corresponding to (22). The common cardinality of the sets involved equals $\dfrac{1}{16}\, n$.

By repeating the argument for new partitions of N, we conclude that we either obtain a function of genus 2 and not of type (21) or $n = 2^r$. Thus, the part of our theorem concerning triply transitive groups follows.

Assume that $n \geqq 5$ and $\mathfrak{G}$ is a quadruply transitive group of degree n. Let $\mathfrak{F}$ be as above. The completeness of $\mathfrak{F}$ follows because we may choose from $\mathfrak{G}$ a permutation mapping the numbers v_i, $i = 1, 2, 3, 4$, into exactly three of the sets V_i. We, thus, obtain a permissible set of representatives whose elements are contained in exactly three sets V_i.

Therefore, we have established our theorem. We note, finally, that the main difficulties in the proof are due to the fact that no analogues of lemma 1.2 in [3] are available.

3. *Special cases.* We shall now show that the condition $n \neq 2^r$ in the statement of our theorem is essential. If $n = 2^r$ $(r \geqq 2)$ there is a triply transitive group of degree n which is not a basic group for $\mathfrak{C}_n$. In what follows, we shall discuss the case $n = 8$ in detail.

Let $\mathfrak{G}_8$ be the holomorph of an Abelian group of order 8 and type (1, 1, 1), expressed in the usual way as a permutation group of degree 8. $\mathfrak{G}_8$ is generated by the two permutations (1376528) and (17)(46). It is of order 1344 and consists of 384 7-cycles, 224 permutations of cyclic structure 3×3, 224 permutations of cyclic structure 6×2, 252 permutations of cyclic structure 4×4, 49 permutations of cyclic structure $2 \times 2 \times 2 \times 2$, 42 permutations of cyclic structure 2×2, 168 permutations of cyclic structure 4×2 and the identity. The group $\mathfrak{G}_8$ can also be characterized by the following six defining relations:

$$X^7 = 1\,,\ Y^2 = 1\,,\ (YX^3)^4 = 1\,,\ (YX)^6 = 1\,,$$

$$(YX^3YX^2YX)^2 = 1\,,\ YX^3(YX)^2YX^4YX^5YX^6YX^5 = 1\,.$$

Obviously, the holomorph of an Abelian group of order 2^r and type $(1, 1, \ldots, 1)$ (i.e. the holomorph of a so-called *generalized Klein group*) is triply transitive. In particular, $\mathfrak{G}_8$ is triply transitive.

However, $\mathfrak{G}_8$ is not a basic group for $\mathfrak{C}_8$. Consider the following function $f(x, y)$ which satisfies Słupecki conditions:

$$f(2x-1\,, y) = y\ , f(2x\,, y) = 9 - y\,.$$

Then the set $\mathfrak{F}$ consisting of $\mathfrak{G}_8$ and $f(x, y)$ is not complete.

To prove this, we quote some terminology and notations, from section 2. We let $E_1 = \{1, 2, 3, 4\}$, $E_2 = \{5, 6, 7, 8\}$, $V_1 = \{1, 2\}$, $V_4 = \{3, 4\}$, $V_2 = \{5, 6\}$ and $V_3 = \{7, 8\}$. The following (unordered) quadruples are called permissible sets of representatives:

1234, 1256, 1278, 1357, 1368, 1458, 1467,
2358, 2367, 2457, 2468, 3456, 3478, 5678.

The permutations in $\mathfrak{G}_8$ always map a permissible set of representatives into a permissible set. Furthermore, they preserve the subset structure (24) of N.

Let $\mathfrak{F}_8 \subset \mathfrak{C}_8$ be the set consisting of the following 1-place functions:

1) Permutations in $\mathfrak{G}_8$.

2) Constants.

3) Those functions of type [2, 2, 2, 2] whose values form a permissible set of representatives and which, furthermore, assume a constant value in the sets V_1^i, V_2^i, V_3^i and V_4^i, for some $i = 1\,, \ldots, 7$, where

$$\begin{aligned}
&V_1^1 = \{1\,,2\}\,,\ V_2^1 = \{3\,,4\}\,,\ V_3^1 = \{5\,,6\}\,,\ V_4^1 = \{7\,,8\}\,;\\
&V_1^2 = \{1\,,3\}\,,\ V_2^2 = \{2\,,4\}\,,\ V_3^2 = \{5\,,7\}\,,\ V_4^2 = \{6\,,8\}\,;\\
&V_1^3 = \{1\,,4\}\,,\ V_2^3 = \{2\,,3\}\,,\ V_3^3 = \{5\,,8\}\,,\ V_4^3 = \{6\,,7\}\,;\\
&V_1^4 = \{1\,,5\}\,,\ V_2^4 = \{2\,,6\}\,,\ V_3^4 = \{3\,,7\}\,,\ V_4^4 = \{4\,,8\}\,;\\
&V_1^5 = \{1\,,6\}\,,\ V_2^5 = \{4\,,7\}\,,\ V_3^5 = \{2\,,5\}\,,\ V_4^5 = \{3\,,8\}\,;\\
&V_1^6 = \{1\,,7\}\,,\ V_2^6 = \{3\,,5\}\,,\ V_3^6 = \{2\,,8\}\,,\ V_4^6 = \{4\,,6\}\,;\\
&V_1^7 = \{1\,,8\}\,,\ V_2^7 = \{4\,,5\}\,,\ V_3^7 = \{2\,,7\}\,,\ V_4^7 = \{3\,,6\}\,.
\end{aligned}$$

4) Those functions of type [4, 4] which, for some i, assume a constant value in one of the sets $V_1^i \cup V_2^i$, $V_1^i \cup V_3^i$ or $V_1^i \cup V_4^i$.

The set $\mathfrak{F}_8$ is closed under composition. In classes 1)—4) there are, respectively, 1344, 8, 2352 and 392 functions. Thus, card $(\mathfrak{F}_8) = 4096$. This number can be computed more directly as follows. $\mathfrak{F}_8$ consists of all functions which map every permissible set of representatives into a permissible set, a quadruple of type [2, 2] or of type [4]. (In what follows, quadruples of these three forms are called *permissible images*.) Thus, we may choose arbitrarily the values $h(1), h(2), h(3)$ of a function $h(x) \in \mathfrak{F}_8$. They determine uniquely the value $h(4)$. Again, $h(5)$ may be chosen arbitrarily but then the values $h(6), h(7), h(8)$ are uniquely determined. Hence,

$$\text{card}\ (\mathfrak{F}_8) = 8^4 = 4096\,.$$

Our function $f(x, y)$ forms a closure in the set $\mathfrak{F}_8$, i.e. if $g_1(x), g_2(x) \in \mathfrak{F}_8$ then also $f(g_1(x), g_2(x)) \in \mathfrak{F}_8$. To prove this, it suffices to show that if (i_1, i_2, i_3, i_4) and (j_1, j_2, j_3, j_4) are two permissible images then also

$$(f(i_1\,, j_1)\,, f(i_2\,, j_2)\,, f(i_3\,, j_3)\,, f(i_4\,, j_4))$$

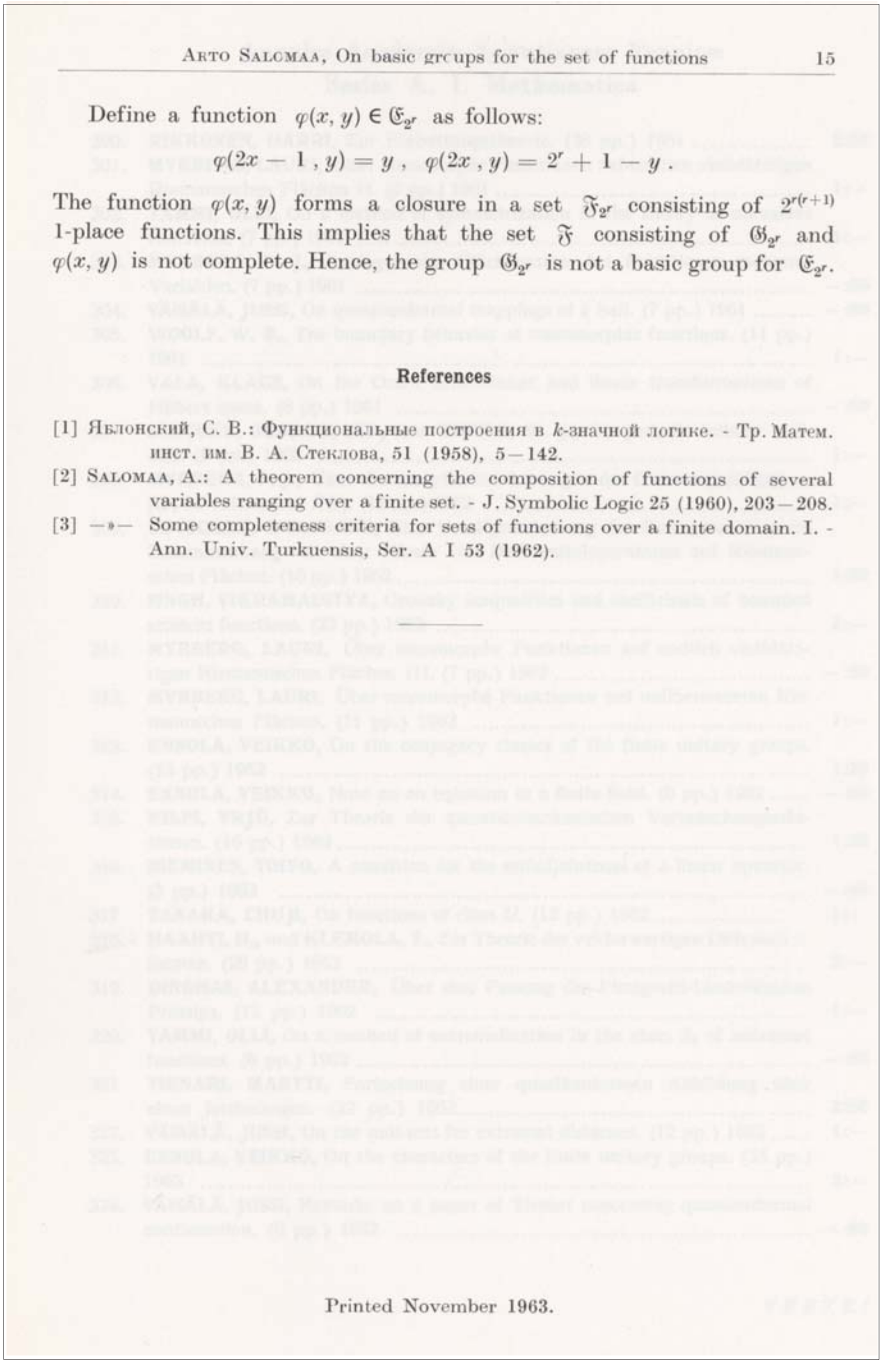
is a permissible image. This can be readily verified by considering the matrix of $f(x, y)$.

Thus, $\mathfrak{F}$ generates no 1-place functions other than the functions in $\mathfrak{F}_8$. This proves that $\mathfrak{F}$ is not complete. Clearly, instead of the function $f(x, y)$, we may choose any function which satisfies Słupecki conditions and forms a closure in the set $\mathfrak{F}_8$.

Consider the general case[1]) $n = 2^r, r \geqq 3$. Let $\mathfrak{G}_{2^r}$ be the holomorph of an Abelian group of order 2^r and type $(1, 1, \ldots, 1)$. The order of this triply transitive group $\mathfrak{G}_{2^r}$ equals

$$2^r(2^r - 1)(2^r - 2)(2^r - 2^2) \cdots (2^r - 2^{r-1})\,.$$

[1]) We have regarded the case $n = 8$ as the first exceptional case. In fact, also the case $n = 4$ may be considered as exceptional, the exceptional group being the holomorph of the four-group (which equals the symmetric group of degree 4). Our theorem is not valid for $n = 3$ because lemma 3 is not valid in this case.



Define a function $\varphi(x, y) \in \mathfrak{E}_{2^r}$ as follows:

$$\varphi(2x-1\,,y) = y\;,\;\; \varphi(2x\,,y) = 2^r + 1 - y\;.$$

The function $\varphi(x, y)$ forms a closure in a set $\mathfrak{F}_{2^r}$ consisting of $2^{r(r+1)}$ 1-place functions. This implies that the set $\mathfrak{F}$ consisting of $\mathfrak{G}_{2^r}$ and $\varphi(x, y)$ is not complete. Hence, the group $\mathfrak{G}_{2^r}$ is not a basic group for $\mathfrak{E}_{2^r}$.

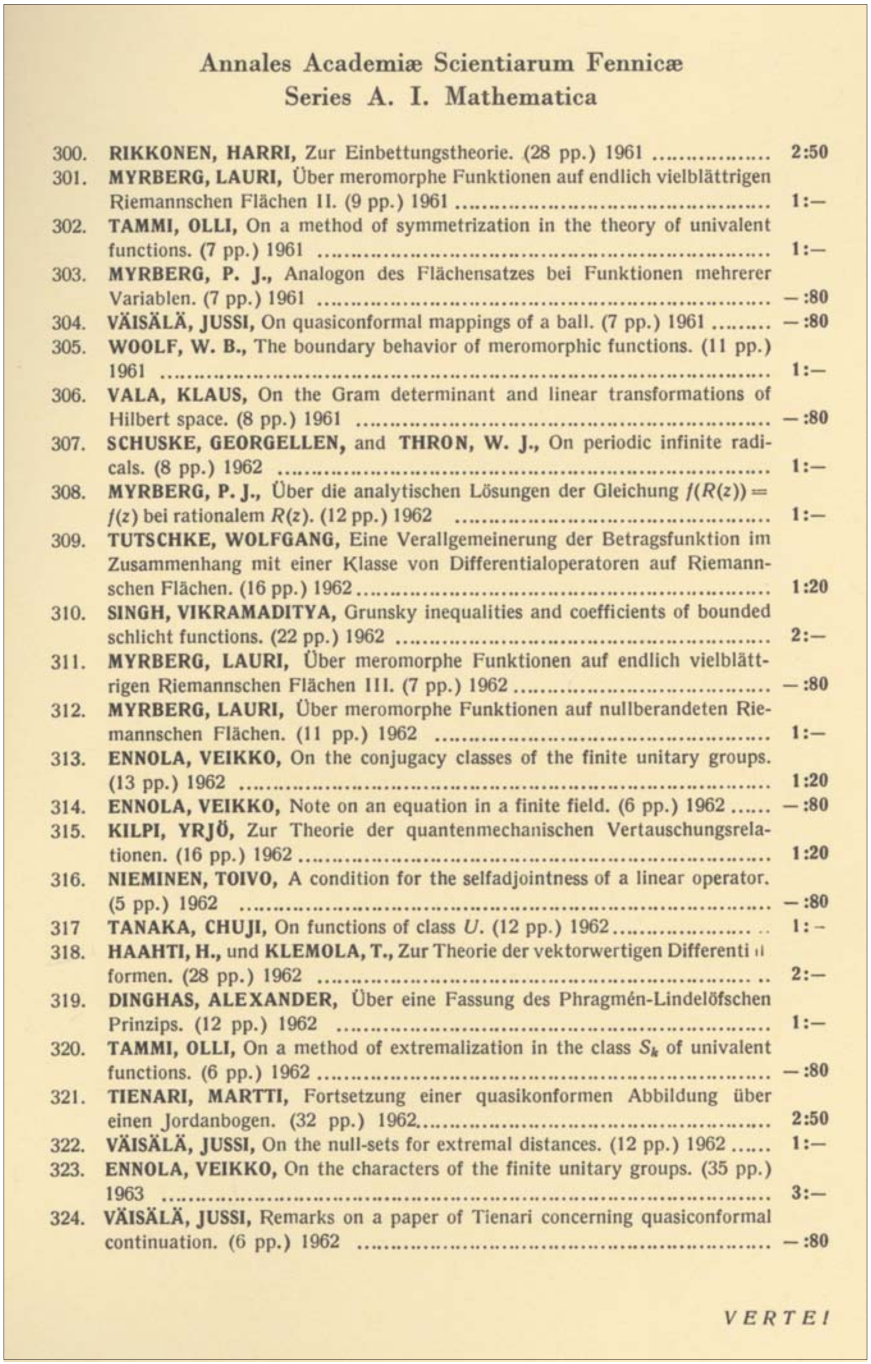
References

[1] Яблонский, С. В.: Функциональные построения в k-значной логике. - Тр. Матем. инст. им. В. А. Стеклова, 51 (1958), 5–142.

[2] Salomaa, A.: A theorem concerning the composition of functions of several variables ranging over a finite set. - J. Symbolic Logic 25 (1960), 203–208.

[3] —»— Some completeness criteria for sets of functions over a finite domain. I. - Ann. Univ. Turkuensis, Ser. A I 53 (1962).

Printed November 1963.



Annales Academiæ Scientiarum Fennicæ
Series A. I. Mathematica

300. **RIKKONEN, HARRI,** Zur Einbettungstheorie. (28 pp.) 1961 .... 2:50

301. **MYRBERG, LAURI,** Über meromorphe Funktionen auf endlich vielblättrigen Riemannschen Flächen II. (9 pp.) 1961 .... 1:—

302. **TAMMI, OLLI,** On a method of symmetrization in the theory of univalent functions. (7 pp.) 1961 .... 1:—

303. **MYRBERG, P. J.,** Analogon des Flächensatzes bei Funktionen mehrerer Variablen. (7 pp.) 1961 .... —:80

304. **VÄISÄLÄ, JUSSI,** On quasiconformal mappings of a ball. (7 pp.) 1961 .... —:80

305. **WOOLF, W. B.,** The boundary behavior of meromorphic functions. (11 pp.) 1961 .... 1:—

306. **VALA, KLAUS,** On the Gram determinant and linear transformations of Hilbert space. (8 pp.) 1961 .... —:80

307. **SCHUSKE, GEORGELLEN,** and **THRON, W. J.,** On periodic infinite radicals. (8 pp.) 1962 .... 1:—

308. **MYRBERG, P. J.,** Über die analytischen Lösungen der Gleichung $f(R(z)) = f(z)$ bei rationalem $R(z)$. (12 pp.) 1962 .... 1:—

309. **TUTSCHKE, WOLFGANG,** Eine Verallgemeinerung der Betragsfunktion im Zusammenhang mit einer Klasse von Differentialoperatoren auf Riemannschen Flächen. (16 pp.) 1962 .... 1:20

310. **SINGH, VIKRAMADITYA,** Grunsky inequalities and coefficients of bounded schlicht functions. (22 pp.) 1962 .... 2:—

311. **MYRBERG, LAURI,** Über meromorphe Funktionen auf endlich vielblättrigen Riemannschen Flächen III. (7 pp.) 1962 .... —:80

312. **MYRBERG, LAURI,** Über meromorphe Funktionen auf nullberandeten Riemannschen Flächen. (11 pp.) 1962 .... 1:—

313. **ENNOLA, VEIKKO,** On the conjugacy classes of the finite unitary groups. (13 pp.) 1962 .... 1:20

314. **ENNOLA, VEIKKO,** Note on an equation in a finite field. (6 pp.) 1962 .... —:80

315. **KILPI, YRJÖ,** Zur Theorie der quantenmechanischen Vertauschungsrelationen. (16 pp.) 1962 .... 1:20

316. **NIEMINEN, TOIVO,** A condition for the selfadjointness of a linear operator. (5 pp.) 1962 .... —:80

317 **TANAKA, CHUJI,** On functions of class U. (12 pp.) 1962 .... 1:–

318. **HAAHTI, H.,** und **KLEMOLA, T.,** Zur Theorie der vektorwertigen Differentialformen. (28 pp.) 1962 .... 2:—

319. **DINGHAS, ALEXANDER,** Über eine Fassung des Phragmén-Lindelöfschen Prinzips. (12 pp.) 1962 .... 1:—

320. **TAMMI, OLLI,** On a method of extremalization in the class S_k of univalent functions. (6 pp.) 1962 .... —:80

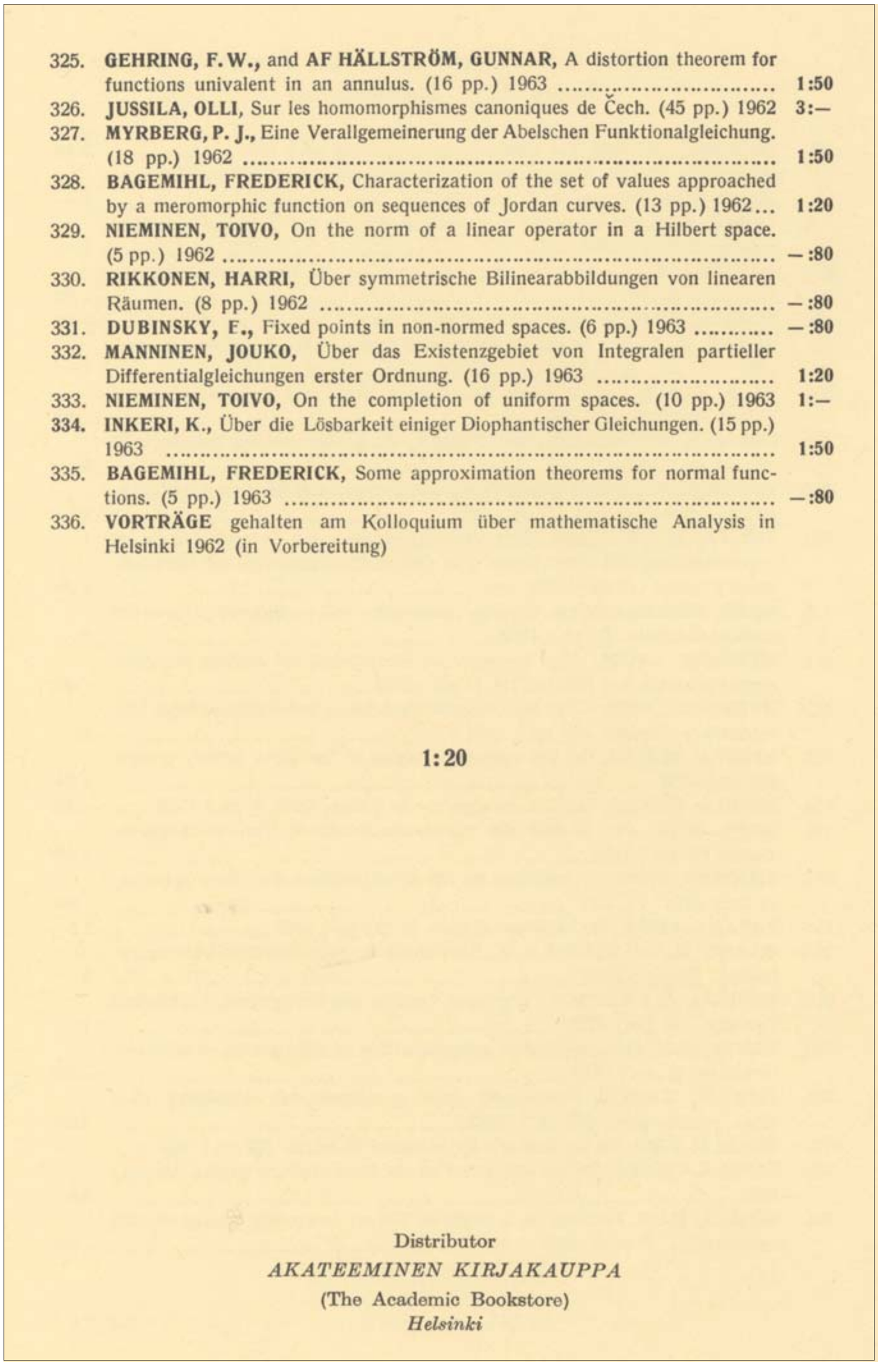
321. **TIENARI, MARTTI,** Fortsetzung einer quasikonformen Abbildung über einen Jordanbogen. (32 pp.) 1962 .... 2:50

322. **VÄISÄLÄ, JUSSI,** On the null-sets for extremal distances. (12 pp.) 1962 .... 1:—

323. **ENNOLA, VEIKKO,** On the characters of the finite unitary groups. (35 pp.) 1963 .... 3:—

324. **VÄISÄLÄ, JUSSI,** Remarks on a paper of Tienari concerning quasiconformal continuation. (6 pp.) 1962 .... —:80

VERTE!



325. **GEHRING, F. W., and AF HÄLLSTRÖM, GUNNAR,** A distortion theorem for functions univalent in an annulus. (16 pp.) 1963 .... 1:50

326. **JUSSILA, OLLI,** Sur les homomorphismes canoniques de Čech. (45 pp.) 1962 3:—

327. **MYRBERG, P. J.,** Eine Verallgemeinerung der Abelschen Funktionalgleichung. (18 pp.) 1962 .... 1:50

328. **BAGEMIHL, FREDERICK,** Characterization of the set of values approached by a meromorphic function on sequences of Jordan curves. (13 pp.) 1962... 1:20

329. **NIEMINEN, TOIVO,** On the norm of a linear operator in a Hilbert space. (5 pp.) 1962 .... —:80

330. **RIKKONEN, HARRI,** Über symmetrische Bilinearabbildungen von linearen Räumen. (8 pp.) 1962 .... —:80

331. **DUBINSKY, E.,** Fixed points in non-normed spaces. (6 pp.) 1963 .... —:80

332. **MANNINEN, JOUKO,** Über das Existenzgebiet von Integralen partieller Differentialgleichungen erster Ordnung. (16 pp.) 1963 .... 1:20

333. **NIEMINEN, TOIVO,** On the completion of uniform spaces. (10 pp.) 1963 1:—

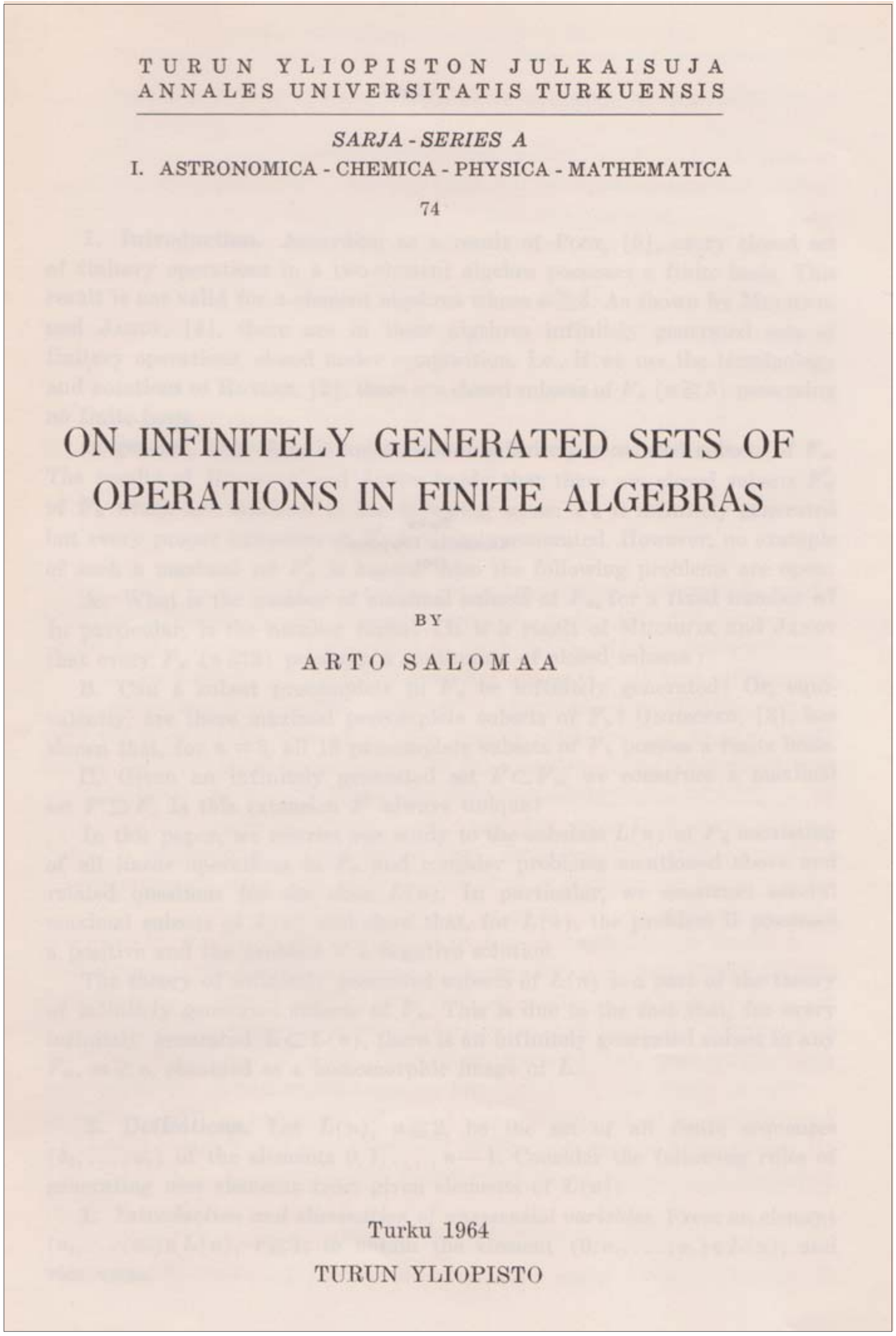
334. **INKERI, K.,** Über die Lösbarkeit einiger Diophantischer Gleichungen. (15 pp.) 1963 .... 1:50

335. **BAGEMIHL, FREDERICK,** Some approximation theorems for normal functions. (5 pp.) 1963 .... —:80

336. **VORTRÄGE** gehalten am Kolloquium über mathematische Analysis in Helsinki 1962 (in Vorbereitung)

1:20

Distributor
AKATEEMINEN KIRJAKAUPPA
(The Academic Bookstore)
Helsinki



TURUN YLIOPISTON JULKAISUJA
ANNALES UNIVERSITATIS TURKUENSIS

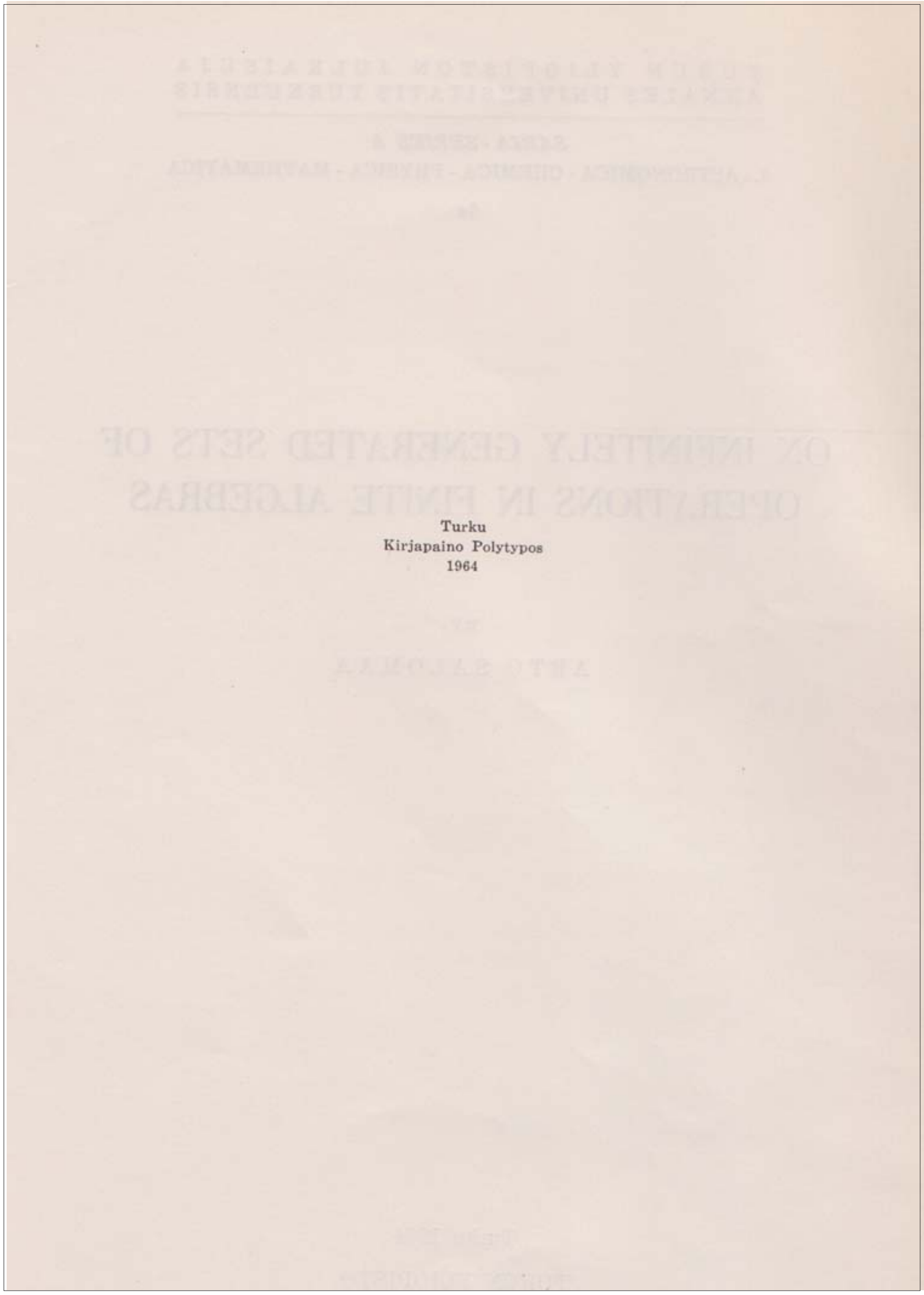
SARJA - SERIES A
I. ASTRONOMICA - CHEMICA - PHYSICA - MATHEMATICA
74

ON INFINITELY GENERATED SETS OF OPERATIONS IN FINITE ALGEBRAS

BY

ARTO SALOMAA

Turku 1964
TURUN YLIOPISTO



Turku
Kirjapaino Polytypos
1964

1. Introduction.

According to a result of Post, [5], every closed set of finitary operations in a two-element algebra possesses a finite basis. This result is not valid for n-element algebras where $n \geqq 3$. As shown by Muchnik and Janov, [4], there are in these algebras infinitely generated sets of finitary operations, closed under composition. I.e., if we use the terminology and notations of Butler, [2], there are closed subsets of F_n $(n \geqq 3)$ possessing no finite basis.

In general, very little is known about infinitely generated subsets of F_n. The results of Muchnik and Janov imply that there are closed subsets F'_n of F_n which are *maximal* in the following sense: F'_n is infinitely generated but every proper extension of F'_n is finitely generated. However, no example of such a maximal set F'_n is known. Also the following problems are open:

A. What is the number of maximal subsets of F_n, for a fixed number n? In particular, is the number finite? (It is a result of Muchnik and Janov that every F_n $(n \geqq 3)$ possesses a continuum of closed subsets.)

B. Can a subset precomplete in F_n be infinitely generated? Or, equivalently, are there maximal precomplete subsets of F_n? Gnidenko, [3], has shown that, for $n = 3$, all 18 precomplete subsets of F_n possess a finite basis.

C. Given an infinitely generated set $F \subset F_n$, we construct a maximal set $F' \supset F$. Is this extension F' always unique?

In this paper, we restrict our study to the subclass $L(n)$ of F_n consisting of all *linear* operations in F_n and consider problems mentioned above and related questions for the class $L(n)$. In particular, we construct several maximal subsets of $L(n)$ and show that, for $L(n)$, the problem B possesses a positive and the problem C a negative solution.

The theory of infinitely generated subsets of $L(n)$ is a part of the theory of infinitely generated subsets of F_n. This is due to the fact that, for every infinitely generated $L \subset L(n)$, there is an infinitely generated subset in any F_m, $m \geqq n$, obtained as a homomorphic image of L.

2. Definitions.

Let $L(n)$, $n \geqq 2$, be the set of all finite sequences $(a_1, \dots, a_r)$ of the elements $0, 1, \dots, n-1$. Consider the following rules of generating new elements from given elements of $L(n)$:

1. *Introduction and elimination of unessential variables.* From an element $(a_1, \dots, a_r) \in L(n)$, $r \geqq 1$, to obtain the element $(0, a_1, \dots, a_r) \in L(n)$, and vice versa.

2. *Renaming of variables.* From an element

$$(a_1, \dots, a_r, a_{r+1}) \in L(n)$$

and a permutation $P(x)$ of the index set $\{1, \dots, r\}$ to obtain the element $(a_{P(1)}, \dots, a_{P(r)}, a_{r+1}) \in L(n)$.

3. *Identification of variables.* From an element

$$(a_1, a_2, \dots, a_r, a_{r+1}) \in L(n),\ r \geqq 2,$$

to obtain the element $(a_1 + a_2, \dots, a_r, a_{r+1}) \in L(n)$ where addition is carried out modulo n.

4. *Composition.* From two elements

$$(a_1, a_2, \dots, a_r, a_{r+1}),\ (b_1, \dots, b_s, b_{s+1}) \in L(n),\ r, s \geqq 1,$$

to obtain the element

$$(a_1 b_1, \dots, a_1 b_s, a_2, \dots, a_r, a_1 b_{s+1} + a_{r+1}) \in L(n)$$

where addition and multiplication are carried out modulo n.

Remark. Cf. [6] where different methods of compounding finitary operations are considered. If $L(n)$ is interpreted as the set of all linear polynomials modulo n then the rules 1—4 include all of these methods.

A set $L \subset L(n)$ is said to be *closed* if it is closed under the rules 1—4. For $L \subset L(n)$, we define the *closure* of L, in symbols, $\mathrm{Cl}(L)$ to be the least closed extension of L. (Clearly, Cl is a closure operation in the sense of [1, p. 49].) A set $L \subset L(n)$ *generates* a set L' if $L' \subset \mathrm{Cl}(L)$. Obviously, the set consisting of $(1, 1, 0)$ and $(1, 1)$ generates the whole set $L(n)$.

If a set $L \subset L(n)$ generates $L(n)$ we say that L is *complete*. A closed set is termed *precomplete* if it is not complete but every proper extension of it is complete.

A closed set $L \subset L(n)$ is said to be *finitely generated* (or to possess a *finite basis*) if there is a finite set $L_1 \subset L$ which generates L, i.e. $L = \mathrm{Cl}(L_1)$, for some finite $L_1 \subset L$. Otherwise, L is said to be *infinitely generated*. If L is infinitely generated but every closed proper extension of L is finitely generated we say that L is *maximal*.

For a closed set $L \subset L(n)$ and a natural number k, we define the *k-restriction* of L, in symbols, $\mathrm{Re}_k(L)$ to be the subset of L consisting of all sequences of at most k elements. The *order* of a closed subset L of $L(n)$ is defined to be the smallest integer k such that

$$\mathrm{Cl}(\mathrm{Re}_{k+1}(L)) = L.$$

If no such integer k exists, L is said to be of infinite order. (The notion of order is due to GNIDENKO, [3].) Clearly, L is infinitely generated if and only if it is of infinite order.

Let L be infinitely generated. For any natural number k, there is an element $\varphi \in L - \mathrm{Cl}(\mathrm{Re}_k(L))$. On the other hand, for any $\varphi \in L$, there is a natural number l such that $\varphi \in \mathrm{Re}_l(L)$. Hence, we have the following

THEOREM 1. *Every infinitely generated set contains an infinity of closed subsets.*

For $n = \Pi_{i=1}^{m} p_i^{\alpha_i}$, an element $\varphi = (a_1, \dots, a_r) \in L(n)$ and a fixed i, $1 \leqq i \leqq m$, we define $H_i(\varphi) = (a'_1, \dots, a'_r) \in L(p_i^{\alpha_i})$ where a'_j denotes the least non-negative remainder of a_j (mod $p_i^{\alpha_i}$). $H_i(\varphi)$ is termed the *representative* of φ in the set $L(p_i^{\alpha_i})$. Clearly, an element $\varphi \in L(n)$ is uniquely determined if all of its representatives are known. The representative $H_i(L)$ of a set $L \subset L(n)$ is understood to consist of the representatives $H_i(\varphi)$ of the elements $\varphi \in L$.

Obviously, H_i is a homomorphism with respect to the rules 1—4. This implies the following

THEOREM 2. *Every representative of a finitely generated set is finitely generated.*

Theorem 2 enables us to construct infinitely generated subsets of $L(n)$ if an infinitely generated subset of $L(p^j)$, $p^j | n$, is known.

3. Maximal and precomplete maximal sets. For $n = p^k m$ (where p is prime, m is not divisible by p and $k \geqq 1$), we define the following subsets of $L(n)$:

$L_n^{(1-p)} \subset L(n)$ consists of all elements $(a_1, \dots, a_r, a_{r+1}) \in L(n)$ where at least r—1 of the numbers $a_1, \dots, a_r$ are divisible by p. Note that

$$\mathrm{Re}_2(L(n)) \subset L_n^{(1-p)}. \tag{1}$$

If $n = p$ then

$$\mathrm{Cl}(\mathrm{Re}_2(L(n))) = L_n^{(1-p)}.$$

Thus, in this case, $L_n^{(1-p)}$ is of order 1. If $n > p$ then $L_n^{(1-p)}$ is of order 2. Hence, the set $L_n^{(1-p)}$ is always finitely generated.

$L_n^{(p)} \subset L(n)$ consists of all elements $(a_1, \dots, a_r, a_{r+1}) \in L(n)$ where either all the numbers $a_1, \dots, a_r$ are divisible by p or r—1 of these numbers are divisible by p^2. Again, we have

$$\mathrm{Re}_2(L(n)) \subset L_n^{(p)}. \tag{1'}$$

The set $L_n^{(p)}$ is included in the set $L_n^{(1-p)}$, the inclusion being proper if $p^2 \not\equiv p$ (mod n).

It is easy to check that the sets $L_n^{(p)}$ and $L_n^{(1-p)}$ are closed. We shall now prove the following

THEOREM 3. *The set $L_n^{(1-p)}$ is precomplete. If n is divisible by p^2 then the set $L_n^{(p)}$ is maximal.*

Proof. To prove the first part of the theorem, we choose an arbitrary element

$$(2) \qquad \varphi \in L(n) - L_n^{(1-p)}.$$

We have to show that

$$(3) \qquad L' = \mathrm{Cl}(L_n^{(1-p)} \cup \{\varphi\}) = L(n).$$

It follows from (1), (2) and the fact that L' is closed under composition (rule 4) that, for some a and b where ab is not divisible by p,

$$(4) \qquad (a,b,0) \in L'.$$

Bearing in mind that $n = p^k m$, where m is not divisible by p, we choose a number i such that $b+ip \equiv 1 \pmod{m}$. The numbers $b+ip$ and n are relatively prime. Hence, we may choose a number j such that

$$(5) \qquad (b+ip)j \equiv 1 \quad (\mathrm{mod}\ n).$$

From the relation $(1,ip,0) \in L_n^{(1-p)}$ we infer, by (4), that $(a, b+ip, 0) \in L'$. Hence, by (5),

$$(6) \qquad (a,1,0) \in L'.$$

By repeating the same argument, we infer from (6) that $(1,1,0) \in L'$. Hence, by (1), the equation (3) follows.

To prove the latter part of the theorem, we note first that if $k \geqq 2$ then, for any $r \geqq 1$,

$$\underbrace{(p, \ldots, p, 0)}_{r \text{ copies}} \in L_n^{(p)} - \mathrm{Cl}(\mathrm{Re}_r(L_n^{(p)})).$$

This implies that the set $L_n^{(p)}$ is infinitely generated (for $p^2 | n$).

We shall now show that the only closed proper extensions of $L_n^{(p)}$ are the sets $L_n^{(1-p)}$ and $L(n)$. Since both of these sets are finitely generated, we may conclude that $L_n^{(p)}$ is maximal.

Let L'' be an arbitrary closed proper extension of $L_n^{(p)}$ and ψ an arbitrary element of the set $L'' - L_n^{(p)}$. Then

$$(7) \qquad L'' \supset L^* = \mathrm{Cl}(L_n^{(p)} \cup \{\psi\}).$$

By (1′), we may conclude that

$$(8) \qquad (c,d,0) \in L^*,$$

for some c and d where c is not divisible by p and d not divisible by p^2. We choose a number u such that $c+up^2\equiv 1 \pmod m$. Then the numbers $c+up^2$ and n are relatively prime. Finally, we choose a number v such that

$$(c+up^2)v\equiv 1 \pmod n. \tag{9}$$

From (8) and the relation $(up^2,1,0)\in L_n^{(p)}$ we obtain the relation $(c+up^2, d,0)\in L^*$ and hence, by (9), the relation

$$(1,d,0)\in L^*. \tag{10}$$

If d is not divisible by p we infer, by repeating the given argument, that $(1,1,0)\in L^*$. This implies, by (1′), that $L''=L^*=L(n)$.

Therefore, we write $d=pd_1$ where d_1 is not divisible by p. Let u_1 be such that $d_1+u_1p\equiv 1 \pmod m$ and v_1 such that

$$(d_1+u_1p)v_1\equiv 1 \pmod n. \tag{11}$$

Because $(1,u_1p^2,0)\in L_n^{(p)}$ we obtain, by (10), the relation $(1,p(d_1+u_1p),0)\in L^*$ and hence, by (11), the relation $(1,p,0)\in L^*$. This implies, by (1′), that $L^*\supset L_n^{(1-p)}$. Since the set $L_n^{(1-p)}$ is precomplete, we have either $L^*=L_n^{(1-p)}$ or $L^*=L(n)$. Hence, by (7), $L''=L_n^{(1-p)}$ or $L''=L(n)$. This completes the proof of theorem 3.

We shall now consider sets $L(n)$ where n is of the form $n=p^kq^lm$ where p and q are distinct primes, $k\geqq 2$, $l\geqq 1$ and neither p nor q divides m. Let $L_n^{(pq)}\subset L(n)$ be defined as follows:

$L_n^{(pq)}$ consists of all elements $(a_1,\dots,a_r,a_{r+1})\in L(n)$ where either all numbers $a_1,\dots,a_r$ are divisible by p or all divisible by q or r—1 of these numbers are divisible by pq. It is easy to verify that the set $L_n^{(pq)}$ is closed. Furthermore, we have

$$\operatorname{Re}_2(L(n))\subset L_n^{(pq)}. \tag{1″}$$

Our next theorem deals with problems B and C, mentioned in the introduction.

THEOREM 4. *The set $L_n^{(pq)}$ is both precomplete and maximal.*

Proof. For any $r\geqq 1$,

$$(\underbrace{p,\dots,p}_{r\text{ copies}},0)\in L_n^{(pq)}-\operatorname{Cl}(\operatorname{Re}_r(L_n^{(pq)})). \tag{12}$$

The relation (12) follows because n is divisible by both p^2 and pq and, hence, the element on the left side cannot be obtained from the elements of the set $\operatorname{Re}_r(L_n^{(pq)})$ by the rules 1—4 in section 2. (12) implies that $L_n^{(pq)}$ is infinitely generated. Therefore, if $L_n^{(pq)}$ is precomplete then it is also maximal.

To complete the proof of the theorem, we show that $L_n^{(pq)}$ is precomplete. Let $\varphi \in L(n) - L_n^{(pq)}$ be arbitrary and denote

$$L' = \mathrm{Cl}(L_n^{(pq)} \cup \{\varphi\}).$$

We have to show that $L' = L(n)$. It suffices to prove that

$$(1,1,0) \in L'. \tag{13}$$

By (1″), the set L' contains an element $(a,b,0)$ where a is not divisible by p and b not divisible by q. We assume first that b is not divisible by p. Choose a number i such that $b+ipq \equiv 1 \pmod{m}$. Then the numbers $b+ipq$ and n are relatively prime. Since we have $(1,ipq,0) \in L_n^{(pq)}$, we obtain the result $(a,b+ipq,0) \in L'$. This implies that $(a,1,0) \in L'$ and, finally,

$$(a,p,0) \in L'. \tag{14}$$

We assume next that $b = pb_1$. In this case, we choose a number j such that $b_1+jq \equiv 1 \pmod{pm}$. Because b is not divisible by q, this implies that b_1+jq and n are relatively prime. From the relation $(1,jpq,0) \in L_n^{(pq)}$ we infer the relation

$$(a,p(b_1+jq),0) \in L'$$

and, hence, the relation (14).

By a similar procedure, we eliminate the number a from (14) and obtain the result

$$(q,p,0) \in L'. \tag{15}$$

Let u be such that $up^2+q^2 \equiv 1 \pmod{qm}$. Since $(q,q,0)$ and $(up,up,0)$ are elements of the set $L_n^{(pq)}$, the relation

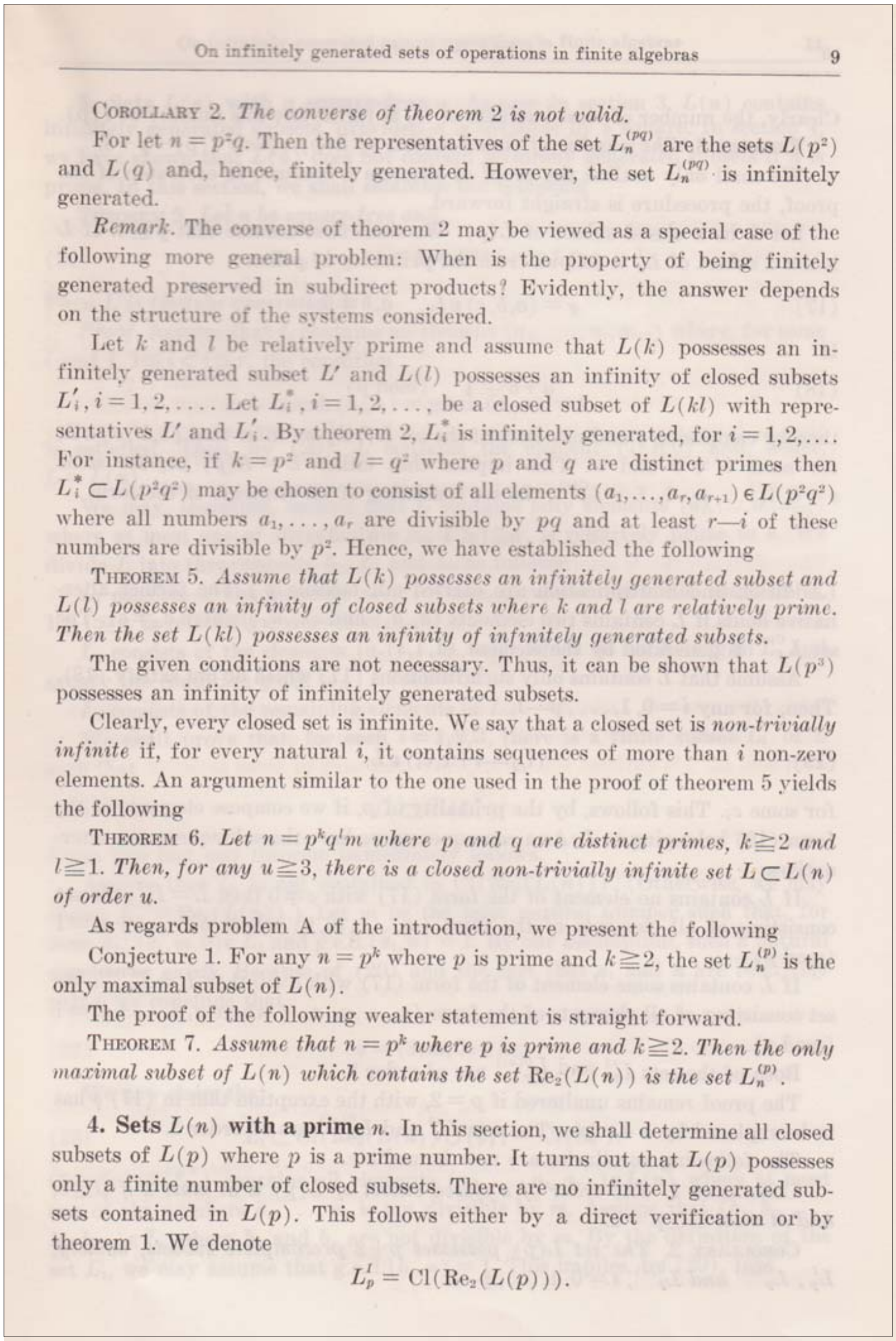
$$(up^2+q^2, up^2+q^2, 0) \in L' \tag{16}$$

is a consequence of (15). Because the numbers up^2+q^2 and n are relatively prime, (13) is implied by (16). Hence, theorem 4 follows.

We shall now present two corollaries of theorem 4.

COROLLARY 1. *Some infinitely generated sets are contained in two distinct maximal sets. (I.e. the maximal extension of an infinitely generated set is not always unique.)*

For let n be such that $L_n^{(pq)}$ is defined. By theorems 3 and 4, both $L_n^{(p)}$ and $L_n^{(pq)}$ are maximal. Consider the set $L_n^{(pp)} \subset L(n)$ consisting of all elements $(a_1,\ldots,a_r,a_{r+1}) \in L(n)$ where all numbers $a_1,\ldots,a_r$ are divisible by p. It is easy to verify that $L_n^{(pp)}$ is closed and infinitely generated. Furthermore, it is contained in both $L_n^{(p)}$ and $L_n^{(pq)}$.



Corollary 2. *The converse of theorem 2 is not valid.*

For let $n = p^2q$. Then the representatives of the set $L_n^{(pq)}$ are the sets $L(p^2)$ and $L(q)$ and, hence, finitely generated. However, the set $L_n^{(pq)}$ is infinitely generated.

Remark. The converse of theorem 2 may be viewed as a special case of the following more general problem: When is the property of being finitely generated preserved in subdirect products? Evidently, the answer depends on the structure of the systems considered.

Let k and l be relatively prime and assume that $L(k)$ possesses an infinitely generated subset L' and $L(l)$ possesses an infinity of closed subsets $L'_i, i = 1, 2, \ldots$. Let $L_i^*, i = 1, 2, \ldots$, be a closed subset of $L(kl)$ with representatives L' and L'_i. By theorem 2, L_i^* is infinitely generated, for $i = 1, 2, \ldots$. For instance, if $k = p^2$ and $l = q^2$ where p and q are distinct primes then $L_i^* \subset L(p^2q^2)$ may be chosen to consist of all elements $(a_1, \ldots, a_r, a_{r+1}) \in L(p^2q^2)$ where all numbers $a_1, \ldots, a_r$ are divisible by pq and at least $r—i$ of these numbers are divisible by p^2. Hence, we have established the following

Theorem 5. *Assume that $L(k)$ possesses an infinitely generated subset and $L(l)$ possesses an infinity of closed subsets where k and l are relatively prime. Then the set $L(kl)$ possesses an infinity of infinitely generated subsets.*

The given conditions are not necessary. Thus, it can be shown that $L(p^3)$ possesses an infinity of infinitely generated subsets.

Clearly, every closed set is infinite. We say that a closed set is *non-trivially infinite* if, for every natural i, it contains sequences of more than i non-zero elements. An argument similar to the one used in the proof of theorem 5 yields the following

Theorem 6. *Let $n = p^kq^lm$ where p and q are distinct primes, $k \geqq 2$ and $l \geqq 1$. Then, for any $u \geqq 3$, there is a closed non-trivially infinite set $L \subset L(n)$ of order u.*

As regards problem A of the introduction, we present the following

Conjecture 1. For any $n = p^k$ where p is prime and $k \geqq 2$, the set $L_n^{(p)}$ is the only maximal subset of $L(n)$.

The proof of the following weaker statement is straight forward.

Theorem 7. *Assume that $n = p^k$ where p is prime and $k \geqq 2$. Then the only maximal subset of $L(n)$ which contains the set $\mathrm{Re}_2(L(n))$ is the set $L_n^{(p)}$.*

4. Sets $L(n)$ with a prime n. In this section, we shall determine all closed subsets of $L(p)$ where p is a prime number. It turns out that $L(p)$ possesses only a finite number of closed subsets. There are no infinitely generated subsets contained in $L(p)$. This follows either by a direct verification or by theorem 1. We denote

$$L_p^I = \mathrm{Cl}(\mathrm{Re}_2(L(p))).$$

Clearly, the number of closed subsets of L_p^I is finite. Let this number be $I(p)$.

THEOREM 8. *The number of closed subsets of* $L(p)$ *equals* $I(p)+p+3$.

We shall only outline the proof of theorem 8 because, at each step of the proof, the procedure is straight forward.

Let L be a closed subset of $L(p)$. We shall first assume that $p \geqq 3$. If L is not a subset of L_p^I it follows from the primality of p that

$$\varphi = (a,b,c) \in L, \quad a,b \neq 0. \tag{17}$$

If

$$a+b \not\equiv 1 \pmod p \tag{18}$$

then by composing φ and members of the set $L \cap L_p^I$ we infer that $(1,b',c') \in L$, for some $b' \neq 0$ and c'. This implies that either $L = L(p)$ or, for some $s = 0, 1, \dots, p-1$, $L = L_p^{C(s)}$, the set consisting of all elements of the form

$$(a_1, \dots, a_r, (a_1 + \dots + a_r - 1)s).$$

(Addition and multiplication are carried out modulo p.) The former alternative holds if L contains two elements (a_1, a_2) and (a_1, a_2') where $a_2 \neq a_2'$. The set $L_p^{C(s)}$ is generated by the element $(1,1,s)$.

Assume that L contains only such functions (17) which do not satisfy (18). Then, for any $i = 0, 1, \dots, p-1$,

$$(i, p-i+1, c_i) \in L, \tag{19}$$

for some c_i. This follows, by the primality of p, if we compose elements of the form (19) belonging to L. As a consequence, we have the subsequent two alternatives:

If L contains no element of the form (17) with $c \neq 0$ then $L = L_p^{+1}$, the set consisting of all elements of the form $(a_1, \dots, a_r, 0)$ where $a_1 + \dots + a_r \equiv 1 \pmod p$.

If L contains some element of the form (17) with $c \neq 0$ then $L = L_p^{C(+1)}$, the set consisting of all elements of the form $(a_1, \dots, a_r, a_{r+1})$ where $a_1 + \dots + a_r \equiv 1 \pmod p$.

Both of the sets L_p^{+1} and $L_p^{C(+1)}$ are of order 2.

The proof remains unaltered if $p = 2$, with the exception that in (17) φ has to be replaced by a 4-tuple. The sets L_2^{+1} and $L_2^{C(+1)}$ are of order 3.

The following corollaries are now immediate.

COROLLARY 1. *The order of a closed subset of* $L(p)$ *is at most* 2 *if* $p \geqq 3$, *and at most* 3 *if* $p = 2$.

COROLLARY 2. *The set* $L(p)$ *possesses* $p+2$ *precomplete subsets, namely,* L_p^I, $L_p^{C(+1)}$ *and* $L_p^{C(s)}$, $s = 0, 1, \dots, p-1$.

5. Sets $L(n)$ with a square-free n. As seen in section 3, $L(n)$ contains infinitely generated subsets, provided n is divisible by a square. In section 4, we have shown that $L(n)$ does not contain infinitely generated subsets if n is prime. In this section, we shall establish the following

THEOREM 9. *Let n be square-free and*

$$\mathrm{Re}_2(L(n)) \subset L = \mathrm{Cl}(L) \subset L(n). \tag{20}$$

Then L is finitely generated.

Proof. Assume that L contains an element $(a_1, \ldots, a_r, a_{r+1})$ where, for some i and j, $1 \leqq i < j \leqq r$, the condition

$$\text{g.c.d. } (a_i, n) = \text{g.c.d. } (a_j, n) = 1$$

is satisfied. Then, by (20), L contains the element $(1, 1, 0)$ and, hence, $L = L(n)$.

We may, therefore, assume that L contains only elements $(a_1, \ldots, a_r, a_{r+1})$ where at most one of the numbers a_i, $1 \leqq i \leqq r$, is relatively prime to n. We divide L into three subsets L_1, L_2 and L_3 as follows:

L_1 consists of the elements $(a_1, \ldots, a_r, a_{r+1})$ where one of the numbers a_i, $1 \leqq i \leqq r$, is relatively prime to n.

L_2 consists of the elements $(a_1, \ldots, a_r, a_{r+1})$ which do not belong to L_1 and satisfy the condition g.c.d. $(a_1, \ldots, a_r) = 1$.

L_3 consists of the remaining elements of L.

We shall prove that, for each $i = 1, 2, 3$, there is a finite subset L_i' of L such that

$$L_i \subset \mathrm{Cl}(L_i'). \tag{21}$$

From this fact, our theorem immediately follows.

Assume that L_1 is not contained in $\mathrm{Cl}(\mathrm{Re}_2(L(n)))$. (Otherwise, we may choose $L_1' = \mathrm{Re}_2(L(n))$.) Let m be the least natural number such that, for some a_1, $(a_1, m, 0) \in L_1$ and g.c.d.$(a_1, n) = 1$. By our assumption, such a natural number m exists. Because of (20) and the fact that a_1 and n are relatively prime we conclude that

$$\varphi = (1, m, 0) \in L_1. \tag{22}$$

We now claim that

$$L_1 \subset \mathrm{Cl}(\mathrm{Re}_2(L(n)) \cup \{\varphi\}) = \mathrm{Cl}(L_1'). \tag{23}$$

Clearly, $\mathrm{Cl}(L_1')$ contains all elements $(a_1, \ldots, a_r, a_{r+1}) \in L(n)$ where at most one of the numbers $a_1, \ldots, a_r$ is not divisible by m. Assume that $(b_1, b_2, \ldots, b_r, b_{r+1}) \in L_1$ where b_1 and b_2 are not divisible by m. By the definition of the set L_1, we may assume that g.c.d.$(b_1, n) = 1$. This implies, by (20), that

$$(24) \qquad (1, b_2, 0) \in L_1.$$

It is a consequence of (20), (22) and (24) that

$$(25) \qquad (1, \text{g.c.d.}(m, b_2), 0) \in L_1.$$

By our assumption concerning b_2, (25) contradicts the choice of m. Hence, (23) follows.

Next, we consider the set L_2. We denote by L_2'' the subset of L_2 consisting of all elements $(a_1, \ldots, a_r, 0) \in L_2$ such that $\text{g.c.d.}(a_1, \ldots, a_r) = 1$ but any r—1 of the numbers $a_1, \ldots, a_r$ possess a g.c.d. > 1. Such an r-tuple $(a_1, \ldots, a_r)$ is referred to as a *minimal system* in the sequel. Obviously, the set L_2'' is finite. Let s be the greatest number of elements in a minimal system and assume that L_2 is not contained in $\text{Cl}(\text{Re}_{s+1}(L_2))$. Let m' be the least natural number such that, for some minimal system $(a_1, \ldots, a_r)$, $(a_1, \ldots, a_r, m', 0) \in L_2$. Then, by (20), $\varphi' = (1, m', 0) \in L$. Now it can be shown that

$$(26) \qquad L_2 \subset \text{Cl}(L_2'' \cup \text{Re}_2(L(n)) \cup \{\varphi'\}).$$

The relation (26) is established in the same fashion as (23).

To show that (21) holds also for $i = 3$, we proceed as follows. For every member $(a_1, \ldots, a_r, a_{r+1}) \in L_3$, the condition

$$(27) \qquad \text{g.c.d.}(a_1, \ldots, a_r) = d > 1$$

holds, for some d. Consider the subset $L_3^{(d)}$ of L_3 consisting of all elements $(a_1, \ldots, a_r, a_{r+1})$ satisfying (27). Because there is only a finite number of such sets $L_3^{(d)}$, it suffices for us to prove that each of them satisfies

$$(28) \qquad L_3^{(d)} \subset \text{Cl}(L_4^{(d)})$$

where $L_4^{(d)} \subset L$ is finite. If d and n are relatively prime then (28) follows, by (20) and the fact that (21) holds for $i = 2$. If $\text{g.c.d.}(d, n) = d_1 > 1$ then either (28) holds or the set $L(nd_1^{-1})$ possesses an infinitely generated subset which contains the set $\text{Re}_2(L(nd_1^{-1}))$. This is a consequence of the fact that n is square-free.

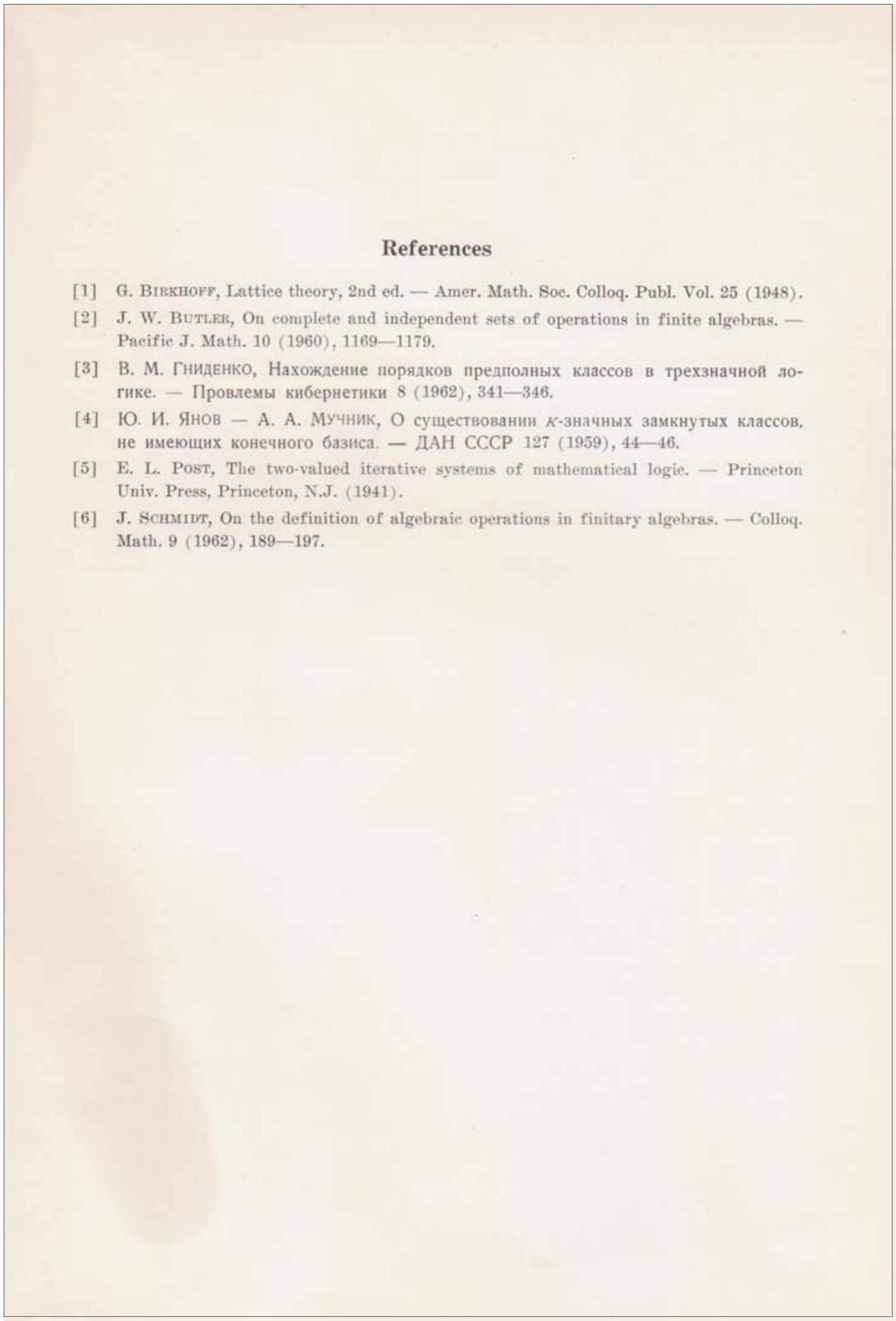
Thus, we have shown that if our theorem is not valid for some square-free n then it is not valid for some square-free n' where $1 < n' < n$. By theorem 8 (and theorem 1), this completes the proof of theorem 9.

We end up with the following

Conjecture 2. The set $L(n)$ does not possess infinitely generated subsets if n is square-free.

Conjecture 2 implies that $L(n)$ possesses infinitely generated subsets if and only if n is divisible by a square. By theorems 7 and 9, both conjecture 1 and conjecture 2 are implied by the following

Conjecture 3. If $L \subset L(n)$ is infinitely generated then also $\text{Cl}(L \cup \{\varphi\})$ is infinitely generated, for any $\varphi \in \text{Re}_2(L(n))$.



References

[1] G. Birkhoff, Lattice theory, 2nd ed. — Amer. Math. Soc. Colloq. Publ. Vol. 25 (1948).

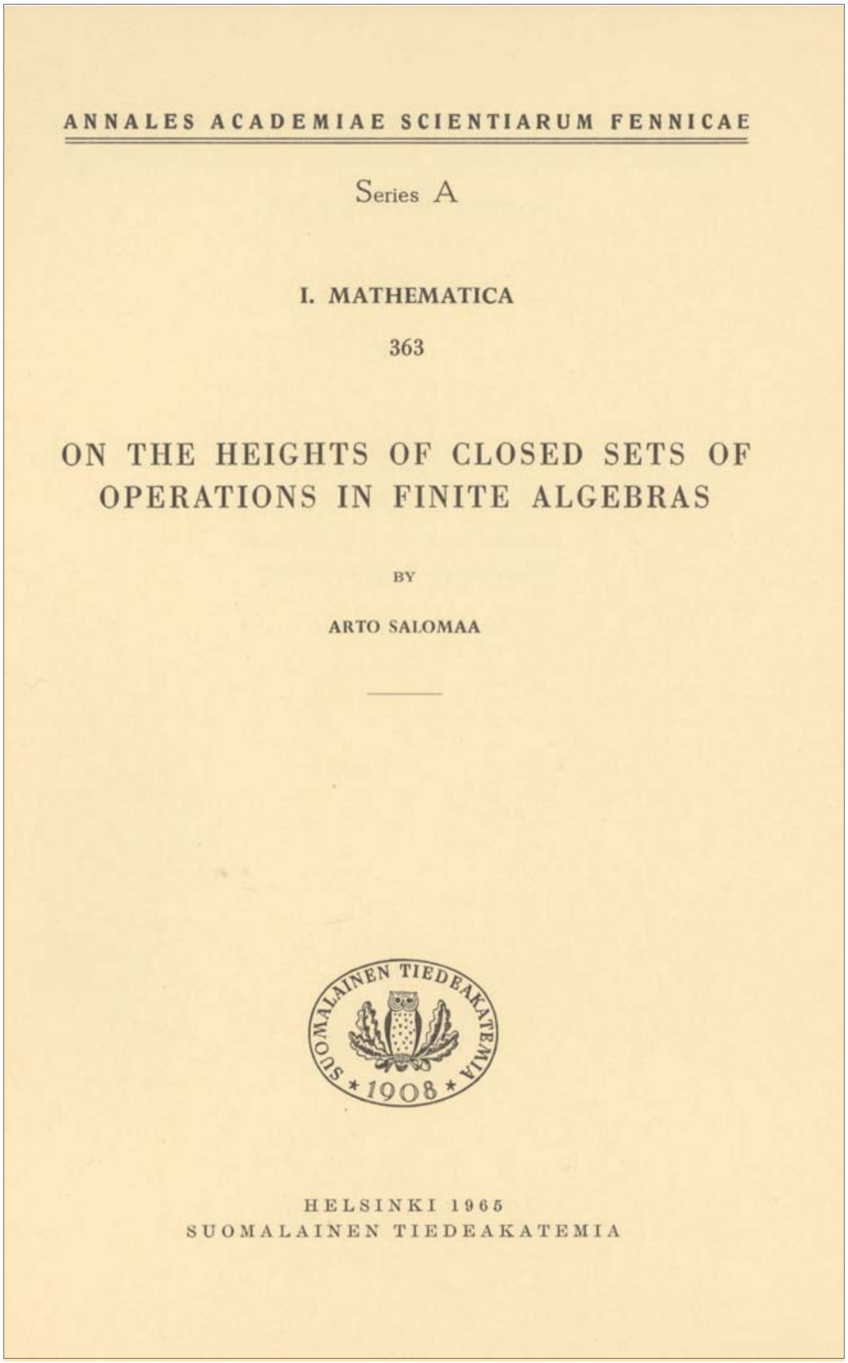
[2] J. W. Butler, On complete and independent sets of operations in finite algebras. — Pacific J. Math. 10 (1960), 1169—1179.

[3] В. М. Гниденко, Нахождение порядков предполных классов в трехзначной логике. — Провлемы кибернетики 8 (1962), 341—346.

[4] Ю. И. Янов — А. А. Мучник, О существовании κ-значных замкнутых классов, не имеющих конечного базиса. — ДАН СССР 127 (1959), 44—46.

[5] E. L. Post, The two-valued iterative systems of mathematical logic. — Princeton Univ. Press, Princeton, N.J. (1941).

[6] J. Schmidt, On the definition of algebraic operations in finitary algebras. — Colloq. Math. 9 (1962), 189—197.



ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

363

ON THE HEIGHTS OF CLOSED SETS OF OPERATIONS IN FINITE ALGEBRAS

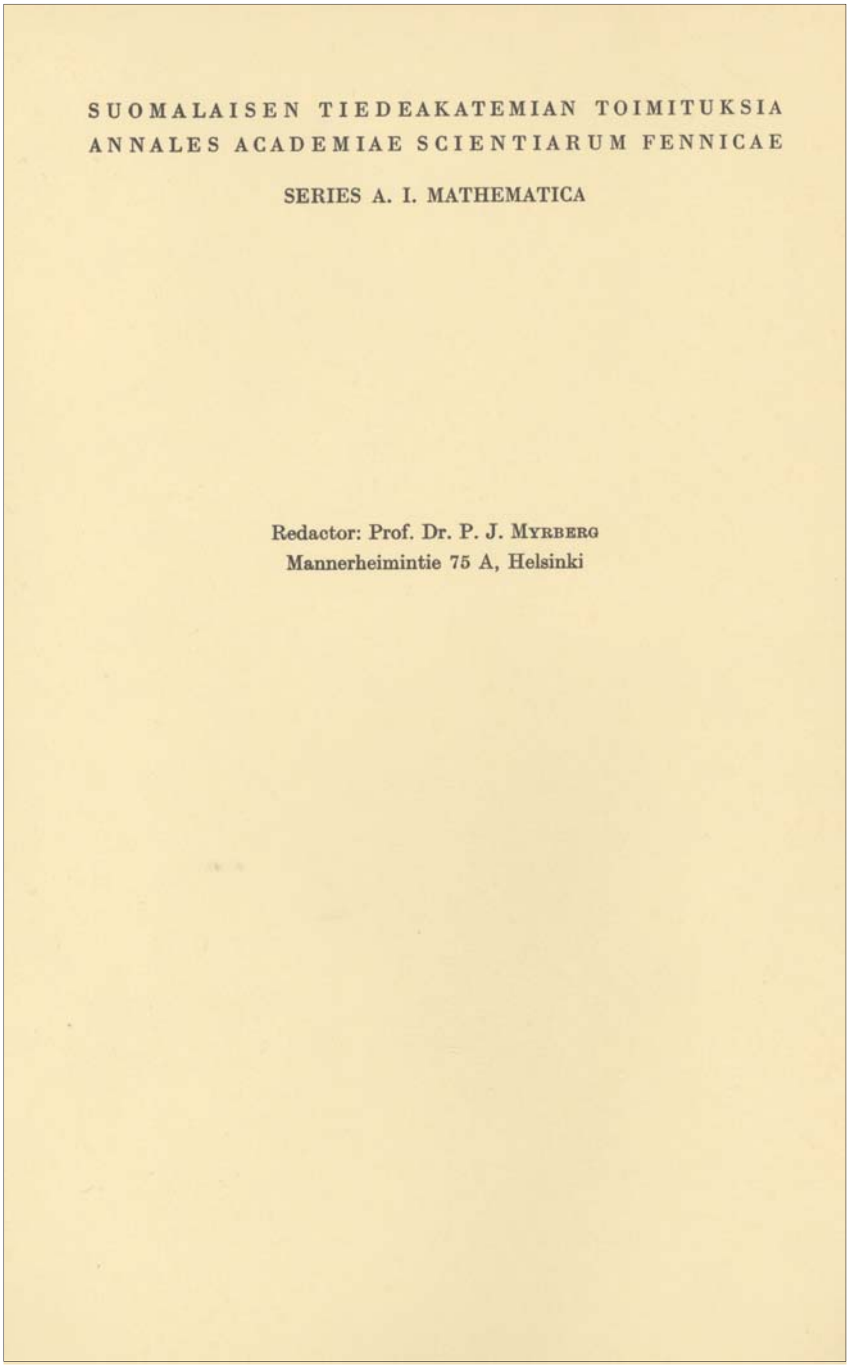
BY

ARTO SALOMAA

SUOMALAINEN TIEDEAKATEMIA

1908

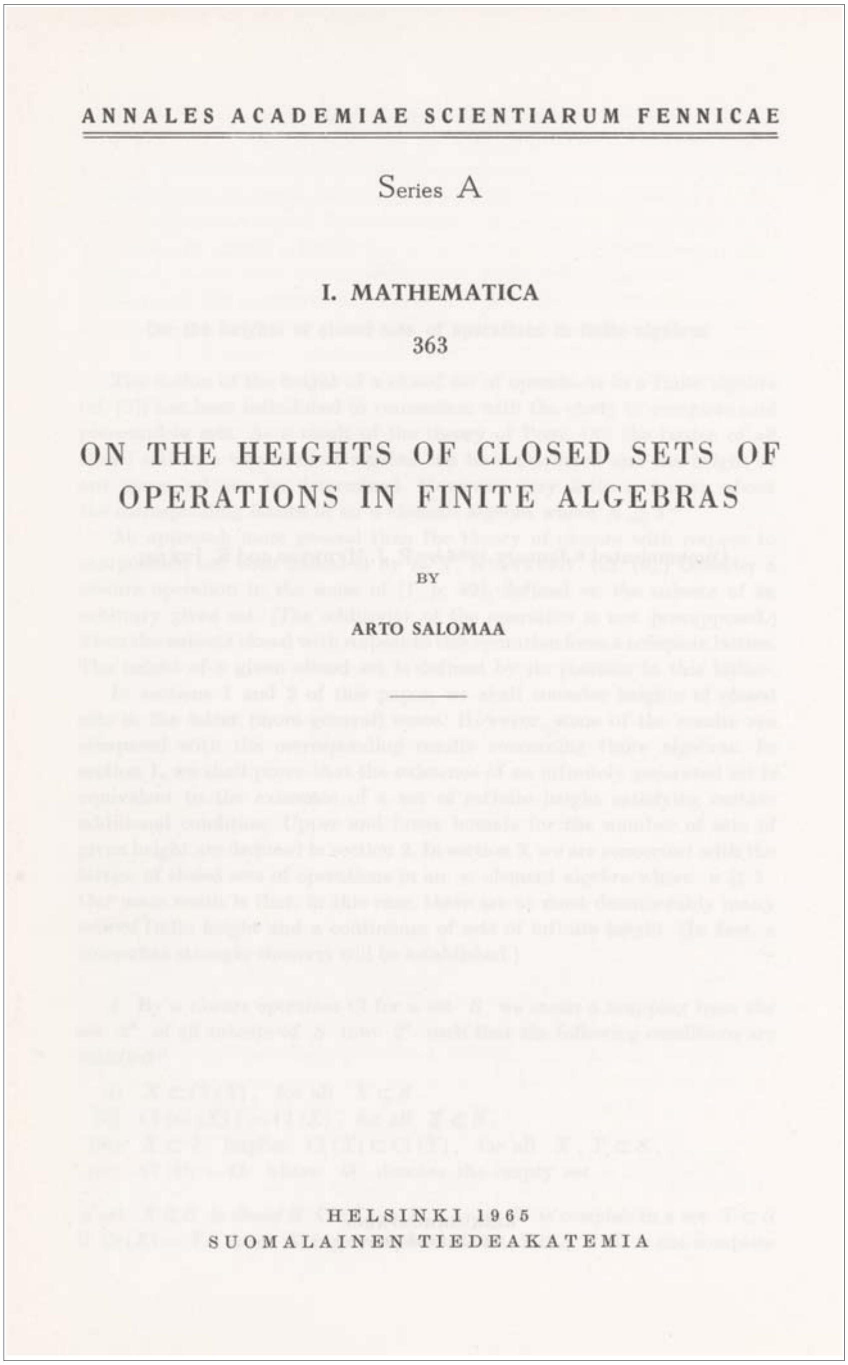
HELSINKI 1965
SUOMALAINEN TIEDEAKATEMIA



SUOMALAISEN TIEDEAKATEMIAN TOIMITUKSIA
ANNALES ACADEMIAE SCIENTIARUM FENNICAE

SERIES A. I. MATHEMATICA

Redactor: Prof. Dr. P. J. Myrberg
Mannerheimintie 75 A, Helsinki



ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

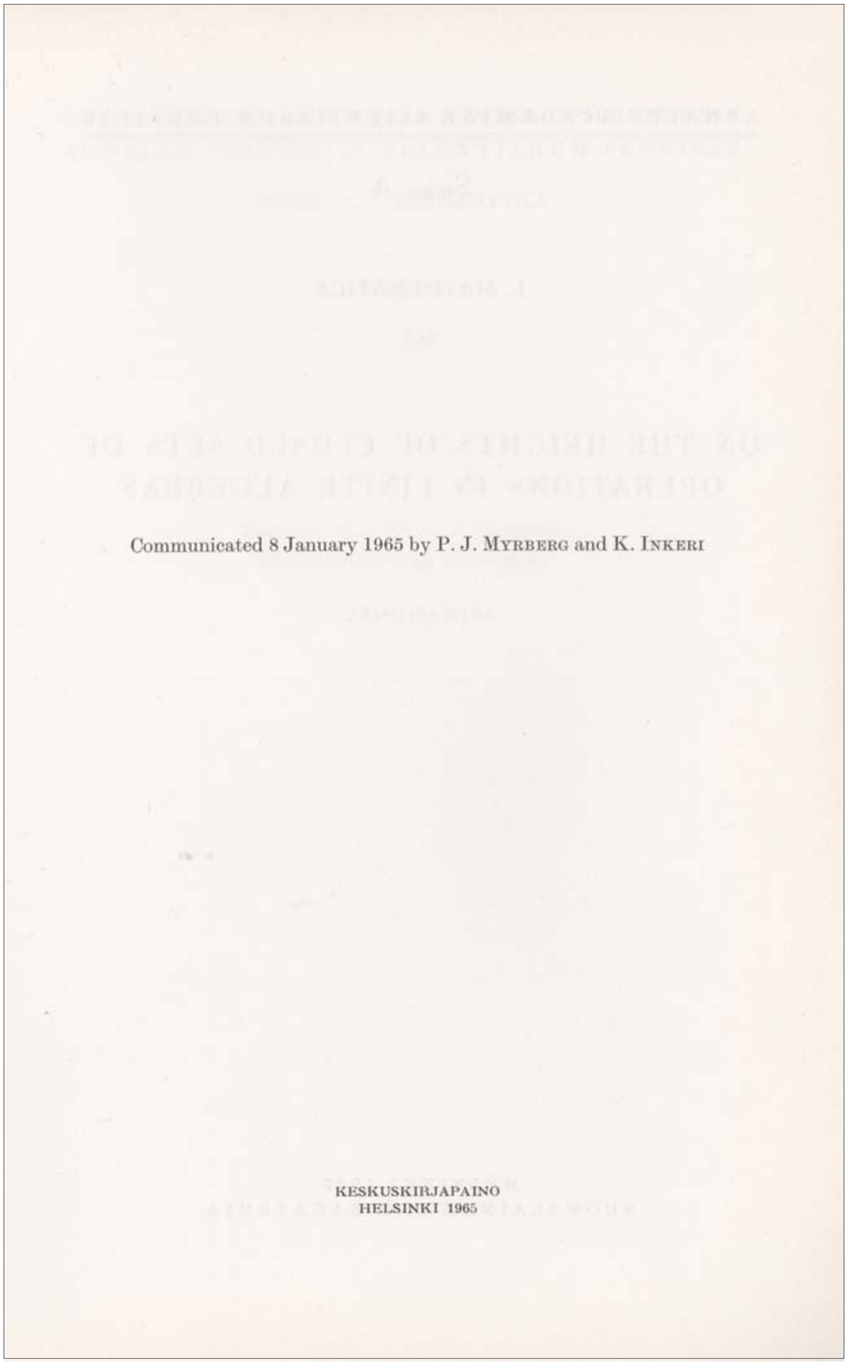
363

ON THE HEIGHTS OF CLOSED SETS OF OPERATIONS IN FINITE ALGEBRAS

BY

ARTO SALOMAA

HELSINKI 1965
SUOMALAINEN TIEDEAKATEMIA



Communicated 8 January 1965 by P. J. Myrberg and K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1965

On the heights of closed sets of operations in finite algebras

The notion of the height of a closed set of operations in a finite algebra (cf. [2]) has been introduced in connection with the study of complete and precomplete sets. As a result of the theory of Post, [8], the lattice of all closed sets in a two-element algebra can be constructed and the height of any given set can be determined. However, very little is known about the corresponding lattice in an n-element algebra where $n \geqq 3$.

An approach more general than the theory of closure with respect to composition has been indicated by A. V. Kuznetsov. (Cf. [6].) Consider a closure operation in the sense of [1, p. 49], defined on the subsets of an arbitrary given set. (The additivity of the operation is not presupposed.) Then the subsets closed with respect to this operation form a complete lattice. The height of a given closed set is defined by its position in this lattice.

In sections 1 and 2 of this paper, we shall consider heights of closed sets in the latter (more general) sense. However, some of the results are compared with the corresponding results concerning finite algebras. In section 1, we shall prove that the existence of an infinitely generated set is equivalent to the existence of a set of infinite height satisfying certain additional condition. Upper and lower bounds for the number of sets of given height are deduced in section 2. In section 3, we are concerned with the lattice of closed sets of operations in an n-element algebra where $n \geqq 3$. Our main result is that, in this case, there are at most denumerably many sets of finite height and a continuum of sets of infinite height. (In fact, a somewhat stronger theorem will be established.)

1. By a *closure operation* Cl for a set S we mean a mapping from the set 2^S of all subsets of S into 2^S such that the following conditions are satisfied:

(i) $X \subset \mathrm{Cl}\,(X)$, for all $X \subset S$.
(ii) $\mathrm{Cl}\,(\mathrm{Cl}\,(X)) = \mathrm{Cl}\,(X)$, for all $X \subset S$.
(iii) $X \subset Y$ implies $\mathrm{Cl}\,(X) \subset \mathrm{Cl}\,(Y)$, for all $X, Y \subset S$.
(iv) $\mathrm{Cl}\,(\emptyset) = \emptyset$ where $\emptyset$ denotes the empty set.

A set $X \subset S$ is *closed* if $\mathrm{Cl}\,(X) = X$. A set X is *complete* in a set $Y \subset S$ if $\mathrm{Cl}\,(X) = Y$. A set X is *precomplete* in a set $Y \subset S$ if X is not complete in Y, the set $Y - X$ is not empty and, for any $z \in Y - X$, the set $X \cup \{z\}$ is complete in Y. (It is obvious that a set precomplete in another set is closed.) Sets complete (precomplete) in S are termed, shortly, complete (precomplete). A set $X \subset S$ is *finitely generated* if there is a finite set $X_1 \subset X$ such that $X \subset \mathrm{Cl}(X_1)$. Otherwise, X is *infinitely generated.*

The *height* of a closed set $X \subset S$ is defined as follows. The height of S equals 0. The height of a set $X \neq S$ equals $l\,(l > 0)$ if, for all elements $z \in S - X$, the height of $\mathrm{Cl}(X \cup \{z\})$ is less than or equal to $l - 1$ and, for some $z_0 \in S - X$, the height of $\mathrm{Cl}(X \cup \{z_0\})$ equals $l - 1$. (Hence, the height of a precomplete set equals 1.) A closed set X is of *infinite height* if, for all natural numbers k, there is a sequence $x_1, \ldots, x_k$ of elements of S such that

$$x_1 \notin X \tag{1}$$

and

$$x_i \notin \mathrm{Cl}(X \cup \{x_1, \ldots, x_{i-1}\}), \tag{2}$$

for all i where $2 \leqq i \leqq k$. A closed set X is of *sequentially infinite height* if there is an infinite sequence x_i, $i = 1, 2, \ldots$, of elements of S satisfying conditions (1) and (2).

It follows that every set of sequentially infinite height is of infinite height. The converse is not true. As a counter-example we mention the well-known sets F_i^∞, $i = 1, \ldots, 8$, defined in [8]. (Whenever possible we consider examples of sets of operations in the algebra of logic or, more generally, in finite algebras where closure means closure with respect to composition.)

Let $X \neq S$ be a closed set. A sequence of closed sets $X_1 = X$, $X_2, \ldots, X_k$ is termed a *composition sequence* of X if X_k is precomplete and, for all i where $1 \leqq i \leqq k - 1$, X_i is precomplete in X_{i+1}. The number k is referred to as the *length* of the composition sequence. A sequence $\{x_i\}$ (finite or infinite) of elements of S satisfying conditions (1) and (2) is termed a *sequence of elements independent of* X or, shortly, an *I-sequence* of X. The number of elements in an I-sequence is referred to as its leng h. We note that neither composition sequences nor I-sequences are unique. Furthermore, every closed set $X \neq S$ possesses an I-sequence whereas it is not necessary for such an X to possess a composition sequence.

We omit the proof of our first theorem because it is straight forward from the definitions.

Theorem 1. *A set X is of infinite height if and only if there is no non-negative integer l, such that X is of height l. Furthermore, for any natural number k, the following three conditions are equivalent:* (1) *The height of X*

equals k. (2) *The length of the longest I-sequence of* X *equals* k. (3) X *possesses a composition sequence of length* k *and no I-sequence of length* $k+1$.

It is a consequence of theorem 1 that if a closed set X with the finite height l_X is properly included in a closed set Y with height l_Y then $l_X \geqq l_Y + 1$. If the equality holds then X is precomplete in Y . The converse of this statement is not valid. (Thus, for the sets considered in [8], D_1 is precomplete in D_3 but the height of the latter equals 1 whereas the height of the former equals 3.) Furthermore, if a set possesses no subsets of a finite height l then it possesses neither subsets of a finite height $l_1 > l$ nor subsets which are of infinite but not of sequentially infinite height. We shall now prove the following

Theorem 2. *If a finitely generated set* X *is included in an infinitely generated set then* X *is a subset of a set of sequentially infinite height. Conversely, if* X *is of sequentially infinite height then it is a subset of some infinitely generated set.*

Proof. Assume that $X \subset Y$ where X is finitely and Y infinitely generated. Hence, there is a finite set $X_1 \subset X$ such that

$$X \subset \mathrm{Cl}\,(X_1)\,. \tag{3}$$

Since Y is infinitely generated, there is an element $z_1 \in Y - \mathrm{Cl}\,(X_1)$. Denote

$$X^{(k)} = \mathrm{Cl}\,(X_1 \cup \{z_1, \ldots, z_k\})\,, \quad k \geqq 1\,. \tag{4}$$

Then there is an element

$$z_{k+1} \in Y - X^{(k)} \tag{5}$$

because the relation

$$Y \subset \mathrm{Cl}\,(X_1 \cup \{z_1, \ldots, z_k\})$$

contradicts our assumption. The relations (3), (4) and (5) guarantee the existence of an infinite sequence satisfying conditions (1) and (2) with X replaced by $\mathrm{Cl}\,(X_1)$. Thus, the first part of theorem 2 follows.

Assume next that X is of sequentially infinite height. Then there is an infinite sequence $\{x_i\}$ satisfying conditions (1) and (2). We claim that the set

$$X' = X \cup \bigcup_{i=1}^{\infty} x_i$$

is infinitely generated. Assume the contrary: there is a finite $Z \subset X'$ such that

$$X' \subset \mathrm{Cl}\,(Z)\,. \tag{6}$$

Since Z is finite, there is a natural number r such that

$$Z \subset X \cup \{x_1, \ldots, x_r\} . \tag{7}$$

By (6) and (7), we obtain

$$x_{r+1} \in X' \subset \mathrm{Cl}\,(Z) \subset \mathrm{Cl}\,(X \cup \{x_1, \ldots, x_r\})$$

which contradicts the condition (2). Hence, X' is infinitely generated. This completes the proof of theorem 2.

Because the unit set of any element is finitely generated and, hence, all infinitely generated sets possess finitely generated subsets we may infer the following theorem as a corollary of theorem 2.

Theorem 3. *For any set S and closure operation Cl, S possesses an infinitely generated subset if and only if S possesses a subset of sequentially infinite height.*

It is a result of Post, [8, p. 94], that there are no infinitely generated sets in the algebra of logic. Hence, by theorem 3, there are no sets of sequentially infinite height. (This result can be obtained directly by considering the corresponding lattice.) In section 3, we shall show that in an n-element algebra $(n \geqq 3)$ there is a continuum of sets of sequentially infinite height.

Our next theorem gives a characterization of finitely generated sets. It is an extension of a theorem by Jablonskiĭ, [4, p. 78], for the general case.

Theorem 4. *If a closed set S is finitely generated then every sequence $\{S_i\}$ of closed sets satisfying conditions*

$$S_1 \subset S_2 \subset \ldots \subset S_i \subset \ldots \tag{8}$$

and

$$S = \bigcup_{i=1}^{\infty} S_i \tag{9}$$

satisfies also condition

$$S = S_r , \text{ for some } r \geqq 1 . \tag{10}$$

Conversely, if a closed set S is denumerable and every sequence $\{S_i\}$ of closed sets satisfying (8) *and* (9) *also satisfies* (10) *then S is finitely generated.*

Proof. The proof of the first part is identical with the corresponding proof for finite algebras. (Cf. [4, p. 78].) To prove the converse part, denote the elements of S by x_i, $i = 1, 2, \ldots$. Then

$$\{\mathrm{Cl}\,(\{x_1, \ldots, x_i\}) \mid i \geqq 1\}$$

is a sequence of closed sets satisfying conditions (8) and (9). By the assumption, it satisfies also condition (10) which means that S is finitely generated. This proves theorem 4.

The latter part of theorem 4 is not valid if S is non-denumerable. If we define (denoting the cardinal of X by card (X)), for $X \subset S$,

$$\mathrm{Cl}\ (X) = \begin{cases} X \text{ if card } (X) < \text{card } (S) \\ S \text{ if card } (X) = \text{card } (S) \end{cases}$$

then every sequence satisfying (8) and (9) also satisfies (10). However, S is not finitely generated.

2. Following [4], we denote by $\mathfrak{P}_n$ the set of functions whose variables, finite in number, range over a fixed finite set N of $n \geqq 2$ elements and whose values are included in N. For $X \subset \mathfrak{P}_n$, $\mathrm{Cl}(X)$ is defined to be the closure of X under composition. One of the basic results (cf. [4, p. 79]) concerning finite algebras thus defined is that every finitely generated closed subset of $\mathfrak{P}_n$ (in particular, $\mathfrak{P}_n$ itself) possesses only a finite number of sets precomplete in it. As will be seen below, this result is not valid for arbitrary sets S and closure operations Cl. We shall consider the problem of determining the range of the number of precomplete sets and, more generally, the range of the number of sets of given height.

We denote by $PC(S\,,\mathrm{Cl})$ the cardinal of the family of sets precomplete in S with respect to the closure operation Cl. Furthermore, we use the customary notations $\binom{k}{l}$ for the binomial coefficient and $[x]$ for the greatest integer less than or equal to x. In the next theorem, we shall give an upper bound for $PC(S\,,\mathrm{Cl})$. It is also shown that the given bound is the best-possible in the general case.

Theorem 5. *Assume that the cardinal of a non-empty set S equals $\mathfrak{c}$. Then*

$$PC(S\,,\mathrm{Cl}) \leqq \begin{cases} 2^{\mathfrak{c}} \textit{ if } \mathfrak{c} \textit{ is infinite} \\ \binom{\mathfrak{c}}{[\frac{1}{2}\mathfrak{c}]} \textit{if } \mathfrak{c} \textit{ is finite} \end{cases} \tag{11}$$

and, for any S, Cl may be defined in such a way that the equality holds in (11).

Proof. We assume first that the given set S is infinite. Because $PC(S\,,\mathrm{Cl})$ cannot exceed the cardinal of the family of all subsets of S we obtain the estimate (11). To show that, for any S, the operation Cl may be defined in such a way that there are $2^{\mathfrak{c}}$ sets precomplete in S, we proceed as follows. We divide S into two disjoint subsets S_1 and S_2 satisfying the condition

$$\text{card } (S_1) = \text{card } (S_2) = \text{card } (S) = \mathfrak{c}\,. \tag{12}$$

Let φ be a bijective mapping from S_1 onto S_2. We denote

$$R = \{(x_1\,, x_2)\,|x_1 \in S_1\,, x_2 = \varphi(x_1)\}\,. \tag{13}$$

For $X \subset S$, $\mathrm{Cl}(X)$ is defined as follows:

$$\mathrm{Cl}(X) = \begin{cases} S & \text{if } x_1 , x_2 \in X \text{ such that } (x_1 , x_2) \in R \\ X , & \text{otherwise.} \end{cases}$$

(It is clear that the postulates (i)—(iv) for closure operations are satisfied.) For any $X \subset S_1$, the set

$$X \cup \{\varphi(x) \mid x \in S_1 - X\} \tag{14}$$

is precomplete in S . Because all sets (14) are distinct we conclude, by (12), that there are $2^{\mathfrak{c}}$ sets precomplete in S .

Assume next that the given set S is finite. It is obvious that there are no two precomplete sets such that one of them is included in the other. It is shown in [10] that every family of subsets S_i of a set of finite cardinal $\mathfrak{c}$, such that $S_i \not\subset S_j$ for $i \neq j$ contains at most $\binom{\mathfrak{c}}{[\frac{1}{2}\mathfrak{c}]}$ elements. Thus, we obtain the estimate (11) also in this case. On the other hand, given a set S of finite cardinal $\mathfrak{c}$, we define the operation Cl, for $X \subset S$, as follows:

$$\mathrm{Cl}(X) = \begin{cases} S & \text{if card } (X) > [\frac{1}{2}\mathfrak{c}] \\ X , & \text{otherwise.} \end{cases}$$

Then every set of cardinal $[\frac{1}{2}\mathfrak{c}]$ is precomplete in S and, thus, S possesses $\binom{\mathfrak{c}}{[\frac{1}{2}\mathfrak{c}]}$ precomplete subsets. This completes the proof of theorem 5.

Remark. The first part of the proof shows that a finitely generated set S of infinite cardinal $\mathfrak{c}$ may possess $2^{\mathfrak{c}}$ precomplete subsets. (An obvious modification of the method yields an infinitely generated set with $2^{\mathfrak{c}}$ precomplete subsets.) There are other well-known results concerning finite algebras which are not valid in the general case. Thus, if a set S is finitely generated then every complete set possesses a finite complete subset. By considering the following example (where S is an infinite set and $x_0 \in S$ a fixed element), we see that this result is not valid in the general case:

$$\mathrm{Cl}(X) = \begin{cases} X & \text{if } X \text{ is properly included in } S - \{x_0\} \\ S , & \text{otherwise.} \end{cases}$$

Another result valid for finite algebras (and also for finitely generated groups, cf. [7, theorem 5]) is that every proper subset of a finitely generated set S is also a subset of a set precomplete in S . The following example (where S and x_0 are as above) shows that this result is not valid in the general case:

$$\mathrm{Cl}(X) = \begin{cases} S & \text{if } x_0 \in X \text{ or } X \text{ is infinite} \\ X , & \text{otherwise.} \end{cases} \tag{15}$$

We shall now determine an upper bound for the number of subsets of given height when the basic set S is of infinite cardinal $\mathfrak{c}$. It is obvious that $2^{\mathfrak{c}}$ is an upper bound for this number, and it turns out that it is also the best-possible one. It is easy to define Cl in such a manner that S possesses $2^{\mathfrak{c}}$ subsets of sequentially infinite height. An obvious modification of the first part of the proof of theorem 5 yields $2^{\mathfrak{c}}$ subsets of given finite height l. For the remaining case, the construction is carried out in the proof of the following.

Theorem 6. *For any set S of infinite cardinal $\mathfrak{c}$, there exists a closure operation* Cl *such that the cardinal of the family of subsets which are of infinite but not of sequentially infinite height equals* $2^{\mathfrak{c}}$.

Proof. We divide the given set S into three disjoint subsets S_1, S_2, S_3 such that S_3 is denumerable and S_1 and S_2 satisfy condition (12). Denote the elements of S_3 by $y_i, i = 1, 2, \ldots$. Let φ be a bijective mapping from S_1 onto S_2 and R the set defined by (13). We define the closure operation Cl first for subsets X of the set $S_1 \cup S_2$ as follows:

$$(16) \qquad \mathrm{Cl}(X) = \begin{cases} S_1 \cup S_2 \text{ if } x_1, x_2 \in X \text{ such that } (x_1, x_2) \in R \\ X, \text{ otherwise.} \end{cases}$$

Let $X \subset S$ be arbitrary. Then it possesses a unique decomposition $X = Z \cup Y$ where $Z \subset S_1 \cup S_2$ and $Y \subset S_3$. We define

$$(17) \qquad \mathrm{Cl}(X) = \mathrm{Cl}(Z) \cup \{y_i \mid i \geqq \min_j (y_j \in Y)\}.$$

The equations (16) and (17) constitute a definition of a closure operation Cl such that S possesses $2^{\mathfrak{c}}$ subsets which are of infinite but not of sequentially infinite height. For if $X \subset S_1$ is arbitrary then the set (14) satisfies these requirements. Thus, theorem 6 follows.

We shall finally consider the lower bound for the number of subsets of given height included in a given basic set S. If we define $\mathrm{Cl}(X) = S$, for any non-empty $X \subset S$, then the only set precomplete in S is the empty set and there are no subsets of height > 1. The definition (15) shows that it is not necessary for an infinite set to possess a precomplete subset. Finally, it is easy to prove that a finite set always possesses at least one (possibly empty) precomplete subset. Hence, the best-possible lower bound equals 0 or 1 where the latter value occurs if and only if we are considering precomplete subsets of a finite set.

3. In this section, we shall consider the heights of closed sets of functions in finite algebras (i.e., closed subsets of $\mathfrak{P}_n$) where closure means closure with respect to composition. Because the lattice of closed sets of functions in the algebra of logic (i.e., the lattice of closed subsets of $\mathfrak{P}_2$) is known, cf.

[8, p. 101], it is easy to determine the number of sets of any given height. Thus, there are exactly 28 sets which are of infinite but not of sequentially infinite height. (As we noticed in section 1, there are no sets of sequentially infinite height in the algebra of logic.) The number of sets of any given height is seen from the following table:

Height	0	1	2	3	4	5	6	$\geqq 7$
Number of sets	1	5	11	13	11	12	9	8

We shall now consider subsets of $\mathfrak{P}_n$ where $n \geqq 3$. As we pointed out in the introduction, very little is known about the corresponding lattice. The following results have been presented in the literature. Each $\mathfrak{P}_n$ possesses only a finite number of precomplete subsets, and for $\mathfrak{P}_3$ this number equals 18. (Cf. [4, pp. 80, 109].) Each $\mathfrak{P}_n$ (where $n \geqq 3$) possesses a continuum of closed subsets. (Cf. [5].) The number of subsets of height 2 in $\mathfrak{P}_3$ is finite. (This result follows because it is shown in [3] that every set precomplete in $\mathfrak{P}_3$ is finitely generated. In general, if in $\mathfrak{P}_n$ there is only a finite number of subsets of height l and each of them is finitely generated then there is only a finite number of subsets of height $l + 1$.) We shall now prove that in each $\mathfrak{P}_n$ the number of subsets, which are either of finite height or of infinite but not of sequentially infinite height, is at most denumerable. We shall first establish the following

Theorem 7. *All sets $M \subset \mathfrak{P}_n$ possess at most denumerably many precomplete subsets.*

Proof. For a given (closed) set $M \subset \mathfrak{P}_n$, we denote by M_k, $k = 1, 2, \ldots$, the set of all k-place functions included in M. Let M'_k be an arbitrary proper subset of M_k. We now claim that, for any k and M'_k, there is at most one set E precomplete in M such that

$$E \cap M_k = M'_k \,. \tag{18}$$

To prove this, we consider the subset $G(M'_k)$ of M consisting of all elements f satisfying the following condition:

$$\mathrm{Cl}\,(M'_k \cup \{f\}) \cap M_k = M'_k \,. \tag{19}$$

It is easy to see that the set $G(M'_k)$ (which may be empty) is closed. Furthermore,

$$G\,(M'_k) \neq M \tag{20}$$

because no element of the non-empty set $M_k - M'_k$ belongs to $G(M'_k)$. Let now E be an arbitrary closed set satisfying condition (18). By the definition of the set $G(M'_k)$,

$$E \subset G(M'_k) \,. \tag{21}$$

If E is precomplete in M then, by (20), the inclusion (21) cannot be proper. Hence, if there is a set E precomplete in M and satisfying (18) then necessarily $E = G(M'_k)$.

On the other hand, for any set E precomplete in M, there is a k such that condition (18) holds, for some proper subset M'_k of M_k. To find such a k, it suffices to choose a function

$$f(x_1, \dots, x_k) \in M - E .$$

Hence, the cardinal of the family of the sets precomplete in M cannot exceed the cardinal of the family of the sets M'_k. Since the sets M_k, $k = 1, 2, \dots,$ are finite we have completed the proof of theorem 7.

Remark. It is seen in theorem 5 that, in the general case, a denumerable set may possess a continuum of precomplete subsets. As shown above, this may not happen in connection with finite algebras. The proof is based essentially on the fact that the set of elements satisfying condition (19) is closed. In general, consider an arbitrary denumerable set M and a closure operation Cl for M such that

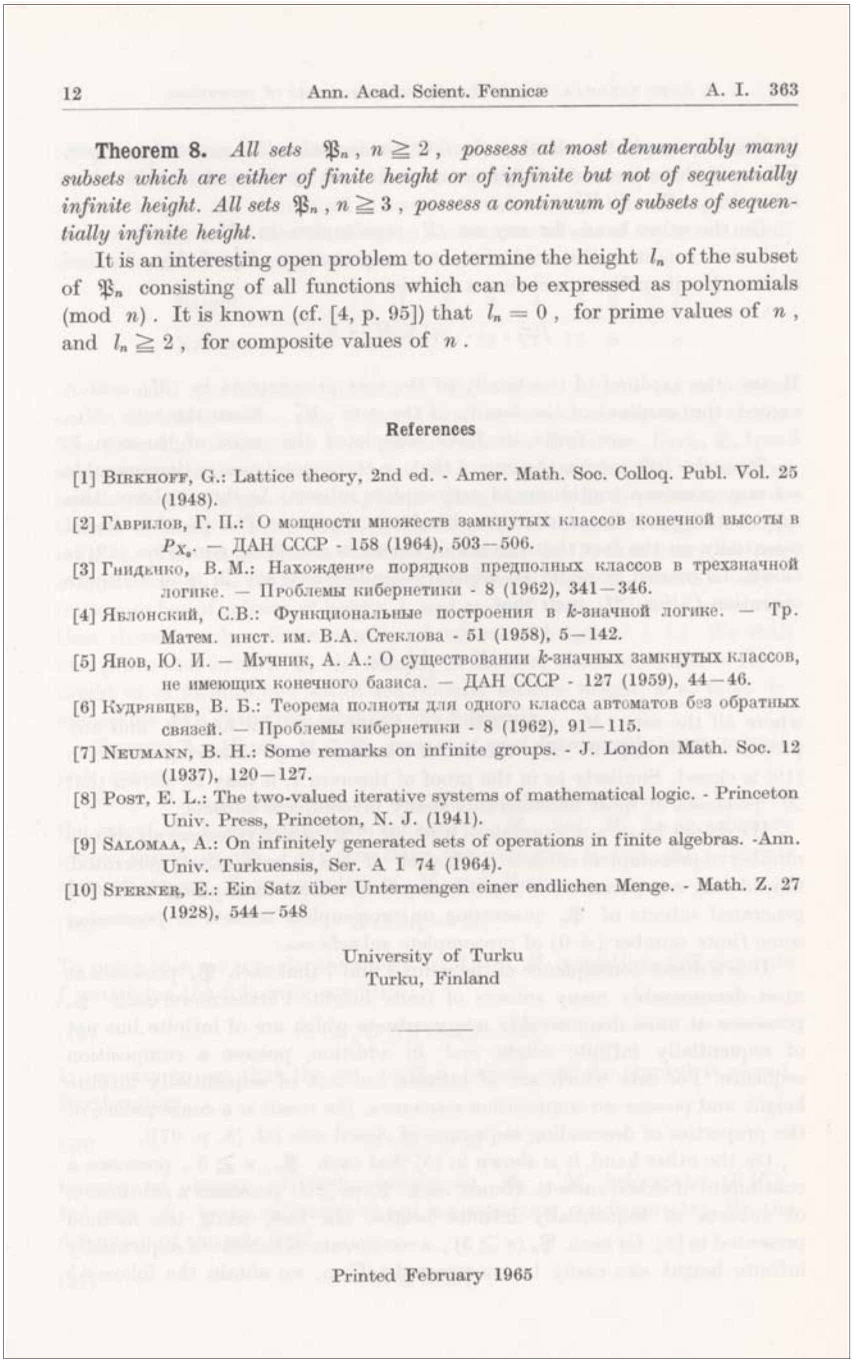
$$M = \bigcup_{k=1}^{\infty} M_k$$

where all the sets M_k are finite and, furthermore, for any k and any proper subset M'_k of M_k, the set of all elements f satisfying condition (19) is closed. Similarly as in the proof of theorem 7, it may be shown that M possesses at most denumerably many precomplete subsets.

We do not know any example of a set $M \subset \mathfrak{P}_n$ which possesses an infinite number of precomplete subsets. Such a set M has to be infinitely generated. Considering sets presented in [9], it is easy to construct examples of infinitely generated subsets of $\mathfrak{P}_n$ possessing no precomplete subsets or possessing some finite number ($\neq 0$) of precomplete subsets.

It is a direct consequence of theorems 1 and 7 that each $\mathfrak{P}_n$ possesses at most denumerably many subsets of finite height. Furthermore, each $\mathfrak{P}_n$ possesses at most denumerably many subsets which are of infinite but not of sequentially infinite height and, in addition, possess a composition sequence. For sets which are of infinite but not of sequentially infinite height and possess no composition sequences, the result is a consequence of the properties of descending sequences of closed sets (cf. [8, p. 97]).

On the other hand, it is shown in [5] that each $\mathfrak{P}_n$, $n \geqq 3$, possesses a continuum of closed subsets. Hence, each $\mathfrak{P}_n$ ($n \geqq 3$) possesses a continuum of subsets of sequentially infinite height. (In fact, using the method presented in [5], for each $\mathfrak{P}_n$ ($n \geqq 3$), a continuum of subsets of sequentially infinite height can easily be constructed.) Thus, we obtain the following



Theorem 8. *All sets $\mathfrak{P}_n$, $n \geqq 2$, possess at most denumerably many subsets which are either of finite height or of infinite but not of sequentially infinite height. All sets $\mathfrak{P}_n$, $n \geqq 3$, possess a continuum of subsets of sequentially infinite height.*

It is an interesting open problem to determine the height l_n of the subset of $\mathfrak{P}_n$ consisting of all functions which can be expressed as polynomials (mod n). It is known (cf. [4, p. 95]) that $l_n = 0$, for prime values of n, and $l_n \geqq 2$, for composite values of n.

References

[1] Birkhoff, G.: Lattice theory, 2nd ed. - Amer. Math. Soc. Colloq. Publ. Vol. 25 (1948).

[2] Гаврилов, Г. П.: О мощности множеств замкнутых классов конечной высоты в P_{X_0}. — ДАН СССР - 158 (1964), 503—506.

[3] Гниденко, В. М.: Нахождение порядков предполных классов в трехзначной логике. — Проблемы кибернетики - 8 (1962), 341—346.

[4] Яблонский, С.В.: Функциональные построения в k-значной логике. — Тр. Матем. инст. им. В.А. Стеклова - 51 (1958), 5—142.

[5] Янов, Ю. И. — Мучник, А. А.: О существовании k-значных замкнутых классов, не имеющих конечного базиса. — ДАН СССР - 127 (1959), 44—46.

[6] Кудрявцев, В. Б.: Теорема полноты для одного класса автоматов без обратных связей. — Проблемы кибернетики - 8 (1962), 91—115.

[7] Neumann, B. H.: Some remarks on infinite groups. - J. London Math. Soc. 12 (1937), 120—127.

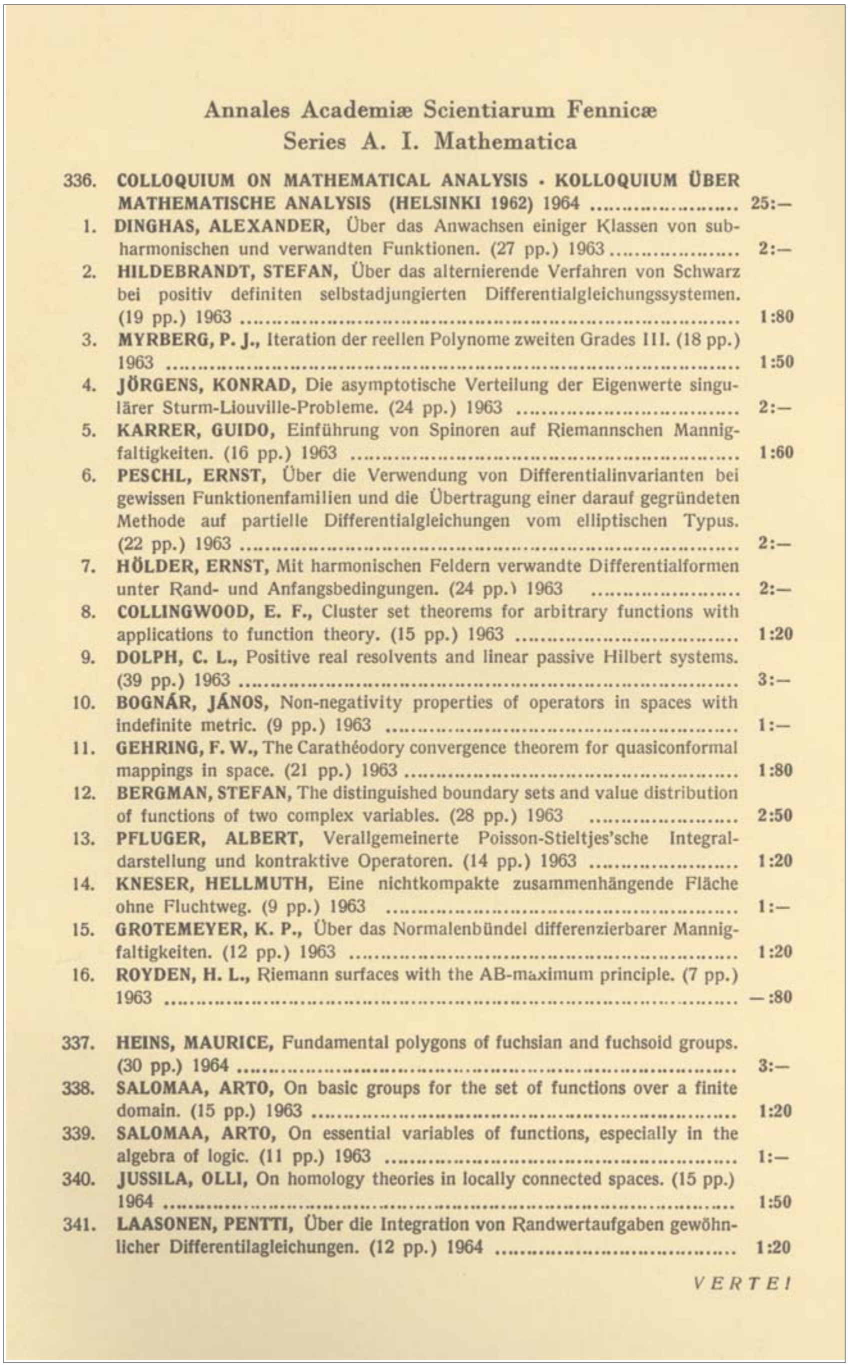
[8] Post, E. L.: The two-valued iterative systems of mathematical logic. - Princeton Univ. Press, Princeton, N. J. (1941).

[9] Salomaa, A.: On infinitely generated sets of operations in finite algebras. -Ann. Univ. Turkuensis, Ser. A I 74 (1964).

[10] Sperner, E.: Ein Satz über Untermengen einer endlichen Menge. - Math. Z. 27 (1928), 544—548

University of Turku
Turku, Finland

Printed February 1965



Annales Academiæ Scientiarum Fennicæ
Series A. I. Mathematica

336. **COLLOQUIUM ON MATHEMATICAL ANALYSIS · KOLLOQUIUM ÜBER MATHEMATISCHE ANALYSIS (HELSINKI 1962) 1964** .... 25:—

1. **DINGHAS, ALEXANDER,** Über das Anwachsen einiger Klassen von subharmonischen und verwandten Funktionen. (27 pp.) 1963 .... 2:—

2. **HILDEBRANDT, STEFAN,** Über das alternierende Verfahren von Schwarz bei positiv definiten selbstadjungierten Differentialgleichungssystemen. (19 pp.) 1963 .... 1:80

3. **MYRBERG, P. J.,** Iteration der reellen Polynome zweiten Grades III. (18 pp.) 1963 .... 1:50

4. **JÖRGENS, KONRAD,** Die asymptotische Verteilung der Eigenwerte singulärer Sturm-Liouville-Probleme. (24 pp.) 1963 .... 2:—

5. **KARRER, GUIDO,** Einführung von Spinoren auf Riemannschen Mannigfaltigkeiten. (16 pp.) 1963 .... 1:60

6. **PESCHL, ERNST,** Über die Verwendung von Differentialinvarianten bei gewissen Funktionenfamilien und die Übertragung einer darauf gegründeten Methode auf partielle Differentialgleichungen vom elliptischen Typus. (22 pp.) 1963 .... 2:—

7. **HÖLDER, ERNST,** Mit harmonischen Feldern verwandte Differentialformen unter Rand- und Anfangsbedingungen. (24 pp.) 1963 .... 2:—

8. **COLLINGWOOD, E. F.,** Cluster set theorems for arbitrary functions with applications to function theory. (15 pp.) 1963 .... 1:20

9. **DOLPH, C. L.,** Positive real resolvents and linear passive Hilbert systems. (39 pp.) 1963 .... 3:—

10. **BOGNÁR, JÁNOS,** Non-negativity properties of operators in spaces with indefinite metric. (9 pp.) 1963 .... 1:—

11. **GEHRING, F. W.,** The Carathéodory convergence theorem for quasiconformal mappings in space. (21 pp.) 1963 .... 1:80

12. **BERGMAN, STEFAN,** The distinguished boundary sets and value distribution of functions of two complex variables. (28 pp.) 1963 .... 2:50

13. **PFLUGER, ALBERT,** Verallgemeinerte Poisson-Stieltjes'sche Integraldarstellung und kontraktive Operatoren. (14 pp.) 1963 .... 1:20

14. **KNESER, HELLMUTH,** Eine nichtkompakte zusammenhängende Fläche ohne Fluchtweg. (9 pp.) 1963 .... 1:—

15. **GROTEMEYER, K. P.,** Über das Normalenbündel differenzierbarer Mannigfaltigkeiten. (12 pp.) 1963 .... 1:20

16. **ROYDEN, H. L.,** Riemann surfaces with the AB-maximum principle. (7 pp.) 1963 .... —:80

337. **HEINS, MAURICE,** Fundamental polygons of fuchsian and fuchsoid groups. (30 pp.) 1964 .... 3:—

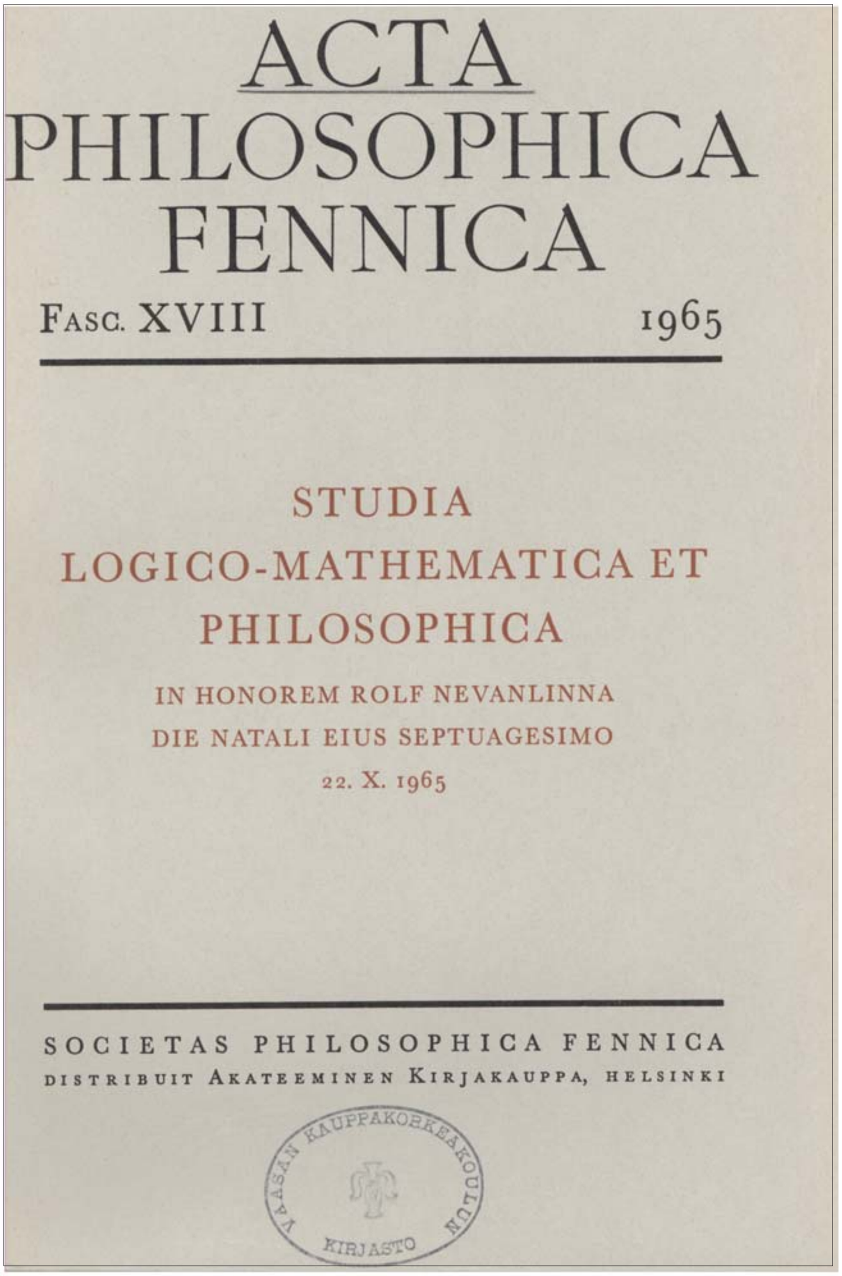
338. **SALOMAA, ARTO,** On basic groups for the set of functions over a finite domain. (15 pp.) 1963 .... 1:20

339. **SALOMAA, ARTO,** On essential variables of functions, especially in the algebra of logic. (11 pp.) 1963 .... 1:—

340. **JUSSILA, OLLI,** On homology theories in locally connected spaces. (15 pp.) 1964 .... 1:50

341. **LAASONEN, PENTTI,** Über die Integration von Randwertaufgaben gewöhnlicher Differentilagleichungen. (12 pp.) 1964 .... 1:20

VERTE!



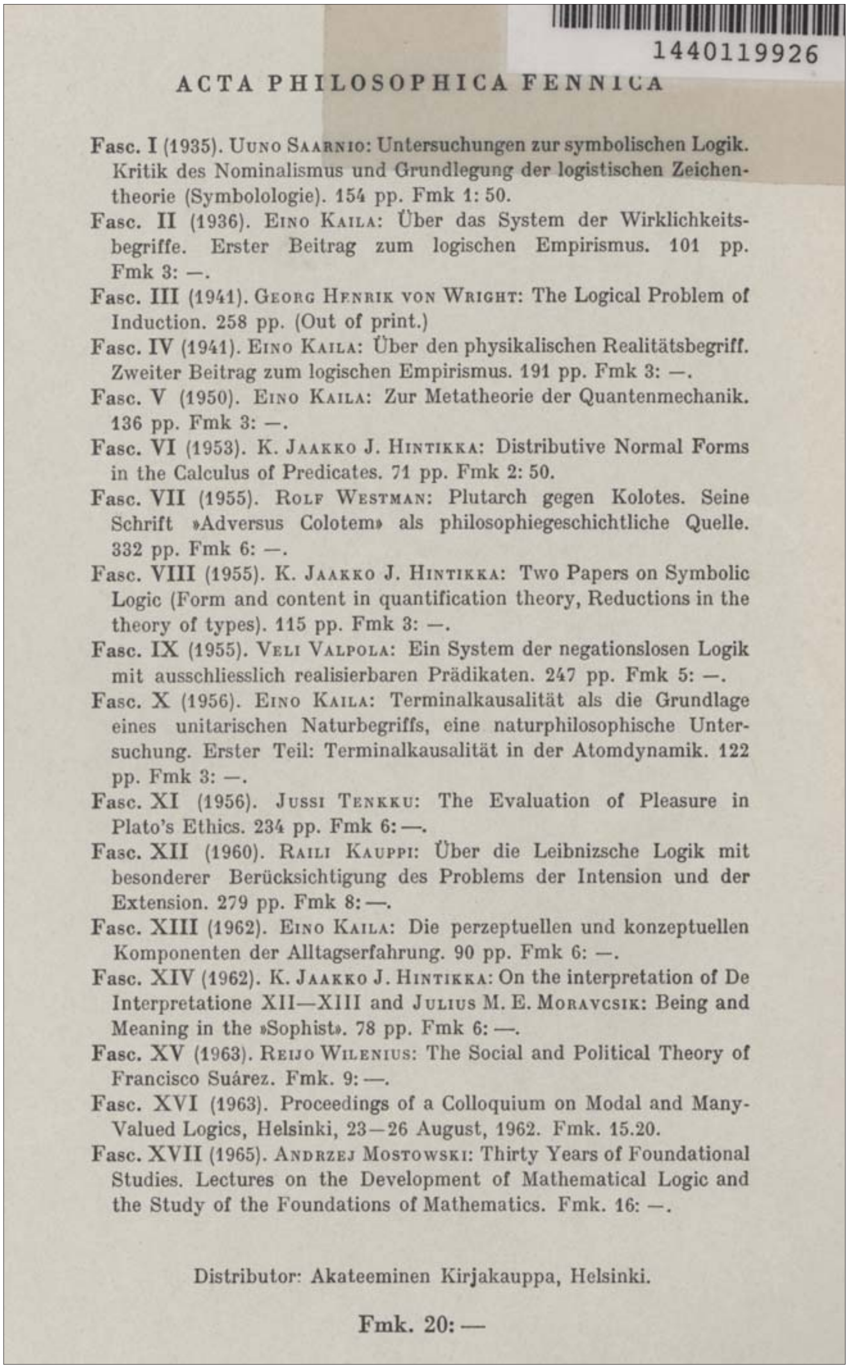
ACTA PHILOSOPHICA FENNICA

FASC. XVIII 1965

STUDIA LOGICO-MATHEMATICA ET PHILOSOPHICA

IN HONOREM ROLF NEVANLINNA
DIE NATALI EIUS SEPTUAGESIMO
22. X. 1965

SOCIETAS PHILOSOPHICA FENNICA
DISTRIBUIT AKATEEMINEN KIRJAKAUPPA, HELSINKI



ACTA PHILOSOPHICA FENNICA

Fasc. I (1935). Uuno Saarnio: Untersuchungen zur symbolischen Logik. Kritik des Nominalismus und Grundlegung der logistischen Zeichentheorie (Symbolologie). 154 pp. Fmk 1: 50.

Fasc. II (1936). Eino Kaila: Über das System der Wirklichkeitsbegriffe. Erster Beitrag zum logischen Empirismus. 101 pp. Fmk 3: —.

Fasc. III (1941). Georg Henrik von Wright: The Logical Problem of Induction. 258 pp. (Out of print.)

Fasc. IV (1941). Eino Kaila: Über den physikalischen Realitätsbegriff. Zweiter Beitrag zum logischen Empirismus. 191 pp. Fmk 3: —.

Fasc. V (1950). Eino Kaila: Zur Metatheorie der Quantenmechanik. 136 pp. Fmk 3: —.

Fasc. VI (1953). K. Jaakko J. Hintikka: Distributive Normal Forms in the Calculus of Predicates. 71 pp. Fmk 2: 50.

Fasc. VII (1955). Rolf Westman: Plutarch gegen Kolotes. Seine Schrift »Adversus Colotem» als philosophiegeschichtliche Quelle. 332 pp. Fmk 6: —.

Fasc. VIII (1955). K. Jaakko J. Hintikka: Two Papers on Symbolic Logic (Form and content in quantification theory, Reductions in the theory of types). 115 pp. Fmk 3: —.

Fasc. IX (1955). Veli Valpola: Ein System der negationslosen Logik mit ausschliesslich realisierbaren Prädikaten. 247 pp. Fmk 5: —.

Fasc. X (1956). Eino Kaila: Terminalkausalität als die Grundlage eines unitarischen Naturbegriffs, eine naturphilosophische Untersuchung. Erster Teil: Terminalkausalität in der Atomdynamik. 122 pp. Fmk 3: —.

Fasc. XI (1956). Jussi Tenkku: The Evaluation of Pleasure in Plato's Ethics. 234 pp. Fmk 6: —.

Fasc. XII (1960). Raili Kauppi: Über die Leibnizsche Logik mit besonderer Berücksichtigung des Problems der Intension und der Extension. 279 pp. Fmk 8: —.

Fasc. XIII (1962). Eino Kaila: Die perzeptuellen und konzeptuellen Komponenten der Alltagserfahrung. 90 pp. Fmk 6: —.

Fasc. XIV (1962). K. Jaakko J. Hintikka: On the interpretation of De Interpretatione XII—XIII and Julius M. E. Moravcsik: Being and Meaning in the »Sophist». 78 pp. Fmk 6: —.

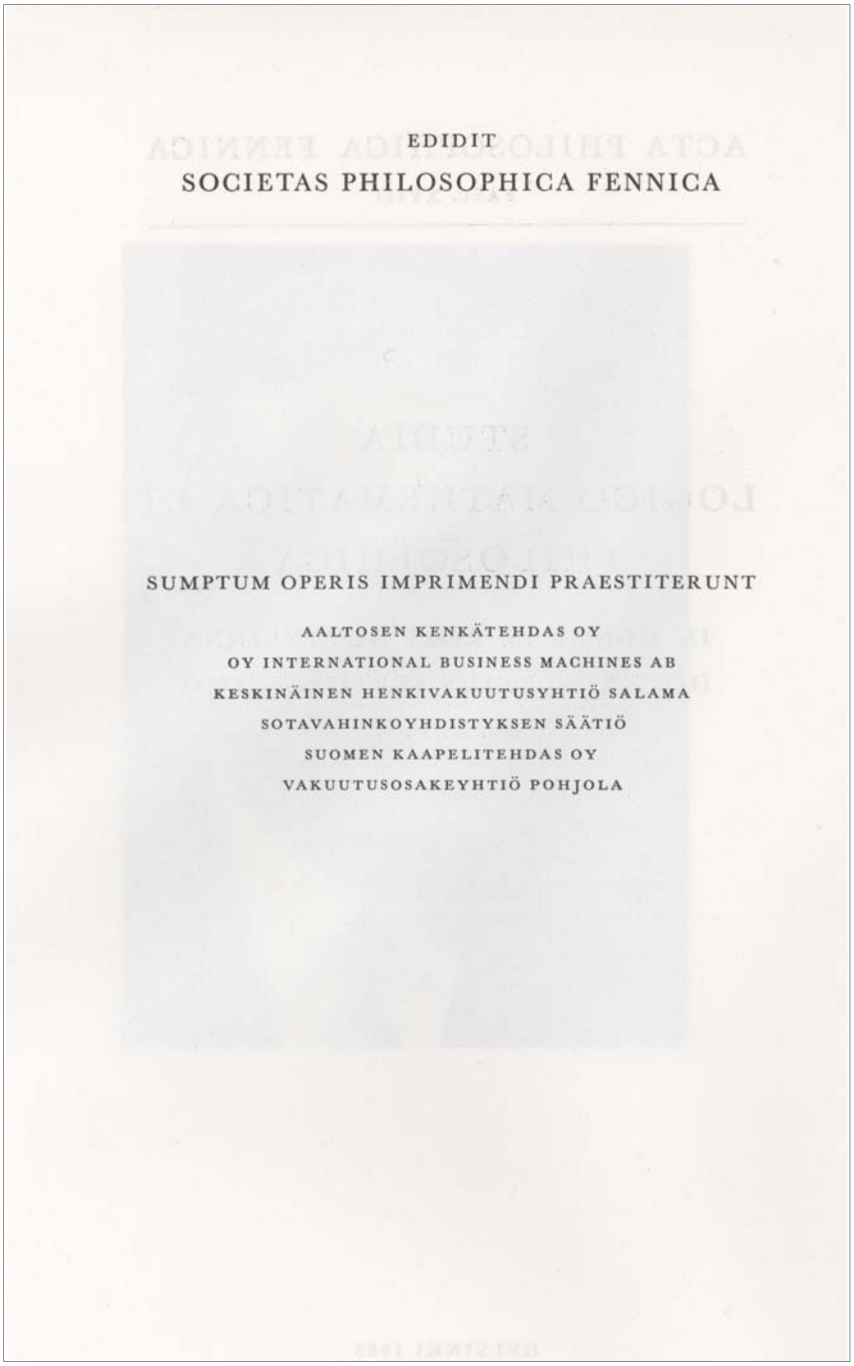
Fasc. XV (1963). Reijo Wilenius: The Social and Political Theory of Francisco Suárez. Fmk. 9: —.

Fasc. XVI (1963). Proceedings of a Colloquium on Modal and Many-Valued Logics, Helsinki, 23—26 August, 1962. Fmk. 15.20.

Fasc. XVII (1965). Andrzej Mostowski: Thirty Years of Foundational Studies. Lectures on the Development of Mathematical Logic and the Study of the Foundations of Mathematics. Fmk. 16: —.

Distributor: Akateeminen Kirjakauppa, Helsinki.

Fmk. 20: —

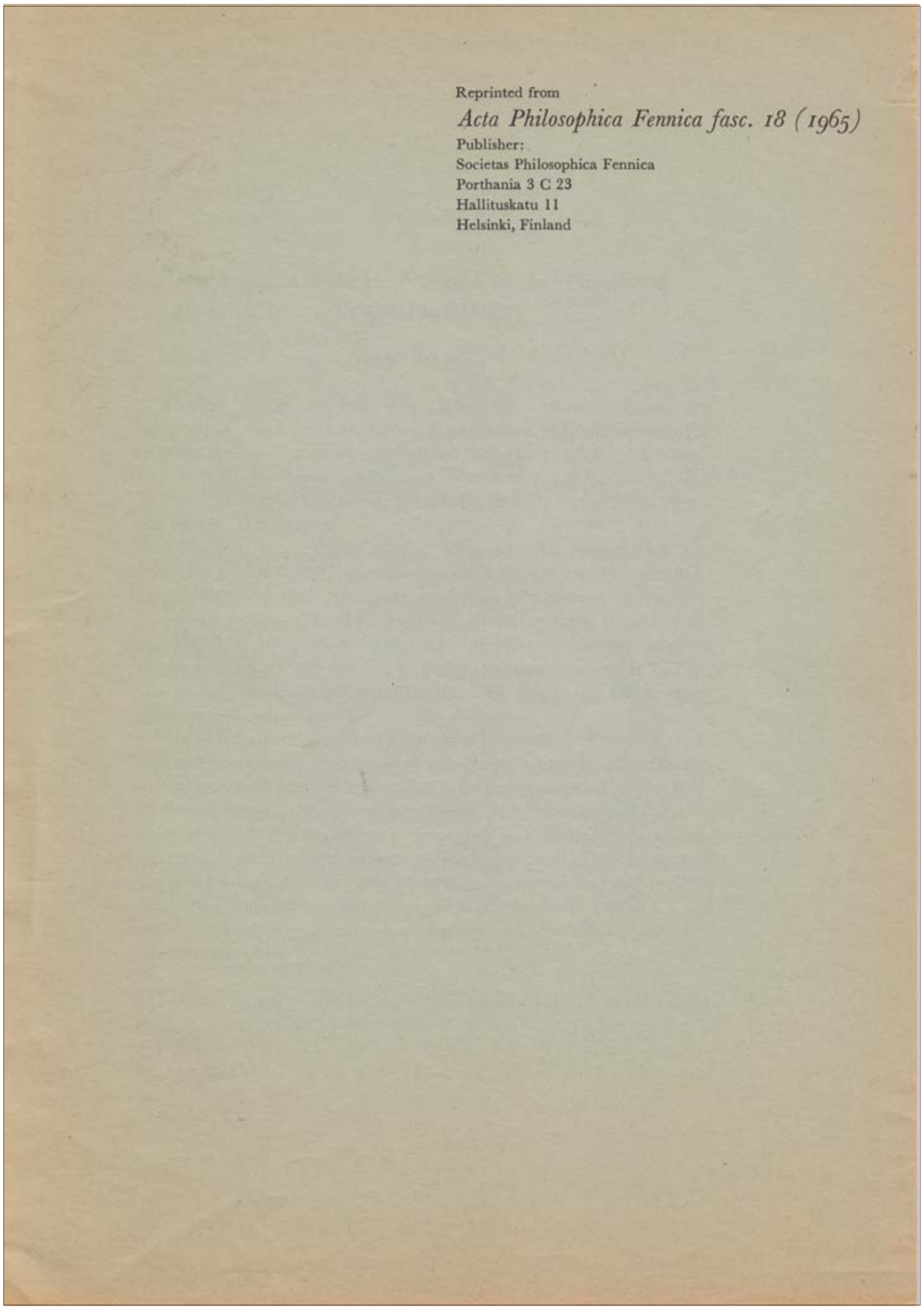


EDIDIT

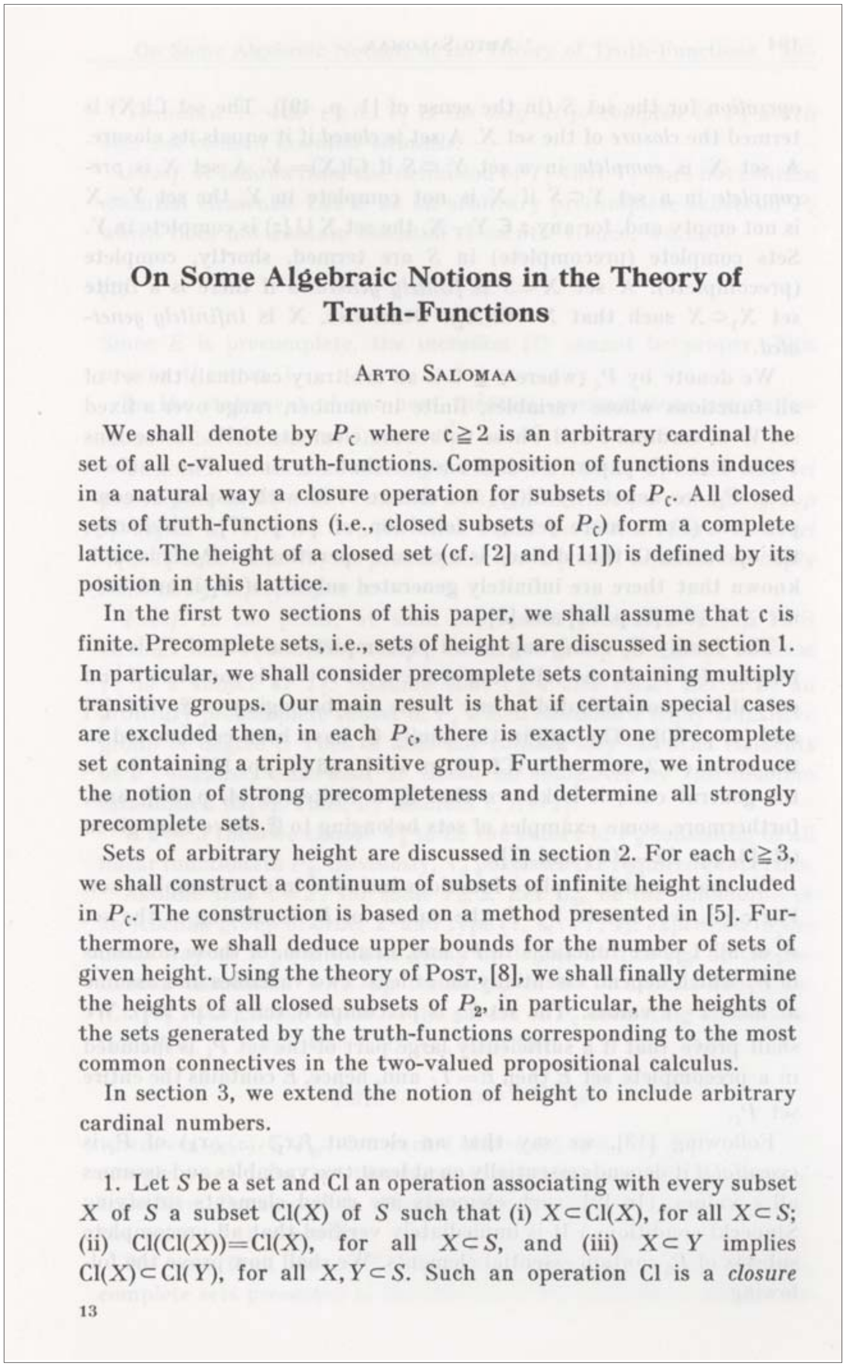
SOCIETAS PHILOSOPHICA FENNICA

SUMPTUM OPERIS IMPRIMENDI PRAESTITERUNT

AALTOSEN KENKÄTEHDAS OY
OY INTERNATIONAL BUSINESS MACHINES AB
KESKINÄINEN HENKIVAKUUTUSYHTIÖ SALAMA
SOTAVAHINKOYHDISTYKSEN SÄÄTIÖ
SUOMEN KAAPELITEHDAS OY
VAKUUTUSOSAKEYHTIÖ POHJOLA



Reprinted from
Acta Philosophica Fennica fasc. 18 (1965)
Publisher:
Societas Philosophica Fennica
Porthania 3 C 23
Hallituskatu 11
Helsinki, Finland



On Some Algebraic Notions in the Theory of Truth-Functions

ARTO SALOMAA

We shall denote by $P_{\mathfrak{c}}$ where $\mathfrak{c} \geqq 2$ is an arbitrary cardinal the set of all $\mathfrak{c}$-valued truth-functions. Composition of functions induces in a natural way a closure operation for subsets of $P_{\mathfrak{c}}$. All closed sets of truth-functions (i.e., closed subsets of $P_{\mathfrak{c}}$) form a complete lattice. The height of a closed set (cf. [2] and [11]) is defined by its position in this lattice.

In the first two sections of this paper, we shall assume that $\mathfrak{c}$ is finite. Precomplete sets, i.e., sets of height 1 are discussed in section 1. In particular, we shall consider precomplete sets containing multiply transitive groups. Our main result is that if certain special cases are excluded then, in each $P_{\mathfrak{c}}$, there is exactly one precomplete set containing a triply transitive group. Furthermore, we introduce the notion of strong precompleteness and determine all strongly precomplete sets.

Sets of arbitrary height are discussed in section 2. For each $\mathfrak{c} \geqq 3$, we shall construct a continuum of subsets of infinite height included in $P_{\mathfrak{c}}$. The construction is based on a method presented in [5]. Furthermore, we shall deduce upper bounds for the number of sets of given height. Using the theory of POST, [8], we shall finally determine the heights of all closed subsets of P_2, in particular, the heights of the sets generated by the truth-functions corresponding to the most common connectives in the two-valued propositional calculus.

In section 3, we extend the notion of height to include arbitrary cardinal numbers.

1. Let S be a set and Cl an operation associating with every subset X of S a subset $\mathrm{Cl}(X)$ of S such that (i) $X \subset \mathrm{Cl}(X)$, for all $X \subset S$; (ii) $\mathrm{Cl}(\mathrm{Cl}(X)) = \mathrm{Cl}(X)$, for all $X \subset S$, and (iii) $X \subset Y$ implies $\mathrm{Cl}(X) \subset \mathrm{Cl}(Y)$, for all $X, Y \subset S$. Such an operation Cl is a *closure*

operation for the set S (in the sense of [1, p. 49]). The set $\mathrm{Cl}(X)$ is termed the *closure* of the set X. A set is *closed* if it equals its closure. A set X is *complete* in a set $Y \subset S$ if $\mathrm{Cl}(X) = Y$. A set X is *precomplete* in a set $Y \subset S$ if X is not complete in Y, the set $Y-X$ is not empty and, for any $z \in Y-X$, the set $X \cup \{z\}$ is complete in Y. Sets complete (precomplete) in S are termed, shortly, complete (precomplete). A set $X \subset S$ is *finitely generated* if there is a finite set $X_1 \subset X$ such that $X \subset \mathrm{Cl}(X_1)$. Otherwise, X is *infinitely generated*.

We denote by $P_\mathfrak{c}$ (where $\mathfrak{c} \geqq 2$ is an arbitrary cardinal) the set of all functions whose variables, finite in number, range over a fixed set W of cardinal $\mathfrak{c}$ and whose values are elements of W. In sections 1 and 2 of this paper, we shall assume that $\mathfrak{c}$ is finite. For a subset X of $P_\mathfrak{c}$, we denote by $\mathrm{Cl}(X)$ the closure of X with respect to composition. (For a more detailed definition, cf. [4, p. 57].) Obviously, the operation Cl thus defined is a closure operation for $P_\mathfrak{c}$. It is well-known that there are infinitely generated subsets of $P_\mathfrak{c}$ if and only if $\mathfrak{c} \geqq 3$. (Cf. [8, p. 94] and [5].)

The family $\mathfrak{E}_\mathfrak{c}$ consisting of all precomplete subsets of $P_\mathfrak{c}$ is criterional for $P_\mathfrak{c}$ in the following sense: a set $X \subset P_\mathfrak{c}$ is complete if and only if it is not included in any of the sets belonging to $\mathfrak{E}_\mathfrak{c}$. (Cf. [6] and [4, p. 80].) The sets in the family $\mathfrak{E}_\mathfrak{c}$ have been constructed in the cases $\mathfrak{c}=2$ and $\mathfrak{c}=3$. (Cf. [8, p. 105] and [4, pp. 109–113].) In the general case, it is known that $\mathfrak{E}_\mathfrak{c}$ is finite (cf. [4, p. 80]) and, furthermore, some examples of sets belonging to $\mathfrak{E}_\mathfrak{c}$ have been given (cf. [4, pp. 82–109] and [7]).

We shall consider 1-place functions included in a precomplete set. For $\mathfrak{c} \geqq 3$, we denote by $T_\mathfrak{c}$ the subset of $P_\mathfrak{c}$ consisting of the set $P^1_\mathfrak{c}$ of all 1-place functions in $P_\mathfrak{c}$ and, in addition, of those functions in $P_\mathfrak{c}$ which depend essentially on at least two variables and assume at most $\mathfrak{c}-1$ values. The set $T_\mathfrak{c}$ is precomplete (cf. [4, p. 90]). We shall prove that if a sufficiently large part of the set $P^1_\mathfrak{c}$ is included in a precomplete set E then $E = T_\mathfrak{c}$ and, hence, E contains the entire set $P^1_\mathfrak{c}$.

Following [13], we say that an element $f(x_1, \ldots, x_k)$ of $P_\mathfrak{c}$ is *essential* if it depends essentially on at least two variables and assumes all $\mathfrak{c}$ values. (In [9], such elements are called elements satisfying Słupecki conditions.) It is immediately verified that all precomplete subsets of P_2 contain essential elements. We shall now prove the following

Theorem 1. *For $\mathfrak{c} \geqq 3$, $T_{\mathfrak{c}}$ is the only set precomplete in $P_{\mathfrak{c}}$ which does not contain essential elements.*

Proof. It follows from the definition of $T_{\mathfrak{c}}$ that $T_{\mathfrak{c}}$ does not contain essential elements. Let E be an arbitrary precomplete subset of $P_{\mathfrak{c}}$ which does not contain essential elements. Hence, we have

$$E \subset T_{\mathfrak{c}}. \tag{1}$$

Since E is precomplete, the inclusion (1) cannot be proper. This proves theorem 1.

In the statement of our next theorem, permutations are understood to be elements of the set $\overset{1}{P}_{\mathfrak{c}}$.

Theorem 2. *Assume that $\mathfrak{c} \geqq 4$ and $\mathfrak{c} \neq 2^r$. Then $T_{\mathfrak{c}}$ is the only set precomplete in $P_{\mathfrak{c}}$ which contains a triply transitive permutation group of degree $\mathfrak{c}$. If $\mathfrak{c}=3$ or, for some $r \geqq 2$, $\mathfrak{c}=2^r$ then there is a set $V_{\mathfrak{c}} \neq T_{\mathfrak{c}}$ such that $V_{\mathfrak{c}}$ is precomplete in $P_{\mathfrak{c}}$ and contains a triply transitive group of degree $\mathfrak{c}$.*

Proof. In the proof, we shall use results presented in [9]. It is obvious that $T_{\mathfrak{c}}$ contains a triply transitive group of degree $\mathfrak{c}$ because $\overset{1}{P}_{\mathfrak{c}}$ is a subset of $T_{\mathfrak{c}}$. Assume that $\mathfrak{c} \geqq 4$ and $\mathfrak{c} \neq 2^r$. Let E be an arbitrary precomplete subset of $P_{\mathfrak{c}}$ which contains a triply transitive group of degree $\mathfrak{c}$. Then E does not contain any essential elements of $P_{\mathfrak{c}}$ because, otherwise, E would be complete, by the theorem established in [9]. Thus, by theorem 1, $E = T_{\mathfrak{c}}$.

If $\mathfrak{c} = 3$ then we choose V_3 to be the subset of P_3 consisting of all linear functions in P_3. Obviously, V_3 possesses the required properties.

Assume that $\mathfrak{c}=2^r$, for some $r \geqq 2$. Let G_{2r} be the holomorph of an Abelian group of order 2^r and type $(1, 1, \ldots, 1)$, expressed in the usual way as a permutation group of degree 2^r. Let F_{2r} be the extension associated with G_{2r} consisting of $2^{r(r+1)}$ 1-place functions. (Cf. [9].) We choose $V_{\mathfrak{c}}$ to be the subset of $P_{\mathfrak{c}}$ consisting of all functions $f(x_1, \ldots, x_k)$, $k = 1, 2, \ldots$, such that

$$f(g_1(x), \ldots, g_k(x)) \in F_{2r}$$

whenever $g_i(x) \in F_{2r}$, for each i where $1 \leqq i \leqq k$. By [9], $V_{\mathfrak{c}}$ is precomplete in $P_{\mathfrak{c}}$. On the other hand, it is well-known that G_{2r} is triply transitive. Because it is obvious that $V_{\mathfrak{c}} \neq T_{\mathfrak{c}}$ we have completed the proof of theorem 2.

We note that, for $\mathfrak{c}=2^r$, the sets $V_{\mathfrak{c}}$ are different from the precomplete sets presented in the literature. We shall now consider the set V_4 in detail. We denote by F_4 the subset of P_4^1 consisting of all permutations of the elements 1, 2, 3, 4 and, in addition, of all functions which assume some value twice and another (not necessarily distinct) value twice. (F_4 consists of 64 elements.) Then V_4 is the subset of P_4 consisting of all functions $f(x_1, \dots, x_k)$, $k=1, 2, \dots$, such that

$$f(g_1(x), \dots, g_k(x)) \in F_4$$

whenever $g_i(x) \in F_4$, for each i where $1 \leqq i \leqq k$. The following function $f(x, y)$ is an example of an essential element in the set V_4:

x y	1	2	3	4
1	2	2	3	3
2	3	3	2	2
3	1	1	4	4
4	4	4	1	1

It can be shown that, in the cases $\mathfrak{c}=3$ and $\mathfrak{c}=4$, $T_{\mathfrak{c}}$ and $V_{\mathfrak{c}}$ are the only sets precomplete in $P_{\mathfrak{c}}$ which contain a triply transitive group of degree $\mathfrak{c}$.

We denote by $\overset{1}{H}_{\mathfrak{c}}$ the subset of $\overset{1}{P}_{\mathfrak{c}}$ consisting of all permutations and of all functions assuming at most $\mathfrak{c}$-2 values. The symbol $\overset{2}{H}_{\mathfrak{c}}$ denotes any subset of $\overset{1}{P}_{\mathfrak{c}}$ consisting of a maximal subgroup of the symmetric group $S_{\mathfrak{c}}$ and, in addition, of all functions assuming at most $\mathfrak{c}$-1 values. Furthermore, by the *k-restriction* ($k = 1, 2, \dots$) of a set $X \subset P_{\mathfrak{c}}$, in symbols, $\mathrm{Re}_k(X)$ we mean the set of all k-place functions included in X. A subset X of $P_{\mathfrak{c}}$ is termed *strongly precomplete* if, for every k, the set $\mathrm{Cl}(\mathrm{Re}_k(X))$ is precomplete in the set $\mathrm{Cl}(\mathrm{Re}_k(P_{\mathfrak{c}}))$. It is obvious that every strongly precomplete set is precomplete and, furthermore, generated by the 2-place functions included in it.

We shall now determine all strongly precomplete sets. We shall first establish the following

THEOREM 3. *The sets $\overset{1}{H}_{\mathfrak{c}}$ and $\overset{2}{H}_{\mathfrak{c}}$ are the only sets precomplete in $\overset{1}{P}_{\mathfrak{c}}$.*

Proof. It is easily verified that the sets $\overset{1}{H}_{\mathfrak{c}}$ and $\overset{2}{H}_{\mathfrak{c}}$ are precomplete in $\overset{1}{P}_{\mathfrak{c}}$. If $E \subset \overset{1}{P}_{\mathfrak{c}}$ is an arbitrary set which is not complete in $\overset{1}{P}_{\mathfrak{c}}$ then either

$$E \subset \overset{1}{H}_{\mathfrak{c}} \tag{2}$$

or

(3) $$E \subset \overset{2}{H}_\mathfrak{c},$$

for some set $\overset{2}{H}_\mathfrak{c}$. If, in addition, E is precomplete in $\overset{1}{P}_\mathfrak{c}$ then the corresponding inclusion (2) or (3) cannot be proper. Thus, theorem 3 follows.

Theorem 4. *For* $\mathfrak{c} \geqq 4$, $P_\mathfrak{c}$ *possesses no strongly precomplete subsets. The set of linear functions is the only strongly precomplete subset of* P_3. *The set of monotonous functions is the only strongly precomplete subset of* P_2.

Proof. Assume that $\mathfrak{c} \geqq 3$ and E is a strongly precomplete subset of $P_\mathfrak{c}$. Then necessarily $E \neq T_\mathfrak{c}$ because $\mathrm{Cl}(\mathrm{Re}_1(T_\mathfrak{c}))$ is complete in the set

(4) $$\overset{1}{P}_\mathfrak{c} = \mathrm{Cl}(\mathrm{Re}_1(P_\mathfrak{c})).$$

Hence, by theorem 1, E contains an essential element of $P_\mathfrak{c}$. By theorem 3,

(5) $$\mathrm{Re}_1(E) = \overset{1}{H}_\mathfrak{c}$$

or

(6) $$\mathrm{Re}_1(E) = \overset{2}{H}_\mathfrak{c},$$

for some set $\overset{2}{H}_\mathfrak{c}$. The equation (6) cannot hold true because, otherwise, E would be complete, by the completeness criterion presented in [4, p. 72]. On the other hand, if (5) holds true and $\mathfrak{c} \geqq 4$ then, by the "fundamental lemma" in [4, p. 69], E contains a 1-place function assuming exactly $\mathfrak{c}-1$ values and, hence, E is complete.

Thus, the only possibility is that $\mathfrak{c}=3$ and the equation (5) holds true. By checking through the precomplete subsets of P_3, it is seen that E equals the set of linear functions. Because the latter is generated by the 2-place functions included in it we conclude that E is strongly precomplete.

Assume, finally, that $\mathfrak{c}=2$. The set of monotonous functions and the set of self-dual functions are the only precomplete subsets E of P_2 such that $\mathrm{Cl}(\mathrm{Re}_1(E))$ is precomplete in the set (4) where $\mathfrak{c}=2$. However, only the former of these sets is generated by the 2-place functions included in it. This completes the proof of theorem 4.

It is an open problem whether or not there are infinitely generated precomplete subsets of $P_\mathfrak{c}$. This problem is closely linked with the problem of simplifying completeness criteria for subsets of $P_\mathfrak{c}$. (It is shown in [3] that there are no infinitely generated precomplete subsets of P_3. In [10], we have considered analogous problems for subsets of $P_{\mathfrak{c}}$.) It is easy to find examples of precomplete sets which can or cannot be generated by one element. Some sets of self-conjugate functions provide examples of the former type, and the set $T_{\mathfrak{c}}$ provides an example of the latter type.

2. Consider an arbitrary set S and a closure operation Cl for S. The *height* of a closed subset X of S is defined as follows. The height of S equals 0. The height of a closed set $X \neq S$ equals l ($l>0$) if, for all elements $z \in S-X$, the height of $\mathrm{Cl}(X \cup \{z\})$ is less than or equal to $l-1$ and, for some $z_0 \in S-X$, the height of $\mathrm{Cl}\,(X \cup \{z_0\})$ equals $l-1$. (Hence, the height of a precomplete set equals 1.) A closed set X is of *infinite height* if, for all natural numbers k, there is a sequence $x_1, \ldots, x_k$ of elements of S such that

$$x_1 \,\overline{\in}\, X \tag{7}$$

and

$$x_i \,\overline{\in}\, \mathrm{Cl}(X \cup \{x_1, \ldots, x_{i-1}\}), \tag{8}$$

for all i where $2 \leqq i \leqq k$. A closed set X is of *sequentially infinite height* if there is an infinite sequence x_i, $i=1, 2, \ldots$, of elements of S satisfying conditions (7) and (8). (For other equivalent definitions of the notion of height, cf. [11, theorem 1].)

After these general definitions, we shall turn to the discussion of the sets $P_{\mathfrak{c}}$ for which closure means closure with respect to composition. We have shown in [11] that $P_{\mathfrak{c}}$ possesses a subset of sequentially infinite height if and only if it possesses an infinitely generated subset. Furthermore, if $\mathfrak{c} \geqq 3$ then $P_{\mathfrak{c}}$ possesses a continuum of subsets of sequentially infinite height. Using the method presented in [5], we shall now construct such a family of subsets of $P_{\mathfrak{c}}$. Denote the range W of the variables of the functions in $P_{\mathfrak{c}}$ by $\{1, 2, 3, \ldots, \mathfrak{c}\}$. Consider the following infinite sequence of functions in $P_{\mathfrak{c}}$:

$$g_k(x_1, \ldots, x_k) =$$
$$= \begin{cases} 2 \text{ if } x_1 = \ldots = x_{i-1} = x_{i+1} = \ldots = x_k = 3,\ x_i = 2,\ 3\ (i=1, \ldots, k); \\ 1, \text{ otherwise,} \end{cases}$$

where $k=2, 3, \ldots$. It is shown in [5] that, for every k,

$$g_k \,\overline{\in}\, \mathrm{Cl}\left(\bigcup_{i \neq k} g_i\right). \tag{9}$$

Denote by $B_{\mathfrak{c}}$ the (infinite) set generated by all functions g_{2i}. Then the following theorem is an immediate consequence of the relation (9).

Theorem 5. *For* $\mathfrak{c} \geqq 3$, *there is a continuum of closed subsets of* $B_{\mathfrak{c}}$. *Each of them is of sequentially infinite height.*

We have shown in [11] that each $P_{\mathfrak{c}}$ (where $\mathfrak{c}$ is finite) contains at most denumerably many subsets which are either of finite height or of infinite but not of sequentially infinite height. Assume that $P_{\mathfrak{c}}$ possesses only finitely many, say, r subsets of height l which are all finitely generated. Let s be a number such that every subset of height l is generated by the s-place functions included in it. (By our assumption, such a number s exists.) Using the estimate for the number of precomplete sets included in a given finitely generated set (cf. [4, pp. 79–80]), we obtain the upper bound $r \cdot 2^u$ where $u = \mathfrak{c}^{\mathfrak{c}^s}$ for the number of subsets of height $l+1$ included in $P_{\mathfrak{c}}$. In particular, if there is only a finite number of sets of height l and each of them is finitely generated then there is only a finite number of sets of height $l+1$. (Thus, the result established in [3] implies that P_3 possesses only finitely many subsets of height 2.) Hence, if each subset of finite height included in $P_{\mathfrak{c}}$ is finitely generated then, for each (finite) l, $P_{\mathfrak{c}}$ possesses only finitely many subsets of height l. We note that these results are not valid for arbitrary sets S and closure operations Cl because, in the general case, a finitely generated set may possess an infinite number of precomplete subsets.

We shall now consider the heights of closed sets of functions in the algebra of logic, i.e., the heights of closed subsets of P_2. There are no subsets of sequentially infinite height. The height of any given closed set is seen from the table below which can be constructed using the theory of Post, [8, especially p. 101]. Also his notation is used.

Height	Sets
0	C_1
1	A_1, C_2, C_3, D_3, L_1
2	$A_2, A_3, C_4, L_2, L_3, L_5, P_6, R_{13}, S_6, F_4^2, F_8^2$
3	$A_4, D_1, P_5, R_4, R_{11}, R_{12}, S_5, F_1^2, F_3^2, F_4^3, F_5^2, F_7^2, F_8^3$
4	$L_4, O_9, R_{10}, F_1^3, F_2^2, F_3^3, F_4^4, F_5^3, F_6^2, F_7^3, F_8^4$
5	$D_2, O_4, O_8, R_9, F_1^4, F_2^3, F_3^4, F_4^5, F_5^4, F_6^3, F_7^4, F_8^5$
6	$O_7, F_1^5, F_2^4, F_3^5, F_4^6, F_5^5, F_6^4, F_7^5, F_8^6$
$i \geqq 7$	$F_1^{i-1}, F_2^{i-2}, F_3^{i-1}, F_4^{i}, F_5^{i-1}, F_6^{i-2}, F_7^{i-1}, F_8^{i}$
infinite	$O_1, O_2, O_3, O_5, O_6, P_1, P_2, P_3, P_4, R_1, R_2, R_3, R_5, R_6, R_7, R_8,$ $S_1, S_2, S_3, S_4, F_j^{\infty}\ (1 \leqq j \leqq 8)$

Consequently, we obtain the following

Theorem 6. *The heights of the sets generated by the truth-functions corresponding to negation and equivalence are, respectively,* 5 *and* 2. *The truth-functions corresponding to conjunction, disjunction and implication generate each a set of infinite height.*

As we have pointed out, very little is known about the heights of subsets of $P_{\mathfrak{c}}$ where $\mathfrak{c} \geqq 3$. Even the heights $\overset{1}{l}_{\mathfrak{c}}$ of the set $\overset{1}{P}_{\mathfrak{c}}$ and $\overset{2}{l}_{\mathfrak{c}}$ of the subset of $P_{\mathfrak{c}}$ consisting of all functions which can be expressed as polynomials (mod $\mathfrak{c}$) are not known. The following result can be proved: For every finite l, there is a finite $\mathfrak{c}$ such that both $\overset{1}{l}_{\mathfrak{c}} > l$ and $\overset{2}{l}_{\mathfrak{c}} > l$.

3. We shall now extend the notion of height to include arbitrary cardinals. We shall again first consider an arbitrary set S and a closure operation Cl for S. For two subsets X and Y of S, we say that X is *Y-independent* if, for all $x \in X$,

$$x \mathrel{\overline{\in}} \mathrm{Cl}(Y \cup X - \{x\}).$$

A set X is *independent* if, for some Y (possibly empty), X is Y-independent. A closed set Y is of *independent height* $\mathfrak{c}$ if there is a Y-independent set X of cardinal $\mathfrak{c}$ but no Y-independent set X' of cardinal $\mathfrak{c}' > \mathfrak{c}$.

We note that if $\mathfrak{c}$ is infinite then a set of independent height $\mathfrak{c}$ is also of sequentially infinite height (and, hence, of infinite height). On the other hand, if $\mathfrak{c}$ is finite then a set of independent height $\mathfrak{c}$ is of height $\geqq \mathfrak{c}$. Also the proof of the following theorem is straight forward from the definitions.

Theorem 7. *If S possesses an independent subset of infinite cardinal* $\mathfrak{c}$ *then S possesses at least* $2^{\mathfrak{c}}$ *subsets of independent height greater than or equal to* $\mathfrak{c}$.

We shall now consider sets $P_{\mathfrak{c}}$. The next theorem is an extension of a result established in [2].

Theorem 8. *The set* $P_{\aleph_0}$ *possesses* $2^{\aleph}$ *subsets of independent height* $\aleph$.

Proof. Since the cardinal of $P_{\aleph_0}$ equals $\aleph$ it is clear that there is no family of subsets of $P_{\aleph_0}$ whose cardinal exceeds $2^{\aleph}$, and no subset of $P_{\aleph_0}$ is of independent height greater than $\aleph$. Hence, by theorem 7, it suffices to prove that there is an independent set $X \subset P_{\aleph_0}$ of cardinal $\aleph$.

Denote by natural numbers the range of the functions in $P_{\aleph_0}$.

For every subset N of the set of all natural numbers $\geqq 3$, we define a 1-place function $f_N(x)$ as follows:

$$f_N(x) = \begin{cases} x, \text{ for } x \in N, \\ x+1, \text{ otherwise.} \end{cases}$$

Obviously, the cardinal of the set F of the functions $f_N(x)$ equals $\aleph$. All the functions $f_N(x)$ satisfy condition $f_N(1)=2$ whereas this condition is not satisfied by any composition of the functions in the set F. This implies that F is independent and, thus, theorem 8 follows.

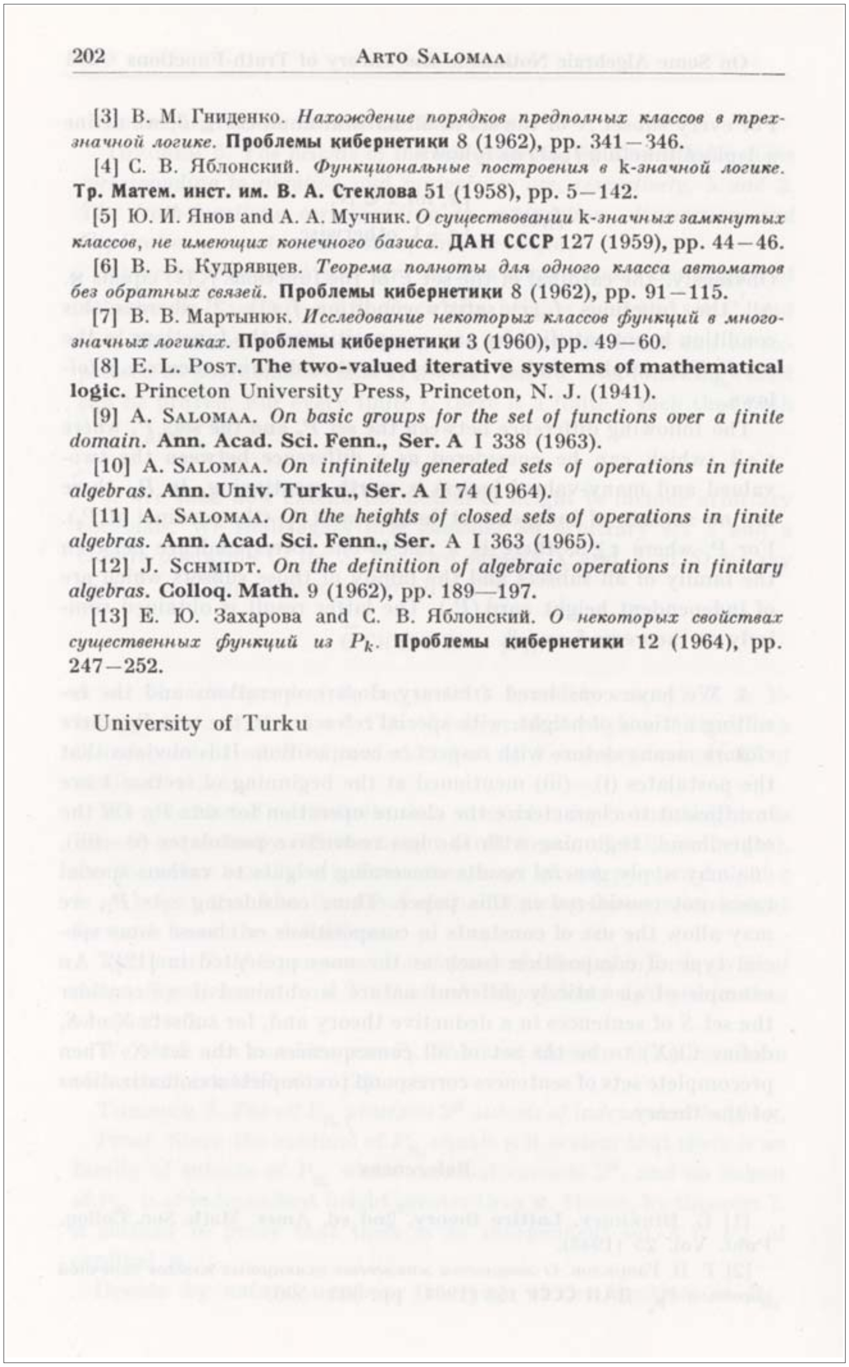
The following difference between the set P_2 and the sets $P_{\mathfrak{c}}$ where $\mathfrak{c} \geqq 3$ (which can be considered as a difference between the two-valued and many-valued logics) is worth mentioning. In P_2, there are no subsets of independent height card(P_2) (the cardinal of P_2). For $P_{\mathfrak{c}}$ where $\mathfrak{c} \geqq 3$, there is a one-to-one correspondence between the family of all subsets and the family of those subsets which are of independent height card $(P_{\mathfrak{c}})$. The latter result is obtained similarly as theorems 5 and 8.

4. We have considered arbitrary closure operations and the resulting notions of height, with special reference to the sets $P_{\mathfrak{c}}$ where closure means closure with respect to composition. It is obvious that the postulates (i)—(iii) mentioned at the beginning of section 1 are insufficient to characterize the closure operation for sets $P_{\mathfrak{c}}$. On the other hand, beginning with the less restrictive postulates (i)—(iii), one may apply general results concerning heights to various special cases not considered in this paper. Thus, considering sets $P_{\mathfrak{c}}$, we may allow the use of constants in compositions or choose some special type of composition (such as the ones presented in [12]). An example of an entirely different nature is obtained if we consider the set S of sentences in a deductive theory and, for subsets X of S, define $\mathrm{Cl}(X)$ to be the set of all consequences of the set X. Then precomplete sets of sentences correspond to complete axiomatizations of the theory.

References

[1] G. Birkhoff. **Lattice theory.** 2nd ed. Amer. Math. Soc. Colloq. Publ. Vol. 25 (1948).

[2] Г. П. Гаврилов. *О мощности множеств замкнутых классов конечной высоты в* $P_{\aleph_0}$. **ДАН СССР** 158 (1964), pp. 503—506.



[3] В. М. Гниденко. *Нахождение порядков предполных классов в трехзначной логике.* **Проблемы кибернетики** 8 (1962), pp. 341—346.

[4] С. В. Яблонский. *Функциональные построения в* k*-значной логике.* **Тр. Матем. инст. им. В. А. Стеклова** 51 (1958), pp. 5—142.

[5] Ю. И. Янов and А. А. Мучник. *О существовании* k*-значных замкнутых классов, не имеющих конечного базиса.* **ДАН СССР** 127 (1959), pp. 44—46.

[6] В. Б. Кудрявцев. *Теорема полноты для одного класса автоматов без обратных связей.* **Проблемы кибернетики** 8 (1962), pp. 91—115.

[7] В. В. Мартынюк. *Исследование некоторых классов функций в многозначных логиках.* **Проблемы кибернетики** 3 (1960), pp. 49—60.

[8] E. L. POST. **The two-valued iterative systems of mathematical logic.** Princeton University Press, Princeton, N. J. (1941).

[9] A. SALOMAA. *On basic groups for the set of functions over a finite domain.* **Ann. Acad. Sci. Fenn., Ser. A** I 338 (1963).

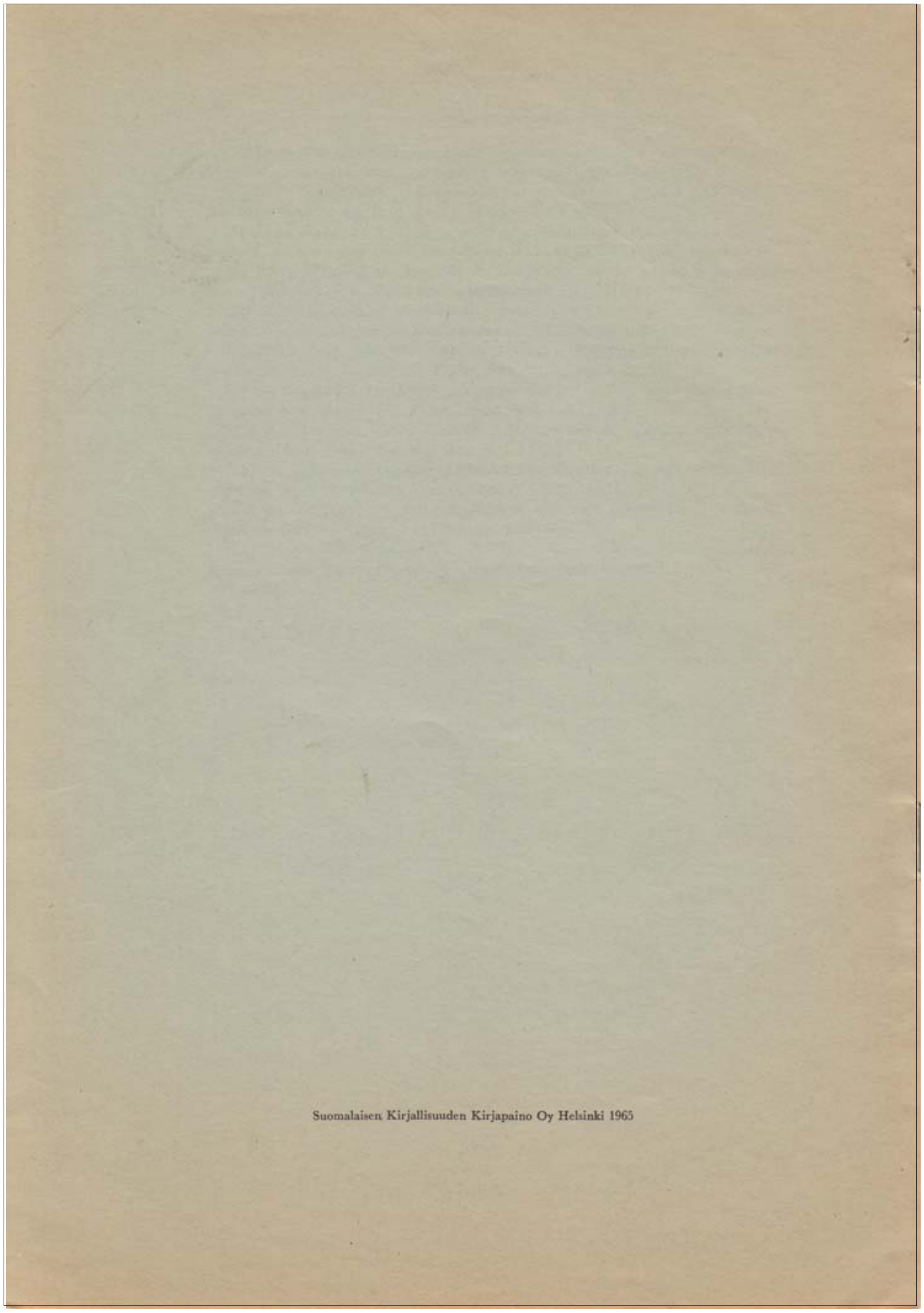
[10] A. SALOMAA. *On infinitely generated sets of operations in finite algebras.* **Ann. Univ. Turku., Ser. A** I 74 (1964).

[11] A. SALOMAA. *On the heights of closed sets of operations in finite algebras.* **Ann. Acad. Sci. Fenn., Ser.** A I 363 (1965).

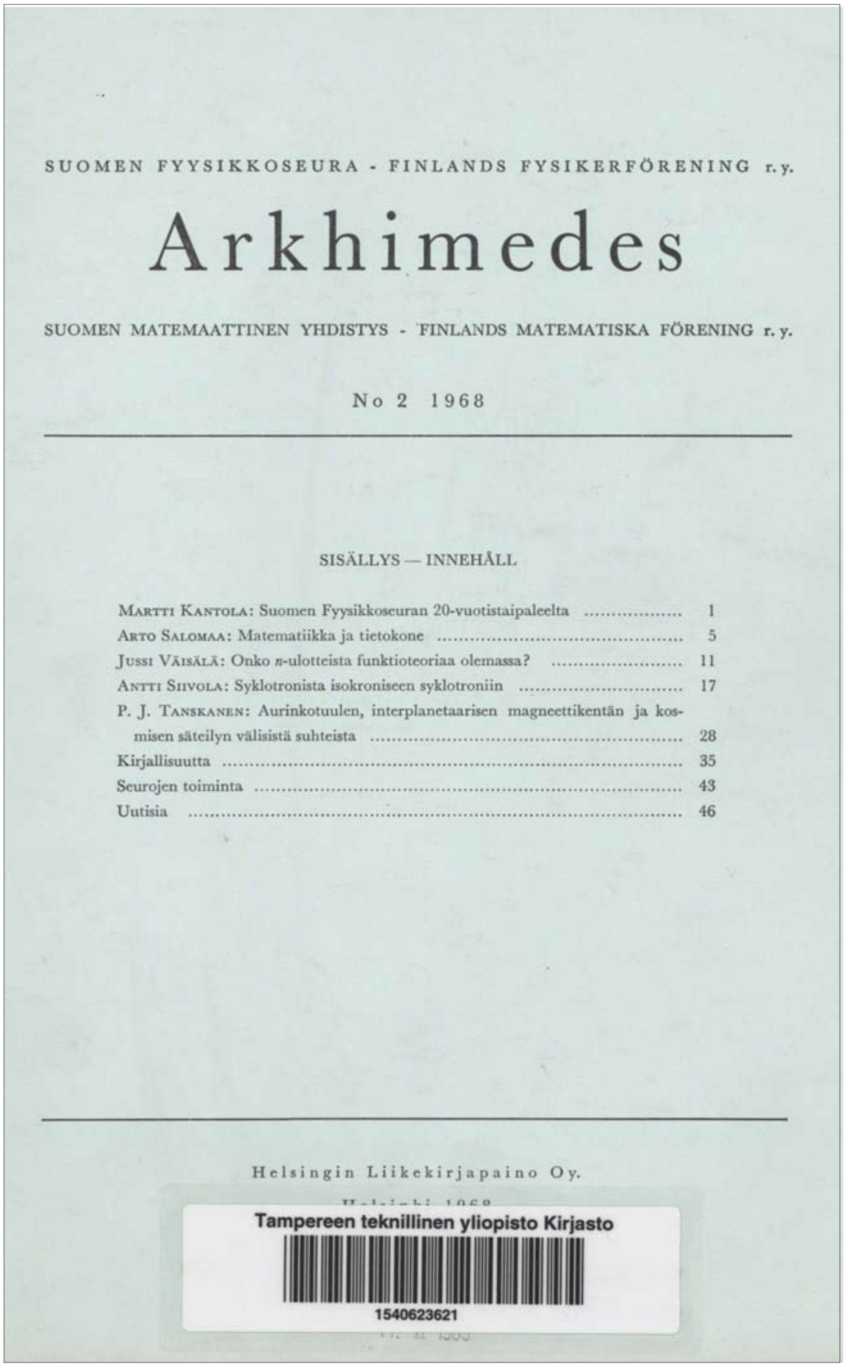
[12] J. SCHMIDT. *On the definition of algebraic operations in finitary algebras.* **Colloq. Math.** 9 (1962), pp. 189—197.

[13] Е. Ю. Захарова and С. В. Яблонский. *О некоторых свойствах существенных функций из* P_k. **Проблемы кибернетики** 12 (1964), pp. 247—252.

University of Turku



Suomalaisen Kirjallisuuden Kirjapaino Oy Helsinki 1965



SUOMEN FYYSIKKOSEURA - FINLANDS FYSIKERFÖRENING r. y.

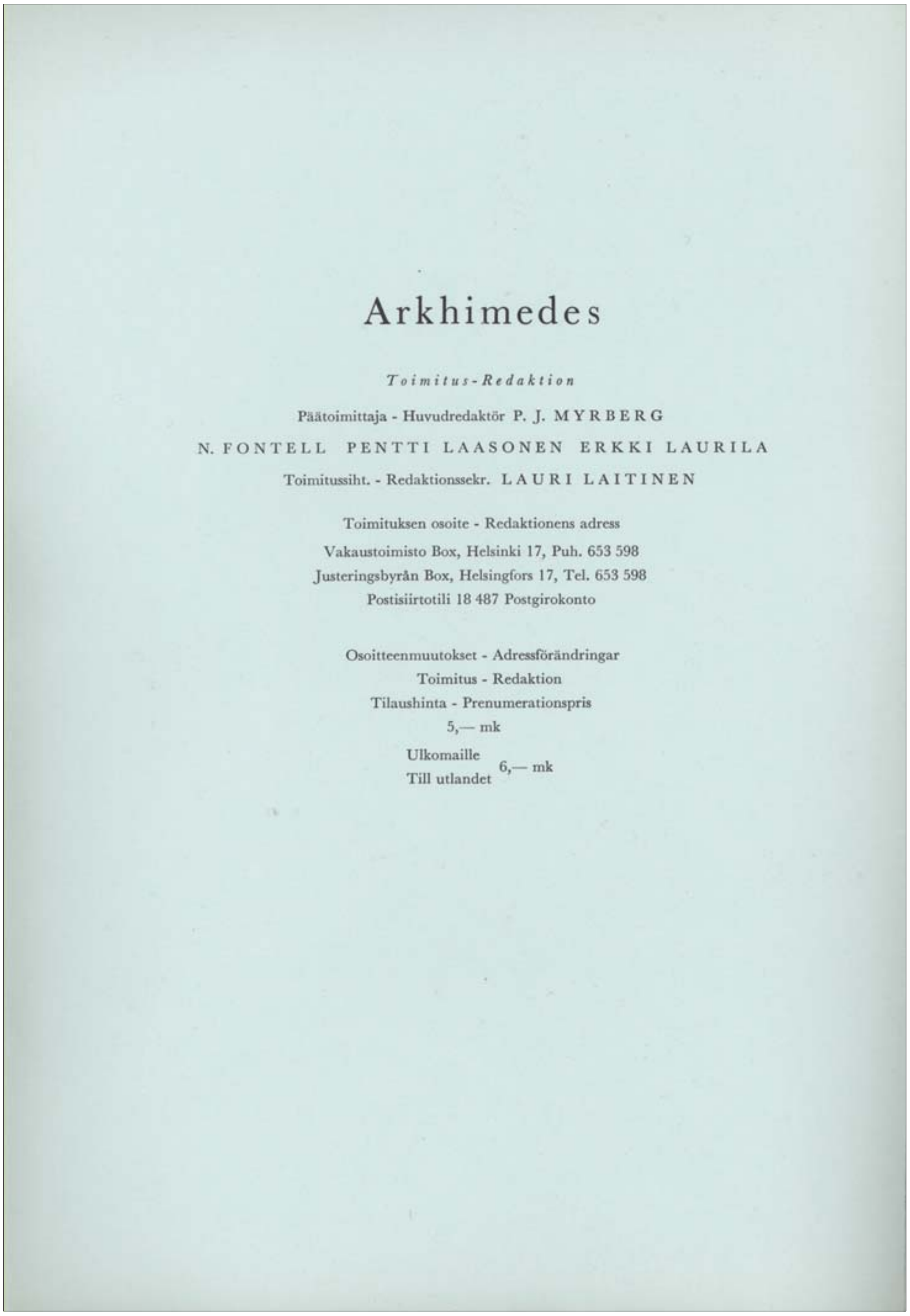
Arkhimedes

SUOMEN MATEMAATTINEN YHDISTYS - FINLANDS MATEMATISKA FÖRENING r. y.

No 2 1968

SISÄLLYS — INNEHÅLL

Helsingin Liikekirjapaino Oy.
Helsinki 1968



Arkhimedes

Toimitus-Redaktion

Päätoimittaja - Huvudredaktör P. J. MYRBERG

N. FONTELL PENTTI LAASONEN ERKKI LAURILA

Toimitussiht. - Redaktionssekr. LAURI LAITINEN

Toimituksen osoite - Redaktionens adress

Vakaustoimisto Box, Helsinki 17, Puh. 653 598
Justeringsbyrån Box, Helsingfors 17, Tel. 653 598
Postisiirtotili 18 487 Postgirokonto

Osoitteenmuutokset - Adressförändringar
Toimitus - Redaktion
Tilaushinta - Prenumerationspris
5,— mk

Ulkomaille
Till utlandet 6,— mk

Matematiikka ja tietokone[1]

Prof. ARTO SALOMAA, Turku

Cambridgen yliopiston matematiikan professori ja tietokonealan huomattava edelläkävijä Charles Babbage kirjoitti viime vuosisadan puolivälissä seuraavasti:

»Laskukoneet ovat mitä parhaita apuvälineitä aritmeettisissa toimituksissa. Jotkut niistä suorittavat koko laskun vain alkuarvot saatuaan ilman että ihminen sen jälkeen puuttuu asiaan. Toiset taas tarvitsevat toimituksen aikana jatkuvaa valvontaa. Nämä jälkimmäiset ovat rakenteeltaan paljon yksinkertaisempia kuin edelliset eivätkä lainkaan niin hyödyllisiä kuin edelliset.»

Kuvattuaan kuinka paljon laskijoita tarvittiin Ranskassa laadittaessa suuren vallankumouksen jälkeen matemaattisia taulukoita Babbage jatkaa:

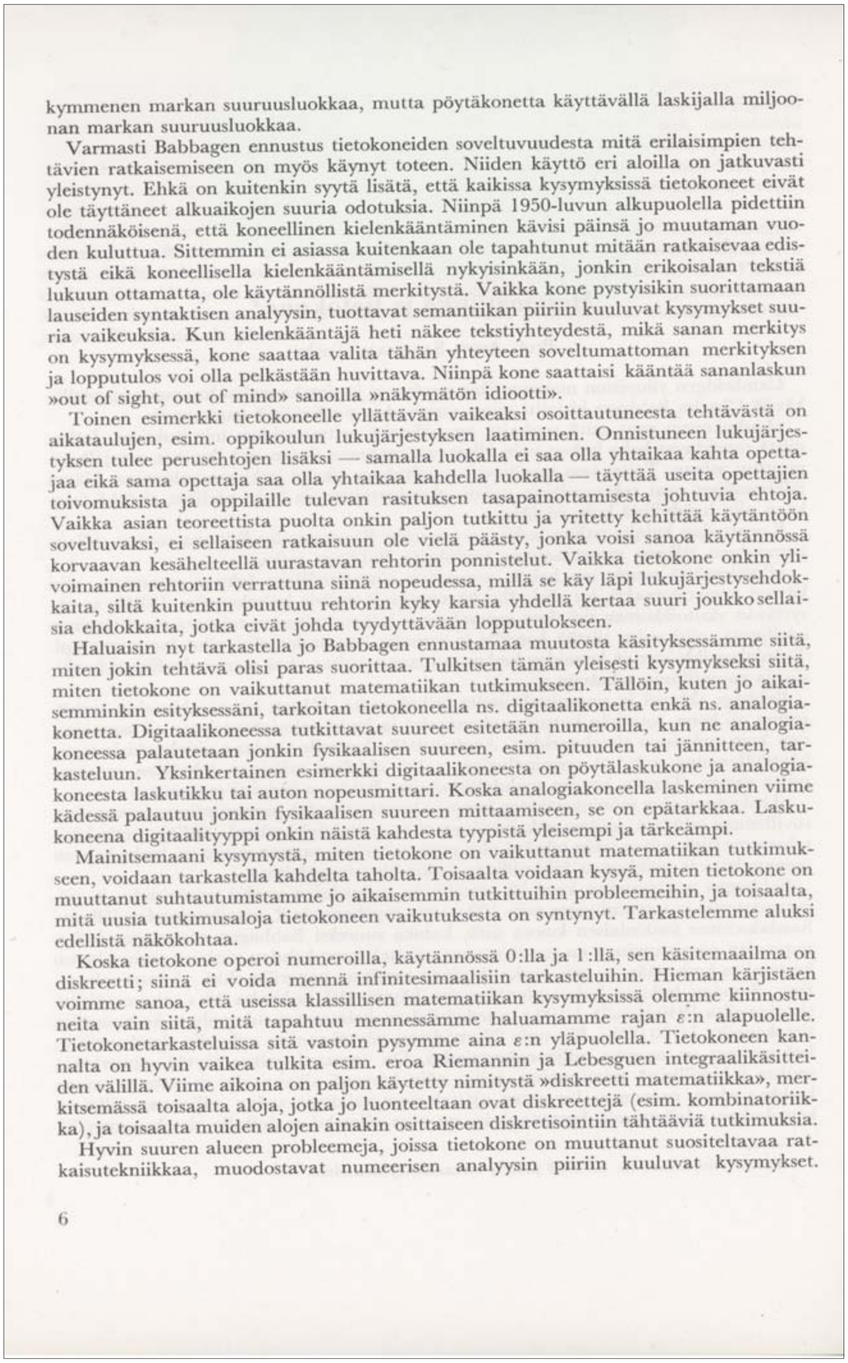
»Epäilemättä suurin osa heistä, muutamia suunnittelijoita lukuun ottamatta, olisi käynyt tarpeettomaksi, jos olisi ollut käytettävissä sopivia laskukoneita. Tällöin se väsyttävän yksitoikkoinen työ, jota samanlaisten laskutoimitusten toistuva suorittaminen edellyttää, olisi voitu siirtää koneille ja samalla lopputulos olisi ollut luotettavampi. Työnjakoa ihmisten ja koneiden kesken voidaan soveltaa yhtä menestyksellisesti henkisiin ja ruumiillisiin tehtäviin.»

Babbage rakensi ja suunnitteli useita laskukoneita. Hänen kunnianhimoisin tavoitteensa oli kone, jota hän kutsui analyyttiseksi ja jonka toimintaperiaate oli samanlainen kuin nykyisten tietokoneiden. Analyyttiselle koneelle voidaan ohjelmakirjastosta, käyttääksemme nykyistä terminologiaa, valita ohjelma erilaisten tehtävien suorittamista varten. Tämän koneen mahdollisuuksista Babbage kirjoitti seuraavasti:

»Laskunopeuden moninkertainen kasvu ja luotettavuuden parantuminen tuovat ulottuvillemme tehtäviä, joiden ratkaiseminen ei muuten kävisi päinsä. Tällöin myös käsityksemme siitä, miten jokin tehtävä olisi paras suorittaa, saattaa muuttua, koska koneen menettelytavat poikkeavat inhimillisten laskijoiden metodeista.»

Babbagen analyyttinen kone jäi teknillisten vaikeuksien vuoksi suunnittelu- ja piirustusasteelle ja toteutui vasta noin 100 vuotta myöhemmin 2. maailmansodan jälkeen. Saadaksemme jonkinlaisen kuvan siitä, kuinka suureksi Babbagen ennustama laskunopeuden parantuminen on muodostunut, ajattelemme kahden viisinumeroisen luvun kertomista keskenään — työ, jonka ihminen suorittaa paperilla ehkä yhdessä minuutissa. Samaan laskuun kuluu pöytäkonetta käyttävältä laskijalta 10 s, ensimmäisiltä tietokoneilta 1940-luvulla 1/100 s ja nykyisiltä ns. kolmannen sukupolven keskisuurilta tietokoneilta 1/100 000 s. Siis noin 20 vuodessa, pöytäkoneista nykyisiin tietokoneisiin, laskunopeus on noussut miljoonakertaiseksi. On varmasti vaikea löytää esimerkkejä muista inhimillisistä toiminnoista, joissa näin lyhyenä aikana olisi saavutettu samaa luokkaa oleva parannus. Jos sitten ajattelemme vaikkapa sadan miljoonan tällaisen kertolaskun edellyttämiä kustannuksia, ne ovat viimeksi mainitulla tietokonetyypillä

[1] Turun Yliopistossa 16. 10. 1968 pidetty virkaanastujaisesitelmä.



kymmenen markan suuruusluokkaa, mutta pöytäkonetta käyttävällä laskijalla miljoonan markan suuruusluokkaa.

Varmasti Babbagen ennustus tietokoneiden soveltuvuudesta mitä erilaisimpien tehtävien ratkaisemiseen on myös käynyt toteen. Niiden käyttö eri aloilla on jatkuvasti yleistynyt. Ehkä on kuitenkin syytä lisätä, että kaikissa kysymyksissä tietokoneet eivät ole täyttäneet alkuaikojen suuria odotuksia. Niinpä 1950-luvun alkupuolella pidettiin todennäköisenä, että koneellinen kielenkääntäminen kävisi päinsä jo muutaman vuoden kuluttua. Sittemmin ei asiassa kuitenkaan ole tapahtunut mitään ratkaisevaa edistystä eikä koneellisella kielenkääntämisellä nykyisinkään, jonkin erikoisalan tekstiä lukuun ottamatta, ole käytännöllistä merkitystä. Vaikka kone pystyisikin suorittamaan lauseiden syntaktisen analyysin, tuottavat semantiikan piiriin kuuluvat kysymykset suuria vaikeuksia. Kun kielenkääntäjä heti näkee tekstiyhteydestä, mikä sanan merkitys on kysymyksessä, kone saattaa valita tähän yhteyteen soveltumattoman merkityksen ja lopputulos voi olla pelkästään huvittava. Niinpä kone saattaisi kääntää sananlaskun »out of sight, out of mind» sanoilla »näkymätön idiootti».

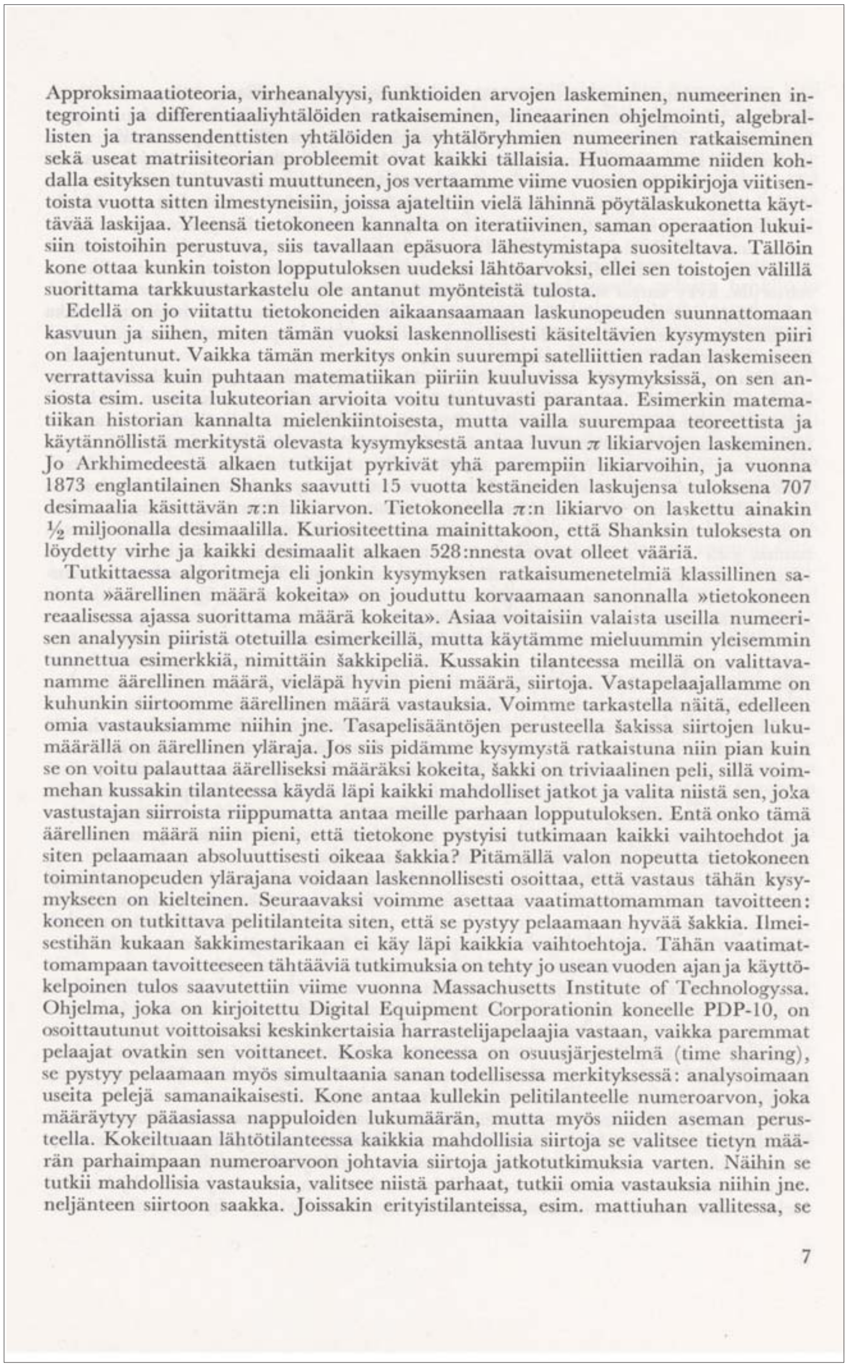
Toinen esimerkki tietokoneelle yllättävän vaikeaksi osoittautuneesta tehtävästä on aikataulujen, esim. oppikoulun lukujärjestyksen laatiminen. Onnistuneen lukujärjestyksen tulee perusehtojen lisäksi — samalla luokalla ei saa olla yhtaikaa kahta opettajaa eikä sama opettaja saa olla yhtaikaa kahdella luokalla — täyttää useita opettajien toivomuksista ja oppilaille tulevan rasituksen tasapainottamisesta johtuvia ehtoja. Vaikka asian teoreettista puolta onkin paljon tutkittu ja yritetty kehittää käytäntöön soveltuvaksi, ei sellaiseen ratkaisuun ole vielä päästy, jonka voisi sanoa käytännössä korvaavan kesähelteellä uurastavan rehtorin ponnistelut. Vaikka tietokone onkin ylivoimainen rehtoriin verrattuna siinä nopeudessa, millä se käy läpi lukujärjestysehdokkaita, siltä kuitenkin puuttuu rehtorin kyky karsia yhdellä kertaa suuri joukko sellaisia ehdokkaita, jotka eivät johda tyydyttävään lopputulokseen.

Haluaisin nyt tarkastella jo Babbagen ennustamaa muutosta käsityksessämme siitä, miten jokin tehtävä olisi paras suorittaa. Tulkitsen tämän yleisesti kysymykseksi siitä, miten tietokone on vaikuttanut matematiikan tutkimukseen. Tällöin, kuten jo aikaisemminkin esityksessäni, tarkoitan tietokoneella ns. digitaalikonetta enkä ns. analogiakonetta. Digitaalikoneessa tutkittavat suureet esitetään numeroilla, kun ne analogiakoneessa palautetaan jonkin fysikaalisen suureen, esim. pituuden tai jännitteen, tarkasteluun. Yksinkertainen esimerkki digitaalikoneesta on pöytälaskukone ja analogiakoneesta laskutikku tai auton nopeusmittari. Koska analogiakoneella laskeminen viime kädessä palautuu jonkin fysikaalisen suureen mittaamiseen, se on epätarkkaa. Laskukoneena digitaalityyppi onkin näistä kahdesta tyypistä yleisempi ja tärkeämpi.

Mainitsemaani kysymystä, miten tietokone on vaikuttanut matematiikan tutkimukseen, voidaan tarkastella kahdelta taholta. Toisaalta voidaan kysyä, miten tietokone on muuttanut suhtautumistamme jo aikaisemmin tutkittuihin probleemeihin, ja toisaalta, mitä uusia tutkimusaloja tietokoneen vaikutuksesta on syntynyt. Tarkastelemme aluksi edellistä näkökohtaa.

Koska tietokone operoi numeroilla, käytännössä 0:lla ja 1:llä, sen käsitemaailma on diskreetti; siinä ei voida mennä infinitesimaalisiin tarkasteluihin. Hieman kärjistäen voimme sanoa, että useissa klassillisen matematiikan kysymyksissä olemme kiinnostuneita vain siitä, mitä tapahtuu mennessämme haluamamme rajan ε:n alapuolelle. Tietokonetarkasteluissa sitä vastoin pysymme aina ε:n yläpuolella. Tietokoneen kannalta on hyvin vaikea tulkita esim. eroa Riemannin ja Lebesguen integraalikäsitteiden välillä. Viime aikoina on paljon käytetty nimitystä »diskreetti matematiikka», merkitsemässä toisaalta aloja, jotka jo luonteeltaan ovat diskreettejä (esim. kombinatoriikka), ja toisaalta muiden alojen ainakin osittaiseen diskretisointiin tähtääviä tutkimuksia.

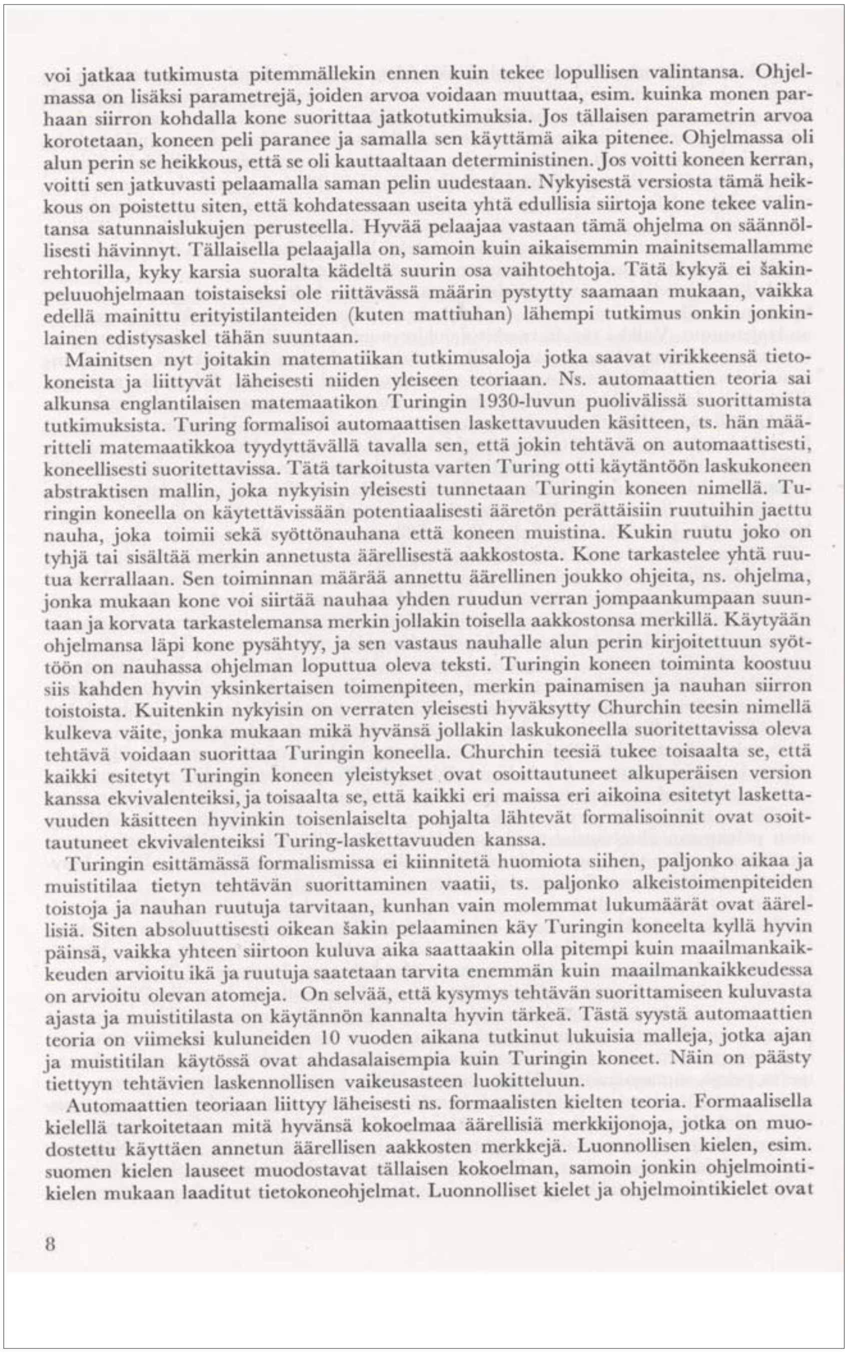
Hyvin suuren alueen probleemeja, joissa tietokone on muuttanut suositeltavaa ratkaisutekniikkaa, muodostavat numeerisen analyysin piiriin kuuluvat kysymykset.



Approksimaatioteoria, virheanalyysi, funktioiden arvojen laskeminen, numeerinen integrointi ja differentiaaliyhtälöiden ratkaiseminen, lineaarinen ohjelmointi, algebrallisten ja transsendenttisten yhtälöiden ja yhtälöryhmien numeerinen ratkaiseminen sekä useat matriisiteorian probleemit ovat kaikki tällaisia. Huomaamme niiden kohdalla esityksen tuntuvasti muuttuneen, jos vertaamme viime vuosien oppikirjoja viitisentoista vuotta sitten ilmestyneisiin, joissa ajateltiin vielä lähinnä pöytälaskukonetta käyttävää laskijaa. Yleensä tietokoneen kannalta on iteratiivinen, saman operaation lukuisiin toistoihin perustuva, siis tavallaan epäsuora lähestymistapa suositeltava. Tällöin kone ottaa kunkin toiston lopputuloksen uudeksi lähtöarvoksi, ellei sen toistojen välillä suorittama tarkkuustarkastelu ole antanut myönteistä tulosta.

Edellä on jo viitattu tietokoneiden aikaansaamaan laskunopeuden suunnattomaan kasvuun ja siihen, miten tämän vuoksi laskennollisesti käsiteltävien kysymysten piiri on laajentunut. Vaikka tämän merkitys onkin suurempi satelliittien radan laskemiseen verrattavissa kuin puhtaan matematiikan piiriin kuuluvissa kysymyksissä, on sen ansiosta esim. useita lukuteorian arvioita voitu tuntuvasti parantaa. Esimerkin matematiikan historian kannalta mielenkiintoisesta, mutta vailla suurempaa teoreettista ja käytännöllistä merkitystä olevasta kysymyksestä antaa luvun π likiarvojen laskeminen. Jo Arkhimedeestä alkaen tutkijat pyrkivät yhä parempiin likiarvoihin, ja vuonna 1873 englantilainen Shanks saavutti 15 vuotta kestäneiden laskujensa tuloksena 707 desimaalia käsittävän π:n likiarvon. Tietokoneella π:n likiarvo on laskettu ainakin ½ miljoonalla desimaalilla. Kuriositeettina mainittakoon, että Shanksin tuloksesta on löydetty virhe ja kaikki desimaalit alkaen 528:nnesta ovat olleet vääriä.

Tutkittaessa algoritmeja eli jonkin kysymyksen ratkaisumenetelmiä klassillinen sanonta »äärellinen määrä kokeita» on jouduttu korvaamaan sanonnalla »tietokoneen reaalisessa ajassa suorittama määrä kokeita». Asiaa voitaisiin valaista useilla numeerisen analyysin piiristä otetuilla esimerkeillä, mutta käytämme mieluummin yleisemmin tunnettua esimerkkiä, nimittäin šakkipeliä. Kussakin tilanteessa meillä on valittavanamme äärellinen määrä, vieläpä hyvin pieni määrä, siirtoja. Vastapelaajallamme on kuhunkin siirtoomme äärellinen määrä vastauksia. Voimme tarkastella näitä, edelleen omia vastauksiamme niihin jne. Tasapelisääntöjen perusteella šakissa siirtojen lukumäärällä on äärellinen yläraja. Jos siis pidämme kysymystä ratkaistuna niin pian kuin se on voitu palauttaa äärelliseksi määräksi kokeita, šakki on triviaalinen peli, sillä voimmehan kussakin tilanteessa käydä läpi kaikki mahdolliset jatkot ja valita niistä sen, joka vastustajan siirroista riippumatta antaa meille parhaan lopputuloksen. Entä onko tämä äärellinen määrä niin pieni, että tietokone pystyisi tutkimaan kaikki vaihtoehdot ja siten pelaamaan absoluuttisesti oikeaa šakkia? Pitämällä valon nopeutta tietokoneen toimintanopeuden ylärajana voidaan laskennollisesti osoittaa, että vastaus tähän kysymykseen on kielteinen. Seuraavaksi voimme asettaa vaatimattomamman tavoitteen: koneen on tutkittava pelitilanteita siten, että se pystyy pelaamaan hyvää šakkia. Ilmeisestihän kukaan šakkimestarikaan ei käy läpi kaikkia vaihtoehtoja. Tähän vaatimattomampaan tavoitteeseen tähtääviä tutkimuksia on tehty jo usean vuoden ajan ja käyttökelpoinen tulos saavutettiin viime vuonna Massachusetts Institute of Technologyssa. Ohjelma, joka on kirjoitettu Digital Equipment Corporationin koneelle PDP-10, on osoittautunut voittoisaksi keskinkertaisia harrastelijapelaajia vastaan, vaikka paremmat pelaajat ovatkin sen voittaneet. Koska koneessa on osuusjärjestelmä (time sharing), se pystyy pelaamaan myös simultaania sanan todellisessa merkityksessä: analysoimaan useita pelejä samanaikaisesti. Kone antaa kullekin pelitilanteelle numeroarvon, joka määräytyy pääasiassa nappuloiden lukumäärän, mutta myös niiden aseman perusteella. Kokeiltuaan lähtötilanteessa kaikkia mahdollisia siirtoja se valitsee tietyn määrän parhaimpaan numeroarvoon johtavia siirtoja jatkotutkimuksia varten. Näihin se tutkii mahdollisia vastauksia, valitsee niistä parhaat, tutkii omia vastauksia niihin jne. neljänteen siirtoon saakka. Joissakin erityistilanteissa, esim. mattiuhan vallitessa, se

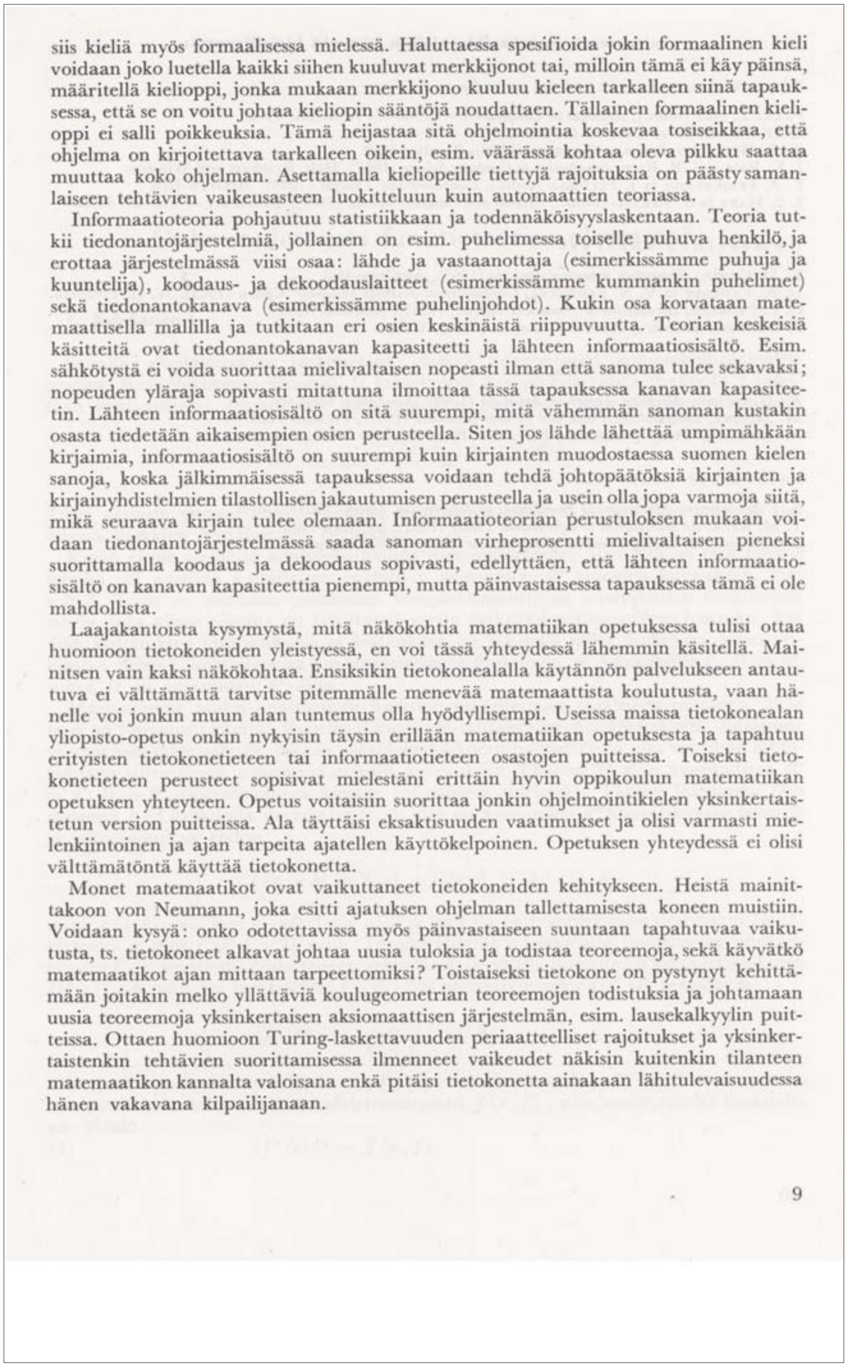


voi jatkaa tutkimusta pitemmällekin ennen kuin tekee lopullisen valintansa. Ohjelmassa on lisäksi parametrejä, joiden arvoa voidaan muuttaa, esim. kuinka monen parhaan siirron kohdalla kone suorittaa jatkotutkimuksia. Jos tällaisen parametrin arvoa korotetaan, koneen peli paranee ja samalla sen käyttämä aika pitenee. Ohjelmassa oli alun perin se heikkous, että se oli kauttaaltaan deterministinen. Jos voitti koneen kerran, voitti sen jatkuvasti pelaamalla saman pelin uudestaan. Nykyisestä versiosta tämä heikkous on poistettu siten, että kohdatessaan useita yhtä edullisia siirtoja kone tekee valintansa satunnaislukujen perusteella. Hyvää pelaajaa vastaan tämä ohjelma on säännöllisesti hävinnyt. Tällaisella pelaajalla on, samoin kuin aikaisemmin mainitsemallamme rehtorilla, kyky karsia suoralta kädeltä suurin osa vaihtoehtoja. Tätä kykyä ei šakinpeluuohjelmaan toistaiseksi ole riittävässä määrin pystytty saamaan mukaan, vaikka edellä mainittu erityistilanteiden (kuten mattiuhan) lähempi tutkimus onkin jonkinlainen edistysaskel tähän suuntaan.

Mainitsen nyt joitakin matematiikan tutkimusaloja jotka saavat virikkeensä tietokoneista ja liittyvät läheisesti niiden yleiseen teoriaan. Ns. automaattien teoria sai alkunsa englantilaisen matematikon Turingin 1930-luvun puolivälissä suorittamista tutkimuksista. Turing formalisoi automaattisen laskettavuuden käsitteen, ts. hän määritteli matemaatikkoa tyydyttävällä tavalla sen, että jokin tehtävä on automaattisesti, koneellisesti suoritettavissa. Tätä tarkoitusta varten Turing otti käytäntöön laskukoneen abstraktisen mallin, joka nykyisin yleisesti tunnetaan Turingin koneen nimellä. Turingin koneella on käytettävissään potentiaalisesti ääretön perättäisiin ruutuihin jaettu nauha, joka toimii sekä syöttönauhana että koneen muistina. Kukin ruutu joko on tyhjä tai sisältää merkin annetusta äärellisestä aakkostosta. Kone tarkastelee yhtä ruutua kerrallaan. Sen toiminnan määrää annettu äärellinen joukko ohjeita, ns. ohjelma, jonka mukaan kone voi siirtää nauhaa yhden ruudun verran jompaankumpaan suuntaan ja korvata tarkastelemansa merkin jollakin toisella aakkostonsa merkillä. Käytyään ohjelmansa läpi kone pysähtyy, ja sen vastaus nauhalle alun perin kirjoitettuun syöttöön on nauhassa ohjelman loputtua oleva teksti. Turingin koneen toiminta koostuu siis kahden hyvin yksinkertaisen toimenpiteen, merkin painamisen ja nauhan siirron toistoista. Kuitenkin nykyisin on verraten yleisesti hyväksytty Churchin teesin nimellä kulkeva väite, jonka mukaan mikä hyvänsä jollakin laskukoneella suoritettavissa oleva tehtävä voidaan suorittaa Turingin koneella. Churchin teesiä tukee toisaalta se, että kaikki esitetyt Turingin koneen yleistykset ovat osoittautuneet alkuperäisen version kanssa ekvivalenteiksi, ja toisaalta se, että kaikki eri maissa eri aikoina esitetyt laskettavuuden käsitteen hyvinkin toisenlaiselta pohjalta lähtevät formalisoinnit ovat osoittautuneet ekvivalenteiksi Turing-laskettavuuden kanssa.

Turingin esittämässä formalismissa ei kiinnitetä huomiota siihen, paljonko aikaa ja muistitilaa tietyn tehtävän suorittaminen vaatii, ts. paljonko alkeistoimenpiteiden toistoja ja nauhan ruutuja tarvitaan, kunhan vain molemmat lukumäärät ovat äärellisiä. Siten absoluuttisesti oikean šakin pelaaminen käy Turingin koneelta kyllä hyvin päinsä, vaikka yhteen siirtoon kuluva aika saattaakin olla pitempi kuin maailmankaikkeuden arvioitu ikä ja ruutuja saatetaan tarvita enemmän kuin maailmankaikkeudessa on arvioitu olevan atomeja. On selvää, että kysymys tehtävän suorittamiseen kuluvasta ajasta ja muistitilasta on käytännön kannalta hyvin tärkeä. Tästä syystä automaattien teoria on viimeksi kuluneiden 10 vuoden aikana tutkinut lukuisia malleja, jotka ajan ja muistitilan käytössä ovat ahdasalaisempia kuin Turingin koneet. Näin on päästy tiettyyn tehtävien laskennollisen vaikeusasteen luokitteluun.

Automaattien teoriaan liittyy läheisesti ns. formaalisten kielten teoria. Formaalisella kielellä tarkoitetaan mitä hyvänsä kokoelmaa äärellisiä merkkijonoja, jotka on muodostettu käyttäen annetun äärellisen aakkosten merkkejä. Luonnollisen kielen, esim. suomen kielen lauseet muodostavat tällaisen kokoelman, samoin jonkin ohjelmointikielen mukaan laaditut tietokoneohjelmat. Luonnolliset kielet ja ohjelmointikielet ovat

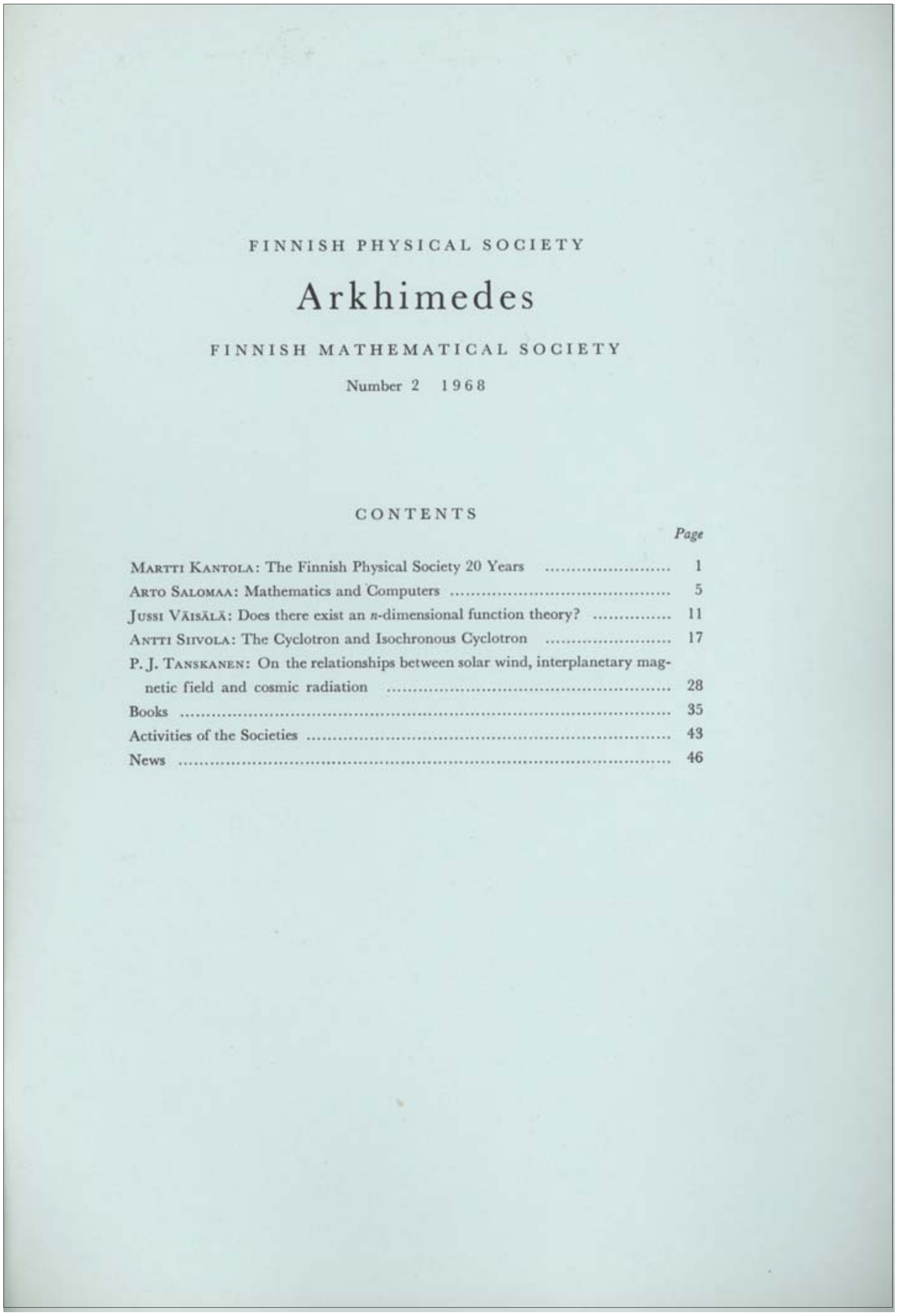


siis kieliä myös formaalisessa mielessä. Haluttaessa spesifioida jokin formaalinen kieli voidaan joko luetella kaikki siihen kuuluvat merkkijonot tai, milloin tämä ei käy päinsä, määritellä kielioppi, jonka mukaan merkkijono kuuluu kieleen tarkalleen siinä tapauksessa, että se on voitu johtaa kieliopin sääntöjä noudattaen. Tällainen formaalinen kielioppi ei salli poikkeuksia. Tämä heijastaa sitä ohjelmointia koskevaa tosiseikkaa, että ohjelma on kirjoitettava tarkalleen oikein, esim. väärässä kohtaa oleva pilkku saattaa muuttaa koko ohjelman. Asettamalla kieliopeille tiettyjä rajoituksia on päästy samanlaiseen tehtävien vaikeusasteen luokitteluun kuin automaattien teoriassa.

Informaatioteoria pohjautuu statistiikkaan ja todennäköisyyslaskentaan. Teoria tutkii tiedonantojärjestelmiä, jollainen on esim. puhelimessa toiselle puhuva henkilö, ja erottaa järjestelmässä viisi osaa: lähde ja vastaanottaja (esimerkissämme puhuja ja kuuntelija), koodaus- ja dekoodauslaitteet (esimerkissämme kummankin puhelimet) sekä tiedonantokanava (esimerkissämme puhelinjohdot). Kukin osa korvataan matemaattisella mallilla ja tutkitaan eri osien keskinäistä riippuvuutta. Teorian keskeisiä käsitteitä ovat tiedonantokanavan kapasiteetti ja lähteen informaatiosisältö. Esim. sähkötystä ei voida suorittaa mielivaltaisen nopeasti ilman että sanoma tulee sekavaksi; nopeuden yläraja sopivasti mitattuna ilmoittaa tässä tapauksessa kanavan kapasiteetin. Lähteen informaatiosisältö on sitä suurempi, mitä vähemmän sanoman kustakin osasta tiedetään aikaisempien osien perusteella. Siten jos lähde lähettää umpimähkään kirjaimia, informaatiosisältö on suurempi kuin kirjainten muodostaessa suomen kielen sanoja, koska jälkimmäisessä tapauksessa voidaan tehdä johtopäätöksiä kirjainten ja kirjainyhdistelmien tilastollisen jakautumisen perusteella ja usein olla jopa varmoja siitä, mikä seuraava kirjain tulee olemaan. Informaatioteorian perustuloksen mukaan voidaan tiedonantojärjestelmässä saada sanoman virheprosentti mielivaltaisen pieneksi suorittamalla koodaus ja dekoodaus sopivasti, edellyttäen, että lähteen informaatiosisältö on kanavan kapasiteettia pienempi, mutta päinvastaisessa tapauksessa tämä ei ole mahdollista.

Laajakantoista kysymystä, mitä näkökohtia matematiikan opetuksessa tulisi ottaa huomioon tietokoneiden yleistyessä, en voi tässä yhteydessä lähemmin käsitellä. Mainitsen vain kaksi näkökohtaa. Ensiksikin tietokonealalla käytännön palvelukseen antautuva ei välttämättä tarvitse pitemmälle menevää matemaattista koulutusta, vaan hänelle voi jonkin muun alan tuntemus olla hyödyllisempi. Useissa maissa tietokonealan yliopisto-opetus onkin nykyisin täysin erillään matematiikan opetuksesta ja tapahtuu erityisten tietokonetieteen tai informaatiotieteen osastojen puitteissa. Toiseksi tietokonetieteen perusteet sopisivat mielestäni erittäin hyvin oppikoulun matematiikan opetuksen yhteyteen. Opetus voitaisiin suorittaa jonkin ohjelmointikielen yksinkertaistetun version puitteissa. Ala täyttäisi eksaktisuuden vaatimukset ja olisi varmasti mielenkiintoinen ja ajan tarpeita ajatellen käyttökelpoinen. Opetuksen yhteydessä ei olisi välttämätöntä käyttää tietokonetta.

Monet matemaatikot ovat vaikuttaneet tietokoneiden kehitykseen. Heistä mainittakoon von Neumann, joka esitti ajatuksen ohjelman tallettamisesta koneen muistiin. Voidaan kysyä: onko odotettavissa myös päinvastaiseen suuntaan tapahtuvaa vaikutusta, ts. tietokoneet alkavat johtaa uusia tuloksia ja todistaa teoreemoja, sekä käyvätkö matemaatikot ajan mittaan tarpeettomiksi? Toistaiseksi tietokone on pystynyt kehittämään joitakin melko yllättäviä koulugeometrian teoreemojen todistuksia ja johtamaan uusia teoreemoja yksinkertaisen aksiomaattisen järjestelmän, esim. lausekalkyylin puitteissa. Ottaen huomioon Turing-laskettavuuden periaatteelliset rajoitukset ja yksinkertaistenkin tehtävien suorittamisessa ilmenneet vaikeudet näkisin kuitenkin tilanteen matemaatikon kannalta valoisana enkä pitäisi tietokonetta ainakaan lähitulevaisuudessa hänen vakavana kilpailijanaan.



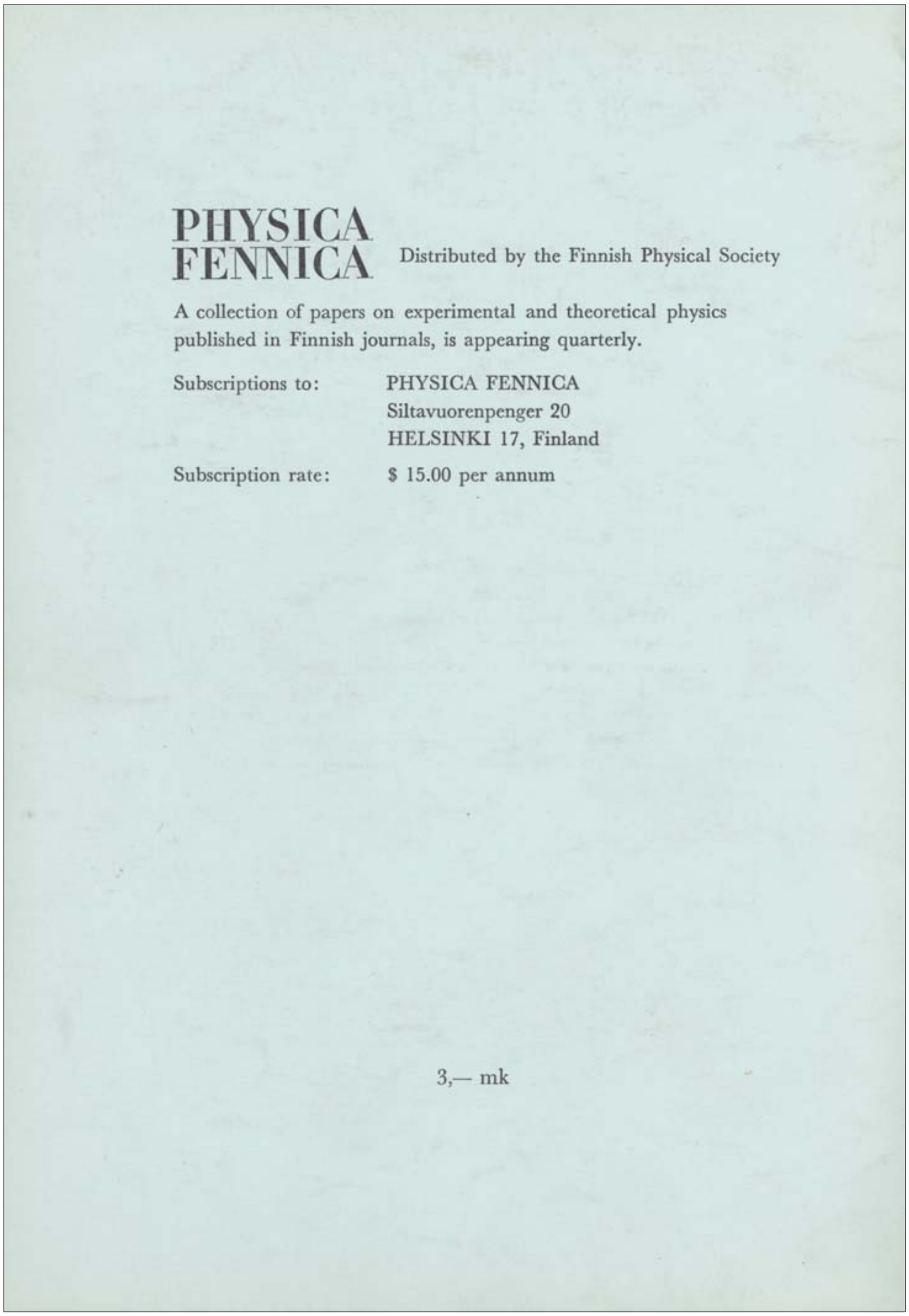
FINNISH PHYSICAL SOCIETY

Arkhimedes

FINNISH MATHEMATICAL SOCIETY

Number 2 1968

CONTENTS



PHYSICA FENNICA Distributed by the Finnish Physical Society

A collection of papers on experimental and theoretical physics published in Finnish journals, is appearing quarterly.

Subscriptions to: PHYSICA FENNICA
Siltavuorenpenger 20
HELSINKI 17, Finland

Subscription rate: $ 15.00 per annum

3,— mk

6 Reviews about the work of Arto Salomaa

This section presents reviews of the work by Arto Salomaa in multiple-valued logic.

1. Review by A.R. Turquette, *The Journal of Symbolic Logic*, Vol. 25, No. 3, September 1960, 291-293.

2. Review by A.R. Turquette, *The Journal of Symbolic Logic*, Vol. 27, No. 2, June 1962, 247.

3. Review by N.M. Martin, *The Journal of Symbolic Logic*, Vol. 29, No. 3, September 1964, 145.

4. Review by A.R. Turquette, *The Journal of Symbolic Logic*, Vol. 31, No. 1, March 1966, 119-120.

5. Review by N.M. Martin, *The Journal of Symbolic Logic*, Vol. 32, No. 4, December 1967, 539.

6. Review by I. Rosenberg, *The Journal of Symbolic Logic*, Vol. 33, No. 2, June 1968, 307.

7. Review by J. Hartmanis, *SIAM Review*, Vol. 17, No. 1, January 1975, 179-180.

8. Review by A. Blikle, *The Journal of Symbolic Logic*, Vol. 42, No. 4, December 1977, 583-584.

Atwell R. Turquette
”On many-valued systems of logic” by Arto Salomaa
”On the composition of functions of several variables ranging over
a finite set” by Arto Salomaa
The Journal of Symbolic Logic, Vol. 25, No. 3, September 1960, 291-293.

is ever shown to be verified or falsified, the claim that it has "middle" value will be shown to be unfounded. But by the same token it is "dangerous" to make any statement of empirical content whatever! To avoid all danger one must say nothing — and have no opinions. (2) Feyerabend insists emphatically that a theory whose consequences are refuted by observation must be changed. Of course. But evidently it suffices to change *some* of the axioms, not all. Usually the logical axioms are left unchanged; but if someone proposes to modify these and leave others unchanged instead, it is not clear why he should be charged with failure to make a "serious" effort to eliminate refutation. (3) Even if Levi is correct in asserting that a three-valued theory of quantum-mechanics should be translatable into a two-valued theory, no justification whatever is adduced for the contention that its translation must be that theory which admits "causal anomalies" (or any other two-valued theory given in advance). Hence the dimness with which he perceives the future of three-valued logic need not be a general affliction. LEON HENKIN

ARTO SALOMAA. *On many-valued systems of logic.* ***Ajatus,*** vol. 22 (1959), pp. 115–159.

ARTO SALOMAA. ***On the composition of functions of several variables ranging over a finite set.*** Annales Universitatis Turkuensis, Series A, Turun Yliopisto, Turku 1960, 48 pp.

The first of these works is divided into two rather independent sections. The shorter is devoted to historical and philosophical remarks relevant to the development of many-valued logics. The longer section is concerned with certain problems of extending to the many-valued case such 2-valued connectives as implication, equivalence, negation, conjunction, and disjunction. The author expresses indebtedness to Professor Georg Henrik von Wright in connection with the historical and philosophical part of his work, and this section, though brief, is more complete and interesting than usual treatments of the subject. For example, he not only shows respect for the work of Jan Łukasiewicz and Emil Post in developing many-valued logics, but also gives proper attention to Hugh MacColl and C. S. Peirce as "the first forerunners of many-valued logics."

The author suggests that it would be more correct historically to refer to such logics as "non-Chrysippian" rather than "non-Aristotelian." In support of this latter view, reference is made to both ancient and mediaeval logic. However, most attention is given to work produced in the field of many-valued logic from the time of MacColl and Peirce to very recent years. In fact, the chief criticism which the reviewer would make of this part of Salomaa's paper is that it pays too little attention to ancient and mediaeval logic. Furthermore, when this period of history is considered, too much use is made of secondary sources and very little attention given to such primary sources as Aristotle's *De interpretatione.*

In the section concerned with the extension of 2-valued connectives to the many-valued case, the basic problem is that of determining what constitutes a *proper analogy* between an M-valued connective ($M > 2$) and a 2-valued connective. For example, it is not clear just how such familiar connectives of the 2-valued propositional calculus as implication, negation, equivalence, conjunction, and disjunction should be characterized in an M-valued propositional calculus ($M > 2$). A brief account is given of some historical solutions to this problem, including the well-known and different extensions of Łukasiewicz, Post, Lewis and Langford, and Webb. A non-exhaustive list of twelve conditions is then presented by the author which he feels should be considered in attempting to extend implication to the many-valued case. This master list is used to define sets of conditions which are ordered in terms of relative strength and tested for consistency and independence in both a weak and strong sense. The same general plan is used in dealing with conditions which might be imposed on negation, equivalence, conjunction, and disjunction in extending them to the many-valued case.

Some important 2-valued tautologies are then selected, mostly from 194***1***, and a study is made of the truth-value properties of the expressions which result from replacing the connectives of the 2-valued tautologies by "analogous" many-valued connectives satisfying the various sets of conditions which have been investigated. A useful table is constructed which summarizes the results obtained by using systems of truth-tables and inductive procedures. In addition to these main results, certain minor problems are considered such as calculating the number of functions satisfying various sets of conditions and deciding whether certain generalized connectives are Sheffer functions.

This is sufficient to indicate that Salomaa's approach to the present problem of determining a "proper analogy" is more general and adequate than usual treatments of the subject. However, to this reviewer it still seems inadequate in at least two respects. Although the author criticises Łukasiewicz for inadequate motivation in the choice of $\max(1, 1 - x + y)$ for implication, his entire account of sets of conditions for many-valued connectives is given with very little motivation. More serious is the fact that a "proper analogy" is often dependent on the role played by a generalized connective in formulating a set of axioms for many-valued logic, and the present treatment gives no attention at all to the axiomatic method.

The second paper is concerned exclusively with one of the minor problems of the first paper; namely, that of constructing and establishing criteria for the existence of Sheffer functions. A Sheffer function is defined essentially as a k-place function which generates all M-valued functions, but consideration is restricted for the most part to the case where $k = 2$ and $M > 2$. Attention is called to the rather large amount of literature on the subject, but no reference is made to Post's VI 114, which seems especially relevant even though it is restricted to the 2-valued case. In fact, the present paper might be thought of as a generalization of some of Post's results. However, more specifically, the paper probably should be thought of as offering an improvement on the results relevant to Sheffer functions obtained in such works as Rose's review of Martin's XVI 275(3) and Słupecki's XI 128, both of which are mentioned by the author. Słupecki's criterion for a full system of many-valued logic, involving the definability of all functions with a single argument, is especially relevant. This becomes apparent from Salomaa's major theorem which is formulated as follows, where "the symmetric group S_n" consists of all permutations of $1, 2, \ldots, n$:

"THEOREM 11.1. *A function $f(x, y)$ which generates the symmetric group S_n is a Sheffer function, provided $n \geqq 3$.*"

This theorem immediately gives rise to the following "criterion C" for Sheffer functions: *If $n \geqq 3$, $f(x, y)$ is a Sheffer function if and only if it generates two permutations $s_1(x)$ and $s_2(x)$ which form a basis of the symmetric group S_n.* Criterion C is said to be "optimal" in the following sense: Let B denote a criterion of the form "$f(x, y)$ is a Sheffer function if and only if it generates every function belonging to the set S." B is *optimal* if no proper subset of S can replace S in B. It is claimed that B is "trivial" if S contains a Sheffer function, so this case is excluded. To this reviewer, such an exclusion does not seem justified since it would appear desirable in many cases to use a B with an S consisting of a single function which is already known to be a Sheffer function. However, such an approach would probably depart from the present emphasis on the symmetric group S_n.

There are many special results in the paper, but most are preliminary to the derivation of theorem 11.1. Once this theorem is obtained with consequence C, attention is focused on the calculation of lower bounds for the number of Sheffer functions when $n \geqq 3$. The author indicates that his results could be improved if the following interesting conjectures could be established:

"CONJECTURE 1. A function $f(x, y)$ which generates the alternating group A_n is a Sheffer function, provided $n \geqq 4$."

"CONJECTURE 2. A function $f(x, y)$ which is not self-conjugate and generates a circular permutation is a Sheffer function, provided n is a prime number."

We are thus still left without an elegant general method for effectively constructing and calculating Sheffer functions for any choice of k and M. In the reviewer's mind, it is not unreasonable to believe that such a method exists, and to him it seems that some of the past difficulties might be overcome if less attention were paid to the matrix structures associated with the case $k = 2$ and more attention given to truth-table structures associated with the case $k > 2$. ATWELL R. TURQUETTE

TAKEO SUGIHARA. *A three-valued logic with meaning-operator.* ***The Memoirs of Fukui University, Librael Arts Department,*** I. Humanities and social sciences, no. 8 (1958), pp. 59–60.

A formal system is described in which the formulas are formed from (propositional) variables by means of ~ ("not"), ⊃ ("implies") and "meaning operators" of the form $(Mp_1, \ldots, p_n)$ where the p's are variables. In a formula $(Mp_1, \ldots, p_n)$F, any of the p's occurring free in F become bound, and if F has no other free variables, $(Mp_1, \ldots, p_n)$F is called a "meaning-closure" of F. It seems necessary also to regard a formula with no free variable as its own meaning-closure, although the author's intention is not clear.

Provability is defined in terms of axioms, a rule of detachment, and presumably substitution, in such a way that the provable formulas are the meaning-closures of the classically provable formulas. Truth-tables are defined with three values interpreted as true, false, and meaningless. Although the author states no results relating truth-value to provability, it can be shown that the provable formulas form a proper subset of the identically true formulas. GENE F. ROSE

Jan ŁUKASIEWICZ. *A system of modal logic.* ***Actes du XIème Congrès International de Philosophie,*** Volume XIV, ***Volume complémentaire et communications du Colloque de Logique,*** North-Holland Publishing Company, Amsterdam 1953, and Editions E. Nauwelaerts, Louvain 1953, pp. 82–87.

JAN ŁUKASIEWICZ. *A system of modal logic.* ***The journal of computing systems,*** vol. 1 no. 3 (1953), pp. 111–149.

IVO THOMAS. *Note on a modal system of Łukasiewicz.* ***Dominican studies,*** vol. 6 (1953), pp. 167–170.

A. N. PRIOR. *The interpretation of two systems of modal logic.* ***The journal of computing systems,*** vol. 1 no. 4 (1954), pp. 201–208.

ALAN ROSS ANDERSON. *On the interpretation of a modal system of Łukasiewicz.* Ibid., pp. 209–210.

JAN ŁUKASIEWICZ. *Arithmetic and modal logic.* Ibid., pp. 213–219.

JAN ŁUKASIEWICZ. *On a controversial problem of Aristotle's modal syllogistic* ***Dominican studies,*** vol. 7 (1954), pp. 114–128.

For the purpose of this review, the above papers are referred to as Ł1, Ł2, T, P, A, Ł3, and Ł4 respectively. In Ł2, Ł1, Ł4, Ł3, and T, a formal system of modal logic is developed and discussed. It is criticised in A and compared with other modal logics in P. The papers are reviewed in the latter order.

In Ł2, Łukasiewicz defines a basic modal logic (BML) which is to be considered as an essential constituent of any modal logic. Using ⊢, ⊣ for assertion and rejection (see XVII 209), and Δ for possibility, BML consists of a classical propositional calculus supplemented by ⊢ $Cp\Delta p$, ⊣ $C\Delta pp$, ⊣ Δp, and ⊢ $E\Delta p\Delta NNp$. Necessity (Γ) is introduced through the definitional equivalence ⊢ $E\Gamma pN\Delta Np$. There are the usual rules of sub-

Atwell R. Turquette
”On the number of simple bases of the set of functions over
a finite domain” by Arto Salomaa
”Some completeness criteria for sets of functions over
a finite domain” by Arto Salomaa
The Journal of Symbolic Logic, Vol. 27, No. 2, June 1962, 247.

products. Similar tables for disjunctive or mixed functions may be produced by converting according to the duality laws.

The second note demonstrates how this table may be generalised for the analysis of Boolean functions constructed from the operations of product, sum, and complement. All the usual steps for the conventional truth-tables can be isomorphically transformed into Boolean equivalents. The columns of T's and F's under the reference formula for the classes x, y, z are represented by alternating vertical bars and empty spaces; x is represented by a single bar and an empty space, y by two bars and two spaces, z by four bars and four spaces.

For example, the analysis of the function

$$F = \{[(x \cap y) \cup z']' \cup (x' \cap y)\}$$

is graphically set out as follows. The reference formula for x, y, z, is put on the left side of the table and the function is written widely spaced on the top. Bars are then entered below each compartment (1) for membership of the sets denoted by the variables, (2) for the complements (if any) of the (1) entries, (3) for the binary operations conjoining the preceding entries, and (4) for the complements of the formulas designated under (3). The function is represented as a whole in the final column.

This table may easily be adapted to the propositional calculus. In a propositional argument we first replace the implications etc. contained therein by their definition in terms of conjunctions and negations. We then proceed as above, except that we now deal with operations on propositions rather than classes. The validity of the argument may be tested by reference to the table, and is indicated by a continuous line down the final column.

The generalised Boole table resembles Martin Gardner's network diagram (cf. pp. 60–79 of his XXIV 78). In the latter, however, continuous bars represent variables and horizontal lines 'shuttling' across these bars indicate operations on them. In Stuermann's table both variables and operations are indicated by bars of varying lengths. W. MAYS

ARTO SALOMAA. ***On the number of simple bases of the set of functions over a finite domain.*** Annales Universitatis Turkuensis, Series A, no. 52, Turun Yliopisto, Turku 1962, 4 pp.

ARTO SALOMAA. ***Some completeness criteria for sets of functions over a finite domain.*** Ibid., no. 53, Turku 1962, 10 pp.

These papers are closely related to the author's XXV 291. They are concerned with problems associated with sets of functionally complete or Post-complete functions of k arguments in n-valued logic.

The first paper calls a function obtained from a given function F by identifying some of its variables a *diagonalization* of F. A diagonalization of F is *proper* if it differs from F. A functionally complete set of functions in n-valued logic is called "a basis of E_n" if none of its proper subsets is functionally complete. Following Shestopal, the author calls a basis B of E_n *simple* if "no set B_1, obtained by replacing some function in B by one of its proper diagonalizations, is complete." The following generalization of a result of Shestopal for two-valued logic is proved: *The number of all simple bases of E_n, $n \geqq 3$, is finite.*

The second paper is concerned with establishing Conjecture 1 in XXV 291. To this end the following theorem is proved: *A function F with k arguments which generates the alternating group A_n is a Sheffer function, provided $n \geqq 4$.* Conjecture 1 follows at once for $k = 2$. ATWELL R. TURQUETTE

Ú. I. ÁNOV and A. A. MUČNIK. *O suščéstvovanii k-značnyh zamknutyh klassov, né iméúščih konéčnogo bazisa* (On the existence of k-valued closed classes not having a finite basis). ***Doklady Akademii Nauk SSSR,*** vol. 127 (1959), pp. 44–46.

Norman M. Martin
”On sequences of functions over an arbitrary domain”
by Arto Salomaa
The Journal of Symbolic Logic, Vol. 29, No. 3, September 1964, 145.

Let $m = \prod_{i=1}^{n} a_i^{b_i}$. For $n \geqq 2$, the author exhibits a complete self m-al set of independent primitives consisting of one two-place function and $\sum_{i=1}^{n} a_i^{b_i}$ one-place functions. For $m \geqq 3$, he also constructs a complete self m-al set of independent primitives consisting of one two-place function and the constants $1, \ldots, m$.

In view of the many results obtained by the author, it is natural to ask whether analogous more general results could be obtained for the notion of conjugacy. So far only two particular permutations $\varphi(x)$ of degree m (namely, $\varphi(x) = m + 1 - x$ and $\varphi(x) = x + 1 \pmod{m}$) in the equation (1) have been considered. It is possible that results analogous to those of the author can be obtained for other permutations φ, perhaps even without specifying the permutation. The following problem is of some interest: given an integer $m \geqq 2$ and a permutation φ of degree m, to determine the smallest number r such that there is a complete self-conjugate (under φ) set of independent m-valued primitives consisting of one two-place function and r one-place functions. It seems obvious that the number r depends on the order of the permutation φ. ARTO SALOMAA

ARTO SALOMAA. ***On sequences of functions over an arbitrary domain.*** Annales Universitatis Turkuensis, Series AI, no. 62, Turun Yliopisto, Turku 1963, 5 pp.

This article may be regarded as a generalization into the denumerable domain of results on Sheffer functions. Assume F_A is the set of functions of finite Cartesian power (so-called "finite place functions") of a denumerable set A into A. The author proves that for every denumerable subset D_A of F_A, there exists a two-place function $f_D(x, y)$ in F_A (but not necessarily in D_A) which generates all functions of D_A. The method employed is reminiscent of XVII 204, using a result of Sierpinski concerning generation of arbitrary infinite sequences of integers instead of the analagous result for finite sequences of Picard. NORMAN M. MARTIN

BRUNO SCARPELLINI. *Die Nichtaxiomatisierbarkeit des unendlichwertigen Prädikatenkalküls von Łukasiewicz.* ***The journal of symbolic logic,*** vol. 27 no. 2 (for 1962, pub. 1963), pp. 159–170.

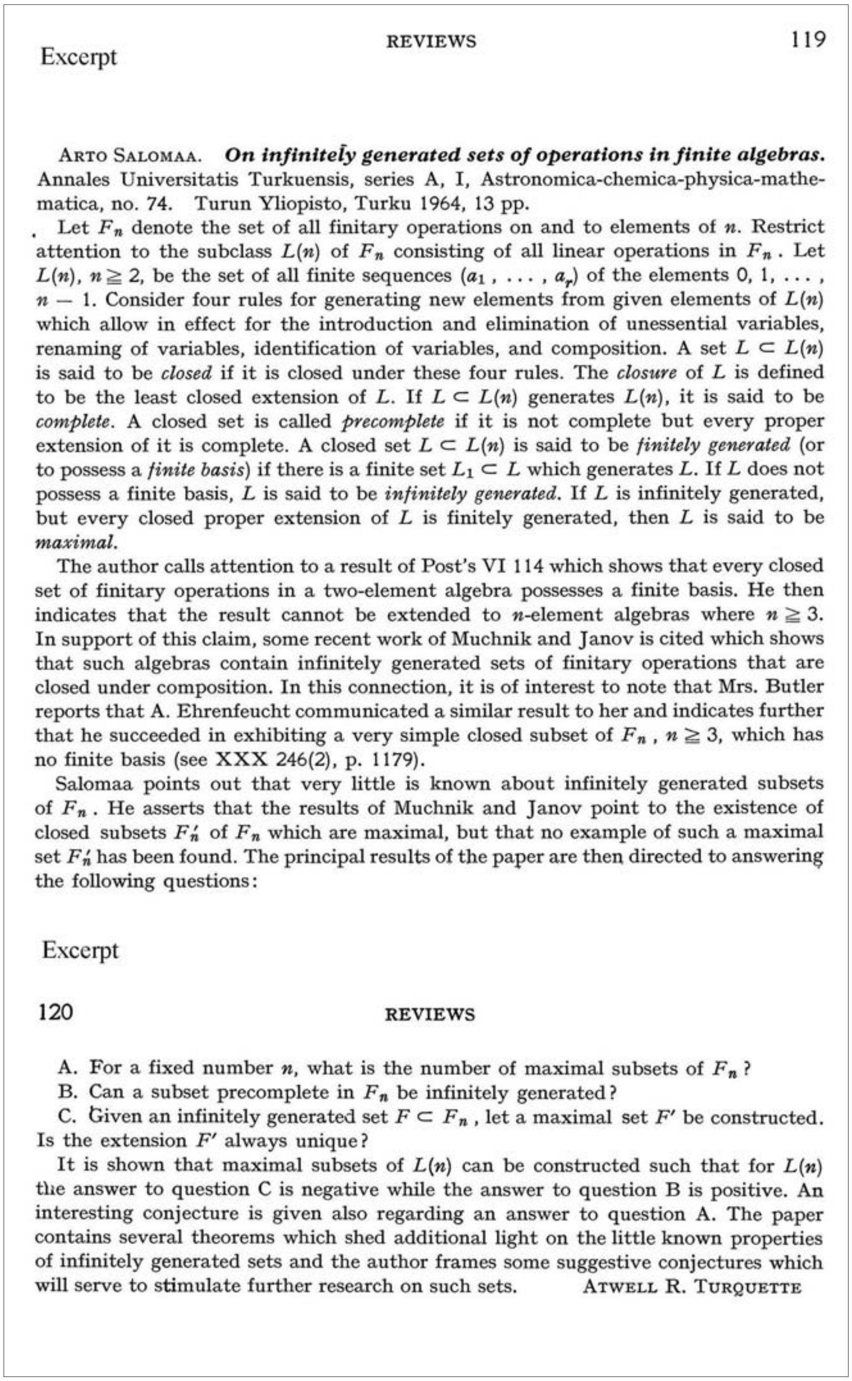
Scarpellini shows that the infinite-valued predicate calculus of first order, corresponding to the infinite-valued propositional calculus of Łukasiewicz, cannot be formalised by means of a finite number of axioms and rules of procedure. He shows that to each formula of the two-valued predicate calculus there corresponds a formula of the infinite-valued predicate calculus such that the former formula is satisfiable in a finite universe if and only if the latter is satisfiable in the set of truth-values x such that $0 < x \leqq 1$. Since the set of formulas of the two-valued calculus which are not satisfiable in any finite universe is not recursively enumerable it then follows, by means of an argument involving Gödel numbers, that the set of formulas of the infinite-valued calculus which always take the value 0 is not recursively enumerable. The required result then follows at once. ALAN ROSE

KURT SCHÜTTE. *Der Interpolationssatz der intuitionistischen Prädikatenlogik.* ***Mathematische Annalen,*** vol. 148 (1962), pp. 192–200.

The author obtains an extension of Craig's interpolation theorem (XXIV 243) by showing that the result also holds for intuitionistic predicate calculus. His proof gives rise to a new proof for the original (classical) case. He uses the cut-free formulation of intuitionistic predicate calculus which he developed in XVI 155 (the calculus obtained from K_3 by the omission of the redundant *Schnitt* rule).

The interpolation theorem is considered in a form which can be briefly summarized as follows. We suppose that if Γ is a sequence $C_1, \ldots, C_n$ of formulas and C is any formula then $\Gamma \rightarrow C$ shall denote $C_1 \rightarrow (C_2 \rightarrow \ldots \rightarrow (C_n \rightarrow C) \ldots)$. Suppose F is a

Atwell R. Turquette
”On infinitely generated sets of operations in finite algebras”
by Arto Salomaa
The Journal of Symbolic Logic, Vol. 31, No. 1, March 1966, 119-120.



Excerpt

Arto Salomaa. ***On infinitely generated sets of operations in finite algebras.*** Annales Universitatis Turkuensis, series A, I, Astronomica-chemica-physica-mathematica, no. 74. Turun Yliopisto, Turku 1964, 13 pp.

Let F_n denote the set of all finitary operations on and to elements of n. Restrict attention to the subclass $L(n)$ of F_n consisting of all linear operations in F_n. Let $L(n)$, $n \geqq 2$, be the set of all finite sequences $(a_1, \ldots, a_r)$ of the elements 0, 1, . . . , $n - 1$. Consider four rules for generating new elements from given elements of $L(n)$ which allow in effect for the introduction and elimination of unessential variables, renaming of variables, identification of variables, and composition. A set $L \subset L(n)$ is said to be *closed* if it is closed under these four rules. The *closure* of L is defined to be the least closed extension of L. If $L \subset L(n)$ generates $L(n)$, it is said to be *complete*. A closed set is called *precomplete* if it is not complete but every proper extension of it is complete. A closed set $L \subset L(n)$ is said to be *finitely generated* (or to possess a *finite basis*) if there is a finite set $L_1 \subset L$ which generates L. If L does not possess a finite basis, L is said to be *infinitely generated*. If L is infinitely generated, but every closed proper extension of L is finitely generated, then L is said to be *maximal*.

The author calls attention to a result of Post's VI 114 which shows that every closed set of finitary operations in a two-element algebra possesses a finite basis. He then indicates that the result cannot be extended to n-element algebras where $n \geqq 3$. In support of this claim, some recent work of Muchnik and Janov is cited which shows that such algebras contain infinitely generated sets of finitary operations that are closed under composition. In this connection, it is of interest to note that Mrs. Butler reports that A. Ehrenfeucht communicated a similar result to her and indicates further that he succeeded in exhibiting a very simple closed subset of F_n, $n \geqq 3$, which has no finite basis (see XXX 246(2), p. 1179).

Salomaa points out that very little is known about infinitely generated subsets of F_n. He asserts that the results of Muchnik and Janov point to the existence of closed subsets F_n' of F_n which are maximal, but that no example of such a maximal set F_n' has been found. The principal results of the paper are then directed to answering the following questions:

Excerpt

A. For a fixed number n, what is the number of maximal subsets of F_n?

B. Can a subset precomplete in F_n be infinitely generated?

C. Given an infinitely generated set $F \subset F_n$, let a maximal set F' be constructed. Is the extension F' always unique?

It is shown that maximal subsets of $L(n)$ can be constructed such that for $L(n)$ the answer to question C is negative while the answer to question B is positive. An interesting conjecture is given also regarding an answer to question A. The paper contains several theorems which shed additional light on the little known properties of infinitely generated sets and the author frames some suggestive conjectures which will serve to stimulate further research on such sets. Atwell R. Turquette

Norman M. Martin
"On essential variables of functions, especially in the Algebra of logic"
by Arto Salomaa
The Journal of Symbolic Logic, Vol. 32, No. 4, December 1967, 539.

Let $m = \Pi_{i=1}^{n} a_i^{b_i}$. For $n \geqq 2$, the author exhibits a complete self m-al set of independent primitives consisting of one two-place function and $\Sigma_{i=1}^{n} a_i^{b_i}$ one-place functions. For $m \geqq 3$, he also constructs a complete self m-al set of independent primitives consisting of one two-place function and the constants $1, \ldots, m$.

In view of the many results obtained by the author, it is natural to ask whether analogous more general results could be obtained for the notion of conjugacy. So far only two particular permutations $\varphi(x)$ of degree m (namely, $\varphi(x) = m + 1 - x$ and $\varphi(x) = x + 1 \pmod{m}$) in the equation (1) have been considered. It is possible that results analogous to those of the author can be obtained for other permutations φ, perhaps even without specifying the permutation. The following problem is of some interest: given an integer $m \geqq 2$ and a permutation φ of degree m, to determine the smallest number r such that there is a complete self-conjugate (under φ) set of independent m-valued primitives consisting of one two-place function and r one-place functions. It seems obvious that the number r depends on the order of the permutation φ. ARTO SALOMAA

ARTO SALOMAA. ***On sequences of functions over an arbitrary domain.*** Annales Universitatis Turkuensis, Series AI, no. 62, Turun Yliopisto, Turku 1963, 5 pp.

This article may be regarded as a generalization into the denumerable domain of results on Sheffer functions. Assume F_A is the set of functions of finite Cartesian power (so-called "finite place functions") of a denumerable set A into A. The author proves that for every denumerable subset D_A of F_A, there exists a two-place function $f_D(x, y)$ in F_A (but not necessarily in D_A) which generates all functions of D_A. The method employed is reminiscent of XVII 204, using a result of Sierpinski concerning generation of arbitrary infinite sequences of integers instead of the analagous result for finite sequences of Picard. NORMAN M. MARTIN

BRUNO SCARPELLINI. *Die Nichtaxiomatisierbarkeit des unendlichwertigen Prädikatenkalküls von Łukasiewicz.* ***The journal of symbolic logic,*** vol. 27 no. 2 (for 1962, pub. 1963), pp. 159–170.

Scarpellini shows that the infinite-valued predicate calculus of first order, corresponding to the infinite-valued propositional calculus of Łukasiewicz, cannot be formalised by means of a finite number of axioms and rules of procedure. He shows that to each formula of the two-valued predicate calculus there corresponds a formula of the infinite-valued predicate calculus such that the former formula is satisfiable in a finite universe if and only if the latter is satisfiable in the set of truth-values x such that $0 < x \leqq 1$. Since the set of formulas of the two-valued calculus which are not satisfiable in any finite universe is not recursively enumerable it then follows, by means of an argument involving Gödel numbers, that the set of formulas of the infinite-valued calculus which always take the value 0 is not recursively enumerable. The required result then follows at once. ALAN ROSE

KURT SCHÜTTE. *Der Interpolationssatz der intuitionistischen Prädikatenlogik.* ***Mathematische Annalen,*** vol. 148 (1962), pp. 192–200.

The author obtains an extension of Craig's interpolation theorem (XXIV 243) by showing that the result also holds for intuitionistic predicate calculus. His proof gives rise to a new proof for the original (classical) case. He uses the cut-free formulation of intuitionistic predicate calculus which he developed in XVI 155 (the calculus obtained from K_3 by the omission of the redundant *Schnitt* rule).

The interpolation theorem is considered in a form which can be briefly summarized as follows. We suppose that if Γ is a sequence $C_1, \ldots, C_n$ of formulas and C is any formula then $\Gamma \rightarrow C$ shall denote $C_1 \rightarrow (C_2 \rightarrow \ldots \rightarrow (C_n \rightarrow C) \ldots)$. Suppose F is a

Ivo Rosenberg
”A theorem concerning the composition of functions of
several variables ranging over a finite set”
by Arto Salomaa
”On basic groups for the set of functions over a finite domain”
by Arto Salomaa
The Journal of Symbolic Logic, Vol. 33, No. 2, June 1968, 307.

thereof, $p \to q \to . s \to s \to t \to t \to (q \to r) \to . p \to r$, $s \to (u \to u \to . p \to r \to t) \to . q \to r \to . p \to q \to . s \to t$, or the last with the consequent permuted.

In the proofs for these implicational fragments, Meredith makes use of an interesting analogy between implicational calculi and combinatory logic developed by Curry in XXXII 267, pp. 313ff. To each thesis in the theory of implication there corresponds a combinator, and deducibility from axioms corresponds to definability in terms of primitive combinators. However, as Curry points out, the analogy is not complete. One set of combinators may be definable by means of another, and yet the respective implicational theorems fail to follow from the corresponding axioms. Meredith gives this case in point: $p \supset q \supset . s \supset p \supset (q \supset r) \supset . p \supset r$ is not (he claims) a sufficient axiom for positive implication, but the corresponding combinator suffices to define combinators corresponding to known axioms (augmentation and permuted distribution) for positive implication. Likewise sufficient are the combinators corresponding to syllogism and augmentation along with $\mathbf{W}_*(\lambda x . xx)$, which however has no implicational analogue.

Łukasiewicz has shown that syllogism, Peirce's law, and any tautologous $p \supset . \mathrm{A} \supset \mathrm{B}$ yield the full calculus of material implication. Meredith gives matrices which show that this ceases to be so if Peirce's law is replaced by $p \supset q \supset r \supset . p \supset r \supset r$, $p \supset q \supset p \supset . p \supset r \supset r$, $p \supset q \supset . p \supset q \supset p \supset r$, or $p \supset r \supset . p \supset q \supset r \supset r$, all of which are proved deductively equivalent in the presence of syllogism.

Authors' corrections. Page 180, line 23, for D5, read **D**5**D**5; page 184, §11, last line, delete ", although 1 is organic." *Further corrections.* Page 175, step 20, for t, read r; page 179, line 11, after the fourth C, insert another one.

JOHN BACON

ARTO SALOMAA. *A theorem concerning the composition of functions of several variables ranging over a finite set.* ***The journal of symbolic logic,*** vol. 25 no. 3 (for 1960, pub. 1962), pp. 203–208.

ARTO SALOMAA. ***On basic groups for the set of functions over a finite domain.*** Annales Academiae Scientiarum Fennicae, Series A.I, Mathematica, no. 338, Helsinki 1963, 15 pp.

Let $\mathfrak{S}_n$ be the set of the functions whose variables, finite in number, range over a fixed finite set $N = \{1, 2, \cdots, n\}$ $(n \geqq 2)$ and whose values are elements of N. If $F \subset \mathfrak{S}_n$ we denote by $\bar{F}$ the closure of F under composition, i.e., the set of all finite compositions of functions of F (whose variables may be not different from each other). F is termed a Sheffer set or complete set if $\bar{F} = \mathfrak{S}_n$. Sheffer sets are very important in many-valued logics. The purpose of the first paper is the following generalization of a basic Słupecki theorem.

THEOREM. Let F be a set consisting of all the $n!$ permutations of the numbers $1, 2, \cdots, n$ and of an arbitrary two-place function $f(x, y)$ which is non-degenerately binary and assumes all of the numbers $1, 2, \cdots, n$ as values. Then, provided $n \geqq 5$, F is a Sheffer set.

The proof of the theorem consists of six lemmas. Another modification of the Słupecki theorem was given by Áblonskij.

A group P of permutations of the numbers $1, 2, \cdots, n$ is termed a basic group for $\mathfrak{S}_n$ if the addition to P of any function of $\mathfrak{S}_n$ depending essentially on at least two variables and assuming all n values yields a complete set. The author has shown in previous papers that the symmetric and even the alternating group are basic groups. In the second paper the following generalization is given.

THEOREM. Every quadruply transitive group of degree n is a basic group for $\mathfrak{S}_n$, provided $n \geqq 5$. If, in addition, $n \neq 2^r$, then every triply transitive group of degree n is a basic group for $\mathfrak{S}_n$.

A counterexample is given for the exceptional case $n = 2^r$ and is studied in detail for $n = 8$.

IVO ROSENBERG

ROBERTO CIGNOLI. *Boolean elements in Lukasiewicz algebras. I.* ***Proceedings of the Japan Academy,*** t. 41 (1965), p. 670–675.

L'auteur étudie l'algèbre łukasiewiczienne trivalente, fondée par Gr. C. Moisil, où l'opérateur M (possibilité) joue un rôle important. Cignoli représente cet opérateur par ∇, défini sur un réticulé distributif A, étant determiné uniquement par l'ensemble K des éléments $k \in A$ tels que $\nabla k = k$.

J. Hartmanis

Formal Languages by Arto Salomaa

SIAM Review, Vol. 17, No. 1, January 1975, 179-180.

especially that done by Soviet mathematicians. The bibliography of some 650 entries is 75 percent composed of items published since 1960.

R. D. DRIVER
University of Rhode Island

Formal Languages. By ARTO SALOMAA. Academic Press, New York 1973. xiii + 322 pp. $19.00.

It should be said at the very beginning that this is a very well written book which gives an elegant and well balanced exposition of the mathematical theory of formal languages and should be a valuable addition to the maturing set of textbooks in theoretical computer science. The author has not tried in this book to cover all aspects of formal languages and their relation to automata, but has limited himself to treat formal languages from the generative devices point of view. Recognition devices are mentioned and even defined, but then only in terms of rewriting systems, and they definitely play a subordinated role in this development of language theory. Furthermore, the author does not stress the applications of formal languages, but concentrates on the development of their mathematical properties. The style of writing is clean and economical, with limited but sufficient motivation. The strength of the book comes from a good selection of topics, the well balanced treatment of these topics and the nice flow of ideas as the topics are developed and compared. The book is divided in three parts as follows.

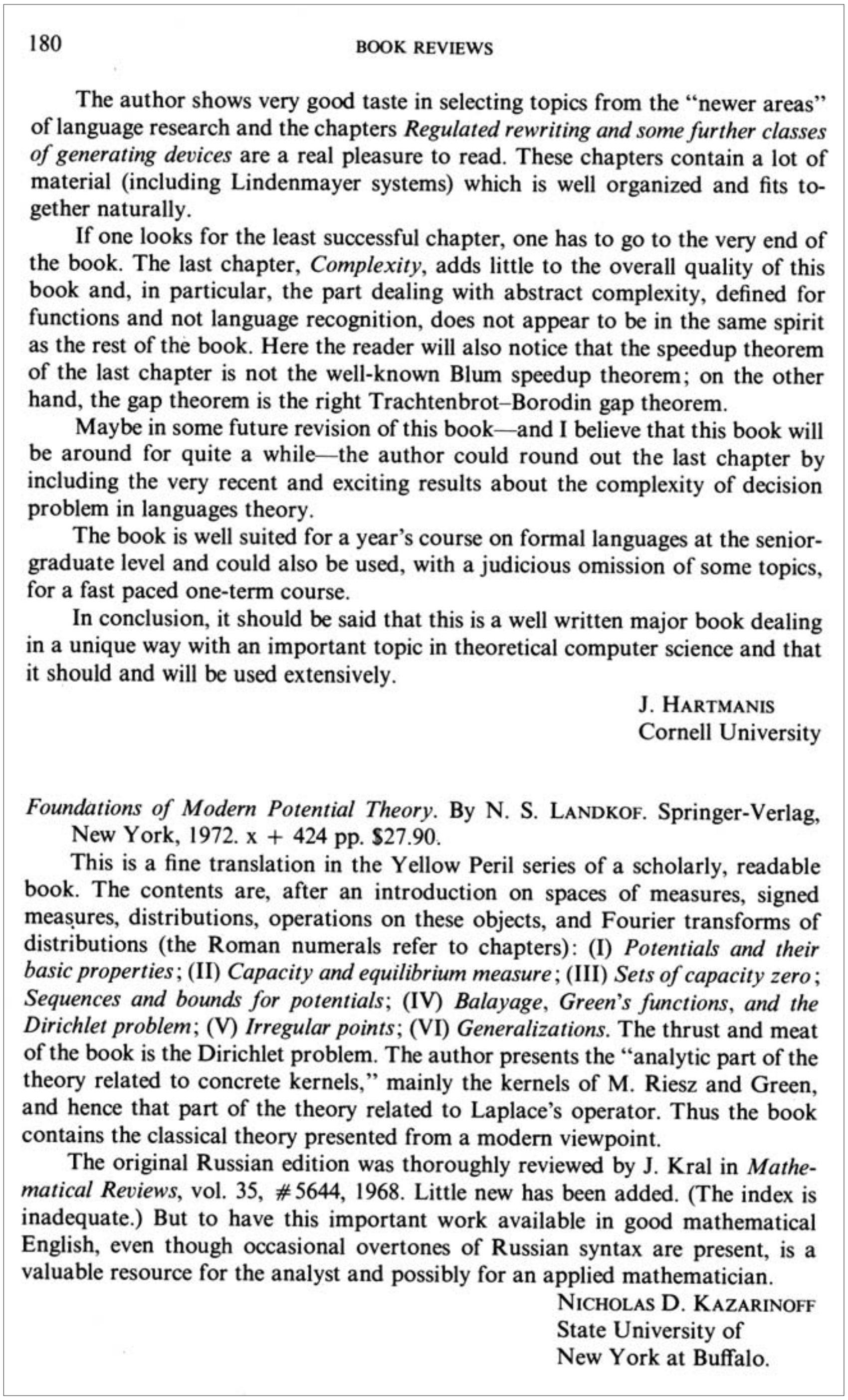
Part One: *Language and grammar*, *Regular and context-free languages*, *Context-sensitive and type-*0 *languages*;

Part Two: *Abstract families of languages*, *Regulated rewriting*, *Context-free languages revisited*, *Some further classes of generative devices*;

Part Three: *Solvability and unsolvability*, *Complexity*.

The reviewer was originally quite surprised that the author has chosen to demote the recognition devices in this book to a very minor role and is still somewhat concerned that this book may deprive the reader of the intuitive help which automata provide in thinking about languages. On the other hand, the approach taken by the author is consistent and well presented and, maybe those who will use this book will not miss very much those nice gadgets " chugging along, changing states and popping and pushing things". In a few places, though, the author has probably gone a bit too far in deemphasizing the recognition devices; for example, it is stated in a proposition that "a language is accepted by a pushdown automaton if and only if it is context-free", but no proof is given. Similarly, there is no proof of the characterization of context-sensitive languages by means of linearly bounded automata. There is a proof that if a language is accepted by a Turing machine, then it is of type 0, but no proof that every type-0 language is accepted by a Turing machine.

At the same time, in the very nice chapter *Abstract families of languages*, one finds with great relief that one is mercifully saved from the detailed definitions of abstract families of acceptors. They are just mentioned in a few lines at the end of the chapter, and here one certainly does not miss these somewhat artificial accepting devices.



The author shows very good taste in selecting topics from the "newer areas" of language research and the chapters *Regulated rewriting and some further classes of generating devices* are a real pleasure to read. These chapters contain a lot of material (including Lindenmayer systems) which is well organized and fits together naturally.

If one looks for the least successful chapter, one has to go to the very end of the book. The last chapter, *Complexity*, adds little to the overall quality of this book and, in particular, the part dealing with abstract complexity, defined for functions and not language recognition, does not appear to be in the same spirit as the rest of the book. Here the reader will also notice that the speedup theorem of the last chapter is not the well-known Blum speedup theorem; on the other hand, the gap theorem is the right Trachtenbrot–Borodin gap theorem.

Maybe in some future revision of this book—and I believe that this book will be around for quite a while—the author could round out the last chapter by including the very recent and exciting results about the complexity of decision problem in languages theory.

The book is well suited for a year's course on formal languages at the senior-graduate level and could also be used, with a judicious omission of some topics, for a fast paced one-term course.

In conclusion, it should be said that this is a well written major book dealing in a unique way with an important topic in theoretical computer science and that it should and will be used extensively.

J. Hartmanis
Cornell University

Foundations of Modern Potential Theory. By N. S. Landkof. Springer-Verlag, New York, 1972. x + 424 pp. $27.90.

This is a fine translation in the Yellow Peril series of a scholarly, readable book. The contents are, after an introduction on spaces of measures, signed measures, distributions, operations on these objects, and Fourier transforms of distributions (the Roman numerals refer to chapters): (I) *Potentials and their basic properties*; (II) *Capacity and equilibrium measure*; (III) *Sets of capacity zero*; *Sequences and bounds for potentials*; (IV) *Balayage, Green's functions, and the Dirichlet problem*; (V) *Irregular points*; (VI) *Generalizations*. The thrust and meat of the book is the Dirichlet problem. The author presents the "analytic part of the theory related to concrete kernels," mainly the kernels of M. Riesz and Green, and hence that part of the theory related to Laplace's operator. Thus the book contains the classical theory presented from a modern viewpoint.

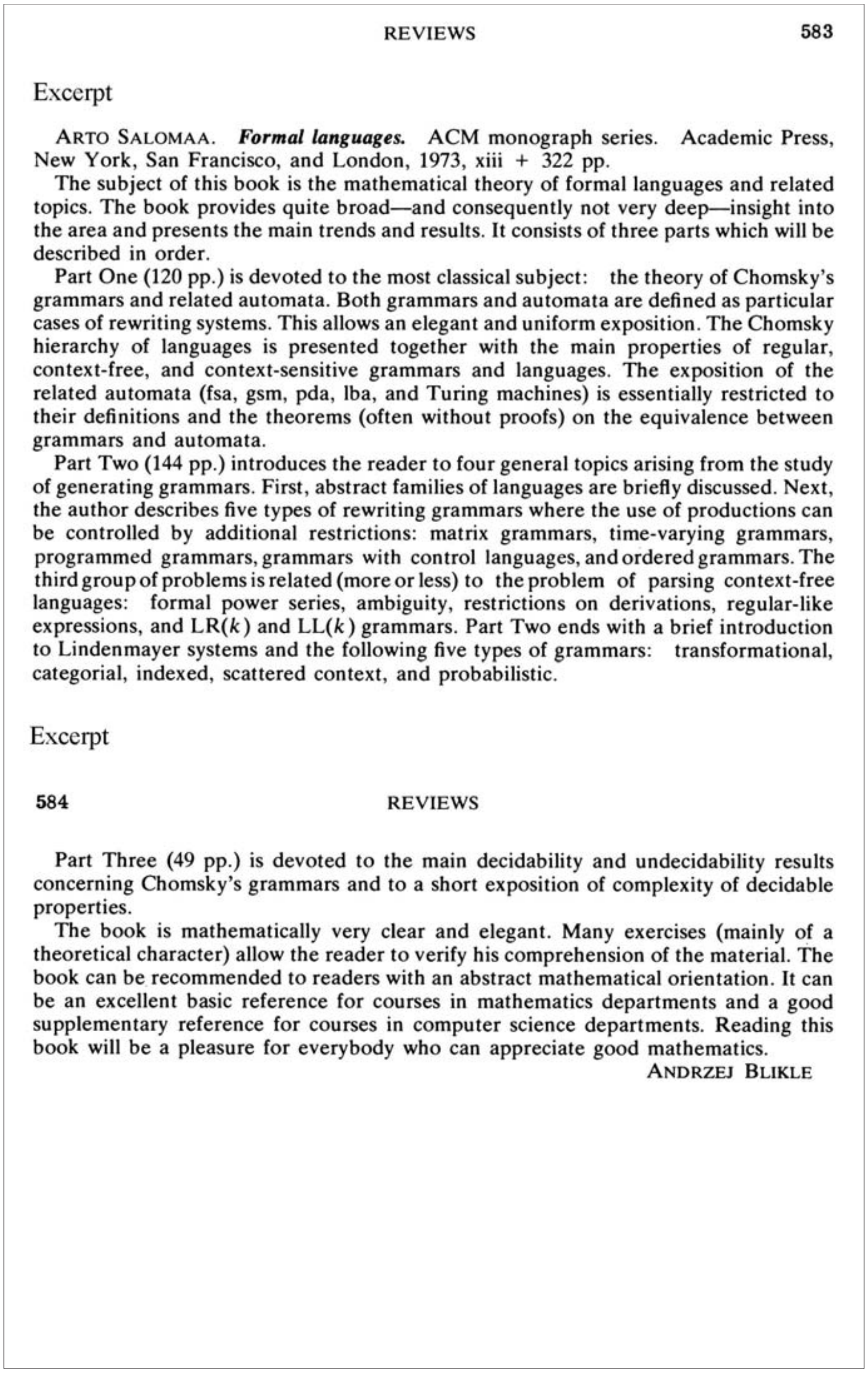
The original Russian edition was thoroughly reviewed by J. Kral in *Mathematical Reviews*, vol. 35, #5644, 1968. Little new has been added. (The index is inadequate.) But to have this important work available in good mathematical English, even though occasional overtones of Russian syntax are present, is a valuable resource for the analyst and possibly for an applied mathematician.

Nicholas D. Kazarinoff
State University of
New York at Buffalo.

Andrzej Blikle

Formal Languages by Arto Salomaa

The Journal of Symbolic Logic, Vol. 42, No. 4, December 1977, 583-584.



Excerpt

ARTO SALOMAA. ***Formal languages.*** ACM monograph series. Academic Press, New York, San Francisco, and London, 1973, xiii + 322 pp.

The subject of this book is the mathematical theory of formal languages and related topics. The book provides quite broad—and consequently not very deep—insight into the area and presents the main trends and results. It consists of three parts which will be described in order.

Part One (120 pp.) is devoted to the most classical subject: the theory of Chomsky's grammars and related automata. Both grammars and automata are defined as particular cases of rewriting systems. This allows an elegant and uniform exposition. The Chomsky hierarchy of languages is presented together with the main properties of regular, context-free, and context-sensitive grammars and languages. The exposition of the related automata (fsa, gsm, pda, lba, and Turing machines) is essentially restricted to their definitions and the theorems (often without proofs) on the equivalence between grammars and automata.

Part Two (144 pp.) introduces the reader to four general topics arising from the study of generating grammars. First, abstract families of languages are briefly discussed. Next, the author describes five types of rewriting grammars where the use of productions can be controlled by additional restrictions: matrix grammars, time-varying grammars, programmed grammars, grammars with control languages, and ordered grammars. The third group of problems is related (more or less) to the problem of parsing context-free languages: formal power series, ambiguity, restrictions on derivations, regular-like expressions, and LR(k) and LL(k) grammars. Part Two ends with a brief introduction to Lindenmayer systems and the following five types of grammars: transformational, categorial, indexed, scattered context, and probabilistic.

Excerpt

Part Three (49 pp.) is devoted to the main decidability and undecidability results concerning Chomsky's grammars and to a short exposition of complexity of decidable properties.

The book is mathematically very clear and elegant. Many exercises (mainly of a theoretical character) allow the reader to verify his comprehension of the material. The book can be recommended to readers with an abstract mathematical orientation. It can be an excellent basic reference for courses in mathematics departments and a good supplementary reference for courses in computer science departments. Reading this book will be a pleasure for everybody who can appreciate good mathematics.

ANDRZEJ BLIKLE

7 Reviews by Arto Salomaa

This section presents reviews written by Arto Salomaa about the work by various researchers in the area of multiple-valued logic.

1. Review for K. Jaakko, J. Hintikka, *The Journal of Symbolic Logic*, Vol. 28, No. 2, June 1963, 165.
2. Review for S.V. Yablonskij, *The Journal of Symbolic Logic*, Vol. 29, No. 4, December 1964, 214-216.
3. Review for A. Rose, *The Journal of Symbolic Logic*, Vol. 29, No. 3, September 1964, 144-145.
4. Review for A.R. Turquette, *The Journal of Symbolic Logic*, Vol. 29, No. 3, September 1964, 143.
5. Review for R.E. Clay, *The Journal of Symbolic Logic*, Vol. 30, No. 1, March 1965, 105.
6. Review for R.E., Clay, *The Journal of Symbolic Logic*, Vol. 30, No. 1, March 1965, 105-106.
7. Review for A. Nakamura, *The Journal of Symbolic Logic*, Vol. 30, No. 3, September 1965, 374-375.
8. Review for A. Nakamura, *The Journal of Symbolic Logic*, Vol. 31, No. 4, December 1966, 665.
9. Review for V.M., Glushkov, *The Journal of Symbolic Logic*, Vol. 33, No. 4, December 1968, 629.
10. Review for O.P. Kuznecov, *The Journal of Symbolic Logic*, Vol. 33, No. 4, December 1968, 629.
11. Review for A.V. Gladkij, *The Journal of Symbolic Logic*, Vol. 35, No. 2, June 1970, 340.
12. Review for S. Ginsburg, *The Journal of Symbolic Logic*, Vol. 41, No. 4, December 1976, 788-789.

Arto Salomaa
”On the logical study of language” by K. Jaakko, J. Hintikka
The Journal of Symbolic Logic, Vol. 28, No. 2, June 1963, 165.

(1′) $$(x)(\Phi x \cdot {\sim}\Psi x \supset Qx),$$

(2′) $$(x)({\sim}\Phi x \cdot \Psi x \supset {\sim}Qx);$$

and the synthetic component has the form

(3) $$(x){\sim}(\Phi x \cdot \Psi x).$$

It should be noted that the conjunction of (1) and (2) is logically equivalent to the conjunction of (1′), (2′), and (3).

The undesirable consequences of adding to a theory even "idle" definitions of theoretical terms (i.e., definitions made by using observable terms) consist in making any theory of the kind investigated by the author equivalent (on the basis of these definitions) with the set of its observable theorems, as well as in making a consistent further development of such theories impossible in many cases. The addition of new criteria of applicability for a theoretical term to a theory can in fact lead to inconsistency in consequence of the definitions adopted, since a definitional formula which is "idle" in a theory T_1 may not be "idle" in a richer theory T_2.

The chief shortcoming of the paper seems to consist in the use of the terms "analytic" and "synthetic" without their having been defined; and its chief merit, in stressing what I should like to call incomplete semantical characterization of theoretical terms by elementary ones in empirical theories — a feature which allows for the enrichment of such theories by new criteria of applicability for theoretical terms without changing the denotations of these terms.

It is a matter of regret that at the time of writing the author apparently was not acquainted with Carnap's XXV 71(2) where the problem of breaking down the postulates of an empirical theory into analytic and synthetic components is treated in a more general way. MARIA KOKOSZYŃSKA

K. JAAKKO J. HINTIKKA. *Loogisen kielentutkimuksen näköaloja* (On the logical study of language). ***Ajatus***, vol. 19 (1956), pp. 81–96.

After some preliminary remarks on philosophical analysis in general, the author discusses Quine's criticism of the notion of analyticity. This leads him to an exposition of Wittgenstein's "language-game." Finally, some related ideas from the theory of recursive functions, as well as from the author's own reduction theory are mentioned.

ARTO SALOMAA

FRANCIS C. OGLESBY. ***An examination of a decision procedure.*** Memoirs of the American Mathematical Society, no. 44. American Mathematical Society, Providence 1962, 148 pp.

F. C. OGLESBY. *Report*: *An examination of a decision procedure.* ***Bulletin of the American Mathematical Society,*** vol. 67 (1961), pp. 300–304.

In 1953, R. Stanley (XXI 197) gave a reduction procedure for the sentences of the lower predicate calculus. In certain cases, this procedure leads to the conclusion that the sentence in question is universally valid (a *theorem*). In the review referred to above, Ackermann gave an example of a theorem whose validity cannot be established by Stanley's procedure. Also in 1953, J. Hintikka (XX 75) developed a theory of distributive normal forms for the lower predicate calculus. In certain cases, Hintikka's method establishes the refutability of a given sentence.

The first paper under review here is, according to a footnote, largely identical with a doctoral dissertation presented to Lehigh University in 1961. In it, the author carries out an extremely detailed and painstaking investigation of Stanley's procedure, taking particular account of the work of Hintikka which was mentioned above. He goes beyond the formal results stated previously by Stanley and Hintikka in several respects. In particular, he shows that Stanley's method can be used as a decision

Arto Salomaa
"Functional constructions in k-valued logic" by S. V. Ablonskij
The Journal of Symbolic Logic, Vol. 29, No. 4, December 1964, 214-216.

symbolic logic in Russia has been done by mathematicians. This unique background of the author is reflected throughout the present work and is, no doubt, a major reason why his conception of the philosophical problems of many-valued logic is so closely connected with the technical and mathematical side of the subject. English readers with very little knowledge of recent logical developments in Russia should find it a rewarding experience to follow Zinov'ev's philosophical approach, even if only a few really new concepts are found. In this connection, the reader will discover a more extensive and better than usual treatment of the interesting work of such logicians as Bočvar, Šestakov, and Jablonskij. It should not be inferred, however, that Zinov'ev focuses attention on Russian logic alone. On the contrary, many-valued logic is surveyed within a broad context of modern logical developments both in and out of Russia.

Łukasiewicz and Post are acknowledged to be the chief originators of many-valued logic. Emphasis is placed on the philosophical motivation of Łukasiewicz and the complete absence of such motivation in Post. It is claimed that analysis of the modal functor "possible" led Łukasiewicz to his three-valued logic, while Post was interested merely in a formal generalization of two-valued logic. "The current of ideas of intuitionistic logic," with its rejection of the law of excluded middle, is interpreted as further stimulating the development of many-valued logic. Brouwer, Heyting, Kolmogorov, Glivenko, and Jaśkowski are taken as important representatives of this current. Other recognized sources of stimulation were such systems as Bočvar's three-valued logic for solving the classical paradoxes, the quantum logics (Birkhoff, von Neumann, Destouches-Février, Reichenbach), the circuit logics of Šestakov, and various systems of strict implication (Lewis, Ackermann, von Wright, Rosser, and this reviewer). No attention is given in this connection to such early forerunners of many-valued logic as Peirce and MacColl, but there is agreement with Łukasiewicz that Aristotle was a many-valued logician and that many-valued logics should be called non-Chrysippean rather than non-Aristotelian.

On the formal side, emphasis is placed on the truth-table development of many-valued logic, although a chapter is devoted to an exposition of the quantification theory of Rosser and the present reviewer. Zinov'ev feels that it is the more-than-two-valuedness which is the essence of many-valued logic. On the side of interpretation, this leads to the problem of defining many-valued truth-values and it is pointed out that this should not be confused with the problem of finding applications for many-valued logical systems. This emphasis on more-than-two-valuedness makes it a bit surprising to find that Zinov'ev leans over backwards to show that there is no conflict between many-valued logic and traditional two-valued logic, especially the "laws of thought" of the latter. Of course, there is a sense in which this is true, but a deep desire for unification should not blind one to significant differences.

The reader should be alert to some rather obvious typographical errors.

ATWELL R. TURQUETTE

S. V. ÁBLONSKIJ. *Funkcional'nyé postroénid v k-značnoj logiké* (Functional constructions in k-valued logic). ***Sbornik statéj po matématičéskoj logiké i éé priložéniám k nékotorym voprosam kibérnétiki,*** Trudy Matématičéskogo Instituta iméni V. A. Stéklova, vol. 51, Izdatél'stvo Akadémii Nauk SSSR, Moscow 1958, pp. 5–142.

The paper under review contains an impressive collection of results on the composition theory of k-valued truth-functions, $k \geqq 2$. Many of the results are credited to A. V. Kuznécov. The author has given a clear and concise account of the topic. His presentation is self-contained and all proofs are carried out in detail. We shall first give the most important definitions. Let P_k, $k \geqq 2$, be the set of functions whose variables, finite in number, range over the set $E^k = \{0, 1, \ldots, k-1\}$ and whose values are elements of E^k. A subset P' of P_k is *complete* (with respect to P_k) if every member of P_k equals a (finite) composition of members of P'. (Here, as usual, renaming and identification of variables is allowed.) A subset P' of P_k is *closed* if every composition of elements of P' is included in P'. Finally, a closed subset P' of P_k is *precomplete* (with respect to P_k) if it is not complete but the addition to P' of any member of the set $P_k - P'$ yields a complete set. The notions of completeness and precompleteness are defined similarly with respect to closed subsets of P_k. The paper is divided into three chapters. In chapters 1 and 3, the sets P_2 and P_3, respectively, are discussed. Chapter 1 contains also an extensive survey of switching circuit theory. The chief purpose of this survey is apparently to indicate some of the applications of the composition theory.

The general theory concerning P_k is given in chapter 2. It is shown that, for each P_k, one may construct a finite family $\{M_i \mid 1 \leqq i \leqq s\}$ of closed subsets of P_k such that an arbitrary subset of P_k is complete if and only if it is not contained in any of the sets M_i. This general criterion is of no practical value because of the enormous number of steps needed in the construction of the sets M_i. For $k = 3$, one has to check through 2^{19683} sets. The author gives various other more practical completeness criteria. Of these we mention the following: For $k \geqq 3$, a subset of P_k is complete if it contains all one-place functions and, in addition, a function which depends essentially on at least two variables and assumes all k values. The long but clear proof of this result is based on an induction on the number k, a method surprisingly seldom successful in the study of k-valued truth-functions. It is an open problem in which smaller sets can be used to replace the set of all one-place functions in this criterion. The author shows that every closed proper subset of P_k can be extended to a precomplete set and that the number of precomplete subsets of P_k is finite. He also considers the problem of whether there are subsets P_∞ of P_k which are not finitely generated, i.e., there is no finite subset P of P_∞ such that every function in P_∞ equals a composition of functions in P. Several examples of such subsets P_∞ of P_k, $k \geqq 3$, have been given since 1958 when the paper under review was published. It remains an open problem whether or not there is a precomplete subset of P_k which is not finitely generated. In the last six sections of chapter 2, the author shows the precompleteness of some subsets of P_k. Every ordering relation $<_r$ for the elements of the basic set E^k induces a lattice ordering for the arguments of functions in P_k. The set M_r^k of functions monotonous with respect to this lattice ordering is precomplete. A function $f(x_1, \ldots, x_n)$ belongs to the set $T^k(E, s)$, $E \subset E^k$, if and only if for every family $\{D_i \mid 1 \leqq i \leqq n, D_i \subset E^k, \operatorname{card}(D_i) = s\}$ there is a subset D of E^k, $\operatorname{card}(D) = s$, such that the conditions $x_i \in E \cup D_i$, $1 \leqq i \leqq n$, imply the condition $f(x_1, \ldots, x_n) \in E \cup D$. The set $T^k(E, s)$ is precomplete if and only if either $E = \varnothing$, $1 < s = k - 1$, or $E \neq \varnothing$, $0 \leqq s < k - \operatorname{card}(E)$. A function belongs to the set $U^k(E_1, \ldots, E_s)$ if and only if the partition of E^k into disjoint sets $E_1, \ldots, E_s$ is invariant under this function. Each of the sets U is precomplete, provided $1 < s < k$. The set L^k consisting of all functions which can be expressed as linear polynomials modulo k is precomplete if and only if k is prime. The set $S^k_{s(x)}$ consisting of all functions self-conjugate under the permutation $s(x)$ on the elements of E^k is precomplete if and only if in the cyclic representation of $s(x)$ every factor is of equal prime order.

Of the contents of chapter 1 which is mainly of expository character, we want to mention the various methods developed for obtaining minimal disjunctive normal forms and the very short and elegant proof of the completeness criterion due to Post. In chapter 3, the author gives a general solution for the completeness problem of P_3. A subset of P_3 is complete if and only if it is not contained in any of the following eighteen precomplete sets: M_i^3 $(1 \leqq i \leqq 3$ where the values of i correspond to the three different orderings of the set E^3), $T^3(\varnothing, 2)$, $T^3(\{i\}, j)$ $(0 \leqq i \leqq 2, 0 \leqq j \leqq 1)$, $T^3(\{0, 1\}, 0)$, $T^3(\{0, 2\}, 0)$, $T^3(\{1, 2\}, 0)$, $U^3(\{0, 1\}, \{2\})$, $U^3(\{0, 2\}, \{1\})$, $U^3(\{1, 2\}, \{0\})$, L^3, S^3_{x+1}.

In addition to the list given at the end of the volume, the reviewer points out the following corrections: page 24, line 20, for "$y\bar{z}$", read "$\bar{y}z$"; page 72, line 26, for "$\beta^{h(x)}$", read "$\beta_i^{h(x)}$"; page 88, line 3, replace the first ")" by "("; page 88, last line, for "$\tilde{a}'$", read "$\tilde{a}^1$"; page 89, line 22, for "φ_i", read "φ_1"; page 91, line 13, for "$\tilde{\sigma}^0$", read "$\tilde{\delta}^0$"; page 97, line 12, for "$\breve{\beta}$", read "β"; several statements in section 19 are valid only if the cyclic representation of the permutation $s(x)$ consists of factors of equal prime order; page 137, last line, "+" should be in columns 6, 16, and 20.

ARTO SALOMAA

ALAN ROSE. *A formalisation of an $\aleph_0$-valued propositional calculus.* ***Proceedings of the Cambridge Philosophical Society,*** vol. 49 (1953), pp. 367–376.

FREDERIC B. FITCH. *An extensional variety of extended basic logic.* ***The journal of symbolic logic,*** vol. 23 (1958), pp. 13–21.

R. J. SOLOMONOFF. *Comments on Dr. S. Watanabe's paper.* ***Synthese,*** vol. 14 (1962), pp. 97–100. [Cf. XXIX 197(3).]

M. GOODALL. *Comments on Dr. S. Watanabe's paper.* Ibid., pp. 101–102. [Cf. XXIX 197(3).]

ERIC H. LENNEBERG. *The relationship of language to the formation of concepts.* Ibid., pp. 103–109.

W. A. VERLOREN VAN THEMAAT. *Formalized and artificial languages.* Ibid., pp. 320–326.

BÉLA JUHOS. *Wahrscheinlichkeitsschlüsse als syntaktische Schlußformen.* ***Actes du XIème Congrès International de Philosophie,*** Volume XIV, ***Volume complémentaire et communications du Colloque de Logique,*** North-Holland Publishing Company, Amsterdam 1953, and Éditions E. Nauwelaerts, Louvain 1953, pp. 105–108.

BÉLA V. JUHOS. *Wahrscheinlichkeitsschlüsse als syntaktische Schlußformen.* ***Studium generale,*** vol. 6 (1953), pp. 206–214.

BÉLA V. JUHOS. *Die neue Logik als Voraussetzung der wissenschaftlichen Erkenntnis.* Ibid., pp. 593–599.

RUDOLF CARNAP. *Meaning and synonymy in natural languages.* A reprint of XX 296. ***American philosophers at work, The philosophic scene in the United States,*** edited by Sidney Hook, Criterion Books, New York 1956, pp. 58–74.

MARY B. HESSE. Review of Jeffreys's ***Scientific inference*** (XXIX 194). ***Philosophy,*** vol. 34 (1959), pp. 66–68.

JERROLD J. KATZ. Review of Ziff's ***Semantic analysis*** (XXIX 193). ***Language,*** vol. 38 (1962), pp. 52–69.

WILLIAM P. ALSTON. *Ziff's Semantic analysis.* ***The journal of philosophy*** vol. 59 (1962), pp. 5–20.

A review of the same.

L. JONATHAN COHEN. Review of the same. ***Ratio*** (Oxford), vol. 4 no. 2 (1962), pp. 162–164.

Arto Salomaa
Mathematische Annaten by Alan Rose
Comptes rendus hebdomadaires des seances de l'Academie des Sciences
Zeitschrift fur mathematische logik und Grundlagen der Mathematik
The Journal of Symbolic Logic, Vol. 29, No. 3, September 1964, 144-145.

pressed in terms of the primitive one-place truth-functions of L, and, hence, (1) represents a disjunctive normal form. In the three-valued case, both functional and canonical completeness are preserved if the two transpositions given by the author are replaced by two permutations such that neither one of them is a power of the other.

ARTO SALOMAA

ALAN ROSE. *Self-dual binary and ternary connectives for m-valued propositional calculi.* **Mathematische Annalen,** vol. 143 (1961), pp. 448–462.

ALAN ROSE. *Sur certains calculs propositionnels à m valeurs ayant un seul foncteur primitif lequel constitue son propre dual.* **Comptes rendus hebdomadaires des séances de l'Académie des Sciences** (Paris), vol. 252 (1961), pp. 3176–3178.

ALAN ROSE. *Sur certains calculs propositionnels à m valeurs ayant deux foncteurs primitifs dont chacun est le dual de l'autre.* Ibid., pp. 3375–3376.

ALAN ROSE. *Sur un ensemble de foncteurs primitifs pour le calcul propositionnel à m valeurs lequel constitue son propre m-al.* Ibid., vol. 254 (1962), pp. 1897–1899.

ALAN ROSE. *Sur un ensemble complet de foncteurs primitifs indépendants pour le calcul propositionnel trivalent lequel constitue son propre trial.* Ibid., p. 2111.

ALAN ROSE. *A simplified self m-al set of primitive functors for the m-valued propositional calculus.* **Zeitschrift für mathematische Logik und Grundlagen der Mathematik,** vol. 8 (1962), pp. 257–266.

The author considers complete self-dual (and self m-al) sets of independent primitive connectives for the m-valued propositional calculus. All results obtained can be expressed in terms of m-valued truth-functions (i.e., functions of several variables ranging over the set $\{1, \ldots, m\}$ and with values in this set).

Assume that, for two given functions $f(x_1, \ldots, x_k)$ and $g(x_1, \ldots, x_k)$ and for a permutation $\varphi(x)$ on the elements $1, \ldots, m$, the equation

$$(1) \qquad \varphi(f(x_1, \ldots, x_k)) = g(\varphi(x_1), \ldots, \varphi(x_k))$$

holds, for all assignments of values for the variables $x_1, \ldots, x_k$. Then f is said to be the *conjugate* of g under the permutation $\varphi(x)$. A set of functions is *self-conjugate* under φ if the conjugate of any function in the set belongs to the set.

In particular, if $\varphi(x) = m + 1 - x$ (i.e., φ is the Łukasiewicz negation function) then the author calls f a *dual* of g. If $\varphi(x) = x + 1 \pmod m$ (i.e., φ is the Post negation function) then he calls f an *m-al of type* 1 of g (or, shortly, an m-al of g). Furthermore, m-als of *type i* are obtained by letting $\varphi(x) = x + i \pmod m$. Self-dual and self m-al sets are defined in the same way as self-conjugate sets above.

In the first paper, a self-dual set of independent generators for m-valued truth-functions, $m \geqq 2$, is constructed, the members of this set being one three-place function and two one-place functions. For this set, the dual of a formula is obtained by writing it backwards and interchanging the two connectives corresponding to the one-place functions. Another self-dual set of independent generators consisting of one two-place function and two one-place functions is constructed for all values of $m \geqq 3$. Some special considerations for the cases $m = 3$ and $m = 2$ are added.

A complete self-dual set of primitives consisting of one three-place function is given, for even values of $m \geqq 4$, in the second paper. It is also shown that no such set consisting of one function exists for odd values of m. In the third paper, a complete self-dual set consisting of two independent two-place functions is given, for odd values of $m \geqq 3$.

In the fourth paper, the author constructs, for values of $m \geqq 4$, a complete self m-al set of independent primitives consisting of one two-place and m one-place functions. As shown in the fifth paper, such a construction may be carried out also in the case $m = 3$. These results are improved in the sixth paper as follows.

Let $m = \prod_{i=1}^{n} a_i^{b_i}$. For $n \geqq 2$, the author exhibits a complete self m-al set of independent primitives consisting of one two-place function and $\sum_{i=1}^{n} a_i^{b_i}$ one-place functions. For $m \geqq 3$, he also constructs a complete self m-al set of independent primitives consisting of one two-place function and the constants $1, \ldots, m$.

In view of the many results obtained by the author, it is natural to ask whether analogous more general results could be obtained for the notion of conjugacy. So far only two particular permutations $\varphi(x)$ of degree m (namely, $\varphi(x) = m + 1 - x$ and $\varphi(x) = x + 1 \pmod{m}$) in the equation (1) have been considered. It is possible that results analogous to those of the author can be obtained for other permutations φ, perhaps even without specifying the permutation. The following problem is of some interest: given an integer $m \geqq 2$ and a permutation φ of degree m, to determine the smallest number r such that there is a complete self-conjugate (under φ) set of independent m-valued primitives consisting of one two-place function and r one-place functions. It seems obvious that the number r depends on the order of the permutation φ. ARTO SALOMAA

ARTO SALOMAA. ***On sequences of functions over an arbitrary domain.*** Annales Universitatis Turkuensis, Series AI, no. 62, Turun Yliopisto, Turku 1963, 5 pp.

This article may be regarded as a generalization into the denumerable domain of results on Sheffer functions. Assume F_A is the set of functions of finite Cartesian power (so-called "finite place functions") of a denumerable set A into A. The author proves that for every denumerable subset D_A of F_A, there exists a two-place function $f_D(x, y)$ in F_A (but not necessarily in D_A) which generates all functions of D_A. The method employed is reminiscent of XVII 204, using a result of Sierpinski concerning generation of arbitrary infinite sequences of integers instead of the analagous result for finite sequences of Picard. NORMAN M. MARTIN

BRUNO SCARPELLINI. *Die Nichtaxiomatisierbarkeit des unendlichwertigen Prädikatenkalküls von Łukasiewicz.* ***The journal of symbolic logic,*** vol. 27 no. 2 (for 1962, pub. 1963), pp. 159–170.

Scarpellini shows that the infinite-valued predicate calculus of first order, corresponding to the infinite-valued propositional calculus of Łukasiewicz, cannot be formalised by means of a finite number of axioms and rules of procedure. He shows that to each formula of the two-valued predicate calculus there corresponds a formula of the infinite-valued predicate calculus such that the former formula is satisfiable in a finite universe if and only if the latter is satisfiable in the set of truth-values x such that $0 < x \leqq 1$. Since the set of formulas of the two-valued calculus which are not satisfiable in any finite universe is not recursively enumerable it then follows, by means of an argument involving Gödel numbers, that the set of formulas of the infinite-valued calculus which always take the value 0 is not recursively enumerable. The required result then follows at once. ALAN ROSE

KURT SCHÜTTE. *Der Interpolationssatz der intuitionistischen Prädikatenlogik.* ***Mathematische Annalen,*** vol. 148 (1962), pp. 192–200.

The author obtains an extension of Craig's interpolation theorem (XXIV 243) by showing that the result also holds for intuitionistic predicate calculus. His proof gives rise to a new proof for the original (classical) case. He uses the cut-free formulation of intuitionistic predicate calculus which he developed in XVI 155 (the calculus obtained from K_3 by the omission of the redundant *Schnitt* rule).

The interpolation theorem is considered in a form which can be briefly summarized as follows. We suppose that if Γ is a sequence $C_1, \ldots, C_n$ of formulas and C is any formula then $\Gamma \rightarrow C$ shall denote $C_1 \rightarrow (C_2 \rightarrow \ldots \rightarrow (C_n \rightarrow C) \ldots)$. Suppose F is a

Arto Salomaa
”A general theory of *k*-place Stroke functions in 2-valued logic”
by A. R. Turquette
The Journal of Symbolic Logic, Vol. 29, No. 3, September 1964, 143.

A. R. Turquette. *A general theory of k-place stroke functions in 2-valued logic.* ***Proceedings of the American Mathematical Society,*** vol. 13 (1962), pp. 822–824.

Using the results of Post (VI 114), the author presents a general method of constructing all two-valued k-place stroke functions. They are $2^{2^k-2} - 2^{2^{k-1}-1}$ in number. The number of k-place self-dual Post δ-functions equals $2^{2^{k-1}-1}$.

The same results can be obtained also by applying the theory of precomplete sets developed by Kuznécov and Áblonskij (e.g., cf. Áblonskij, ***Trudy Matématičéskogo Instituta Akadémii Nauk SSSR iméni V. A. Stéklova,*** vol. 51 (1958), pp. 5–142). A function $f(x_1, \ldots, x_k)$ is a stroke function if and only if each of the following conditions is satisfied: $f(1, \ldots, 1) = 2$, $f(2, \ldots, 2) = 1$, and, for some $x_1, \ldots, x_k$,

$$f(\sim x_1, \ldots, \sim x_k) \neq \sim f(x_1, \ldots, x_k).$$

It seems to the reviewer that an analogous simple method of enumerating all k-place stroke functions could be given for the three-valued case because, in this case, all precomplete sets have been constructed. (Three-valued two-place stroke functions are well known.) On the other hand, very little is known of the precomplete sets in the general M-valued case. The existence of a simple device to calculate the number of M-valued k-place stroke functions does not seem likely. Arto Salomaa

William H. Jobe. *Functional completeness and canonical forms in many-valued logics.* ***The journal of symbolic logic,*** vol. 27 no. 4 (for 1962, pub. 1963), pp. 409–422.

The author calls an M-valued logic L with the truth-values $1, \ldots, M$ *canonically suitable* if $\min(x, y)$ and $\max(x, y)$ are generated by the truth-functions corresponding to the primitive connectives of L. A canonically suitable logic is *canonically complete* if every function $J^i_k(x)$ (where $J^i_k(i) = k$, and $J^i_k(x) = 1$ for $x \neq i$) can be expressed as a disjunctive normal form in terms of $\min(x, y)$, $\max(x, y)$, and the truth-functions corresponding to the primitive unary connectives of L. The Łukasiewicz-Słupecki system with the primitives C, N, and T is canonically incomplete because the truth-functions corresponding to N and T map the intermediate truth-value 2 into itself. The author shows that a three-valued system E with $\min(x, y)$ and the two transpositions (12) and (13) as primitive truth-functions is both functionally and canonically complete. He also presents a method of determining whether a formula is a tautology in E (i.e., assumes always the value 3) and a method of deciding whether two formulas of E are equivalent. Finally, he claims to have shown that in E there exists a procedure other than the truth-table method for recognizing tautologies and demonstrating the equivalence of formulas.

However, it seems to the reviewer that the method given by the author is essentially the same as the truth-table technique. The method consists of expanding the conjunction of the given formula F and the disjunction of each J_3 and of finding out whether the expansion contains each J_3. This happens if and only if F assumes always the value 3.

Many of the proofs of the paper can be shortened if more advanced results concerning functional completeness (e.g., cf. Áblonskij, ***Trudy Matématičéskogo Instituta Akadémii Nauk SSSR iméni V. A. Stéklova,*** vol. 51 (1958), pp. 5–142) are used. Then also the results proved by the author for a particular three-valued system E can be extended to M-valued systems L satisfying certain general conditions. For instance, if a doubly transitive group of permutations on the elements $1, \ldots, M$ is generated by the primitive one-place truth-functions of L then

$$(1) \qquad J^i_k(x) = \min(s_1(x), \ldots, s'_i(x), \ldots, s_M(x))$$

where $s_j(j) = 1$ and $s_j(i) = M$, for each $j \neq i$, and $s'_i(i) = k$. All functions s are ex-

Arto Salomaa
"A simple proof of functional completeness in many-valued logics
based on Lukasiewicz's C and N", by Robert E. Clay
"Note on Slupecki T-functions" by Robert E. Clay
The Journal of Symbolic Logic, Vol. 30, No. 1, March 1965, 105.

philosophical views, and may be recommended to philosophical readers on grounds quite other than its relevance to the field of this JOURNAL. It is listed here because of scattered passages which contain some informal discussion of the law of excluded middle and of the present situation in and various possibilities for modal logic (pp. 112–113, 116–117, 166–169).

The figure 7 which occurs on pages 168 and 169 is evidently a misprint or an editor's mistake for a negation sign. ALONZO CHURCH

ROBERT BLANCHÉ. ***Axiomatics.*** English translation of XXIII 438, by G. B. Keene. Monographs in modern logic. The Free Press of Glencoe, New York 1962, v + 65 pp.

To be more exact, a translation — checked by Prof. Blanché himself — of the first three chapters of his 1955 monograph, to wit: *The defects of Euclid's formalism, Early axiomatics*, and *Formalized axiomatics*. The reader may miss Chapter Four, which touched on the limitations of the axiomatic method (Gödel, Skolem, etc.). There is a bad mistranslation on page 5 where "Il n'y a plus, pour les théorèmes, de vérité séparée et pour ainsi dire atomique..." is rendered by "There remains, for the theorems, simply truth, separated and so to speak atomic." HUGUES LEBLANC

LAYMAN E. ALLEN. ***Wff 'n proof. The game of modern logic.*** Wff 'n proof, New Haven, Conn., 1962, viii + 224 pp.

LAYMAN E. ALLEN. ***Wff. The beginner's game of modern logic.*** Wff 'n proof, New Haven, Conn., 1963, 78 pp.

The "game of modern logic" is actually a series of games concerning the propositional calculus. According to the introduction, "the first few games are quite simple and have been mastered by children as young as six, while the final games are sufficiently complex to be challenging and interesting to university teachers of mathematical logic." An earlier 1961 version of ***Wff 'n proof*** consisted of twenty-four games. The present revised version contains twenty-one games, the first two of which are concerned with constructing well-formed formulas in the Polish notation of Łukasiewicz, while the final nineteen involve the construction of proofs using Fitch's method of subordinate proofs. ***Wff*** is a shortened beginner's manual containing only the first two games. F. C. OGLESBY

ROBERT E. CLAY. *A simple proof of functional completeness in many-valued logics based on Łukasiewicz's C and N.* **Notre Dame journal of formal logic,** vol. 3 (1962), pp. 114–117.

ROBERT E. CLAY. *Note on Słupecki T-functions.* ***The journal of symbolic logic,*** vol. 27 no. 1 (for 1962, pub. 1963), pp. 53–54.

The first paper contains a detailed proof, based upon successive functional constructions, of the following fact: If the constants $i_1, \ldots, i_m$ are added to the Łukasiewicz $(n+1)$-valued propositional calculus with the truth-values $0, 1, \ldots, n$ and the primitives C and N, then the resulting system is functionally complete exactly in case the greatest common divisor $(n, i_1, \ldots, i_m) = 1$. The second paper gives another formulation of this result, the truth-values being denoted by $1, \ldots, n+1$. ARTO SALOMAA

ROBERT E. CLAY. *A standard form for Łukasiewicz many-valued logics.* ***Notre Dame journal of formal logic,*** vol. 4 (1963), pp. 59–66.

Consider functions of several variables ranging over the set of integers. For a given natural number n, let M_n be the smallest set of functions which is closed with respect to composition and contains the constant function n and the two binary functions $x - y$ and $\max(x, y)$. The truncation $f^T(\bar{x}_k)$ of a function $f(\bar{x}_k)$ belonging to the set

Arto Salomaa
”A standard form for Lukasiewicz many-valued logics”
by Robert E. Clay
The Journal of Symbolic Logic, Vol. 30, No. 1, March 1965, 105-106.

philosophical views, and may be recommended to philosophical readers on grounds quite other than its relevance to the field of this JOURNAL. It is listed here because of scattered passages which contain some informal discussion of the law of excluded middle and of the present situation in and various possibilities for modal logic (pp. 112–113, 116–117, 166–169).

The figure 7 which occurs on pages 168 and 169 is evidently a misprint or an editor's mistake for a negation sign. ALONZO CHURCH

ROBERT BLANCHÉ. ***Axiomatics.*** English translation of XXIII 438, by G. B. Keene. Monographs in modern logic. The Free Press of Glencoe, New York 1962, v + 65 pp.

To be more exact, a translation — checked by Prof. Blanché himself — of the first three chapters of his 1955 monograph, to wit: *The defects of Euclid's formalism*, *Early axiomatics*, and *Formalized axiomatics*. The reader may miss Chapter Four, which touched on the limitations of the axiomatic method (Gödel, Skolem, etc.). There is a bad mistranslation on page 5 where "Il n'y a plus, pour les théorèmes, de vérité séparée et pour ainsi dire atomique..." is rendered by "There remains, for the theorems, simply truth, separated and so to speak atomic." HUGUES LEBLANC

LAYMAN E. ALLEN. ***Wff 'n proof. The game of modern logic.*** Wff 'n proof, New Haven, Conn., 1962, viii + 224 pp.

LAYMAN E. ALLEN. ***Wff. The beginner's game of modern logic.*** Wff 'n proof, New Haven, Conn., 1963, 78 pp.

The "game of modern logic" is actually a series of games concerning the propositional calculus. According to the introduction, "the first few games are quite simple and have been mastered by children as young as six, while the final games are sufficiently complex to be challenging and interesting to university teachers of mathematical logic." An earlier 1961 version of ***Wff 'n proof*** consisted of twenty-four games. The present revised version contains twenty-one games, the first two of which are concerned with constructing well-formed formulas in the Polish notation of Łukasiewicz, while the final nineteen involve the construction of proofs using Fitch's method of subordinate proofs. ***Wff*** is a shortened beginner's manual containing only the first two games. F. C. OGLESBY

ROBERT E. CLAY. *A simple proof of functional completeness in many-valued logics based on Łukasiewicz's C and N.* ***Notre Dame journal of formal logic,*** vol. 3 (1962), pp. 114–117.

ROBERT E. CLAY. *Note on Słupecki T-functions.* ***The journal of symbolic logic,*** vol. 27 no. 1 (for 1962, pub. 1963), pp. 53–54.

The first paper contains a detailed proof, based upon successive functional constructions, of the following fact: If the constants $i_1, \ldots, i_m$ are added to the Łukasiewicz $(n+1)$-valued propositional calculus with the truth-values $0, 1, \ldots, n$ and the primitives C and N, then the resulting system is functionally complete exactly in case the greatest common divisor $(n, i_1, \ldots, i_m) = 1$. The second paper gives another formulation of this result, the truth-values being denoted by $1, \ldots, n+1$. ARTO SALOMAA

ROBERT E. CLAY. *A standard form for Łukasiewicz many-valued logics.* ***Notre Dame journal of formal logic,*** vol. 4 (1963), pp. 59–66.

Consider functions of several variables ranging over the set of integers. For a given natural number n, let M_n be the smallest set of functions which is closed with respect to composition and contains the constant function n and the two binary functions $x - y$ and $\max(x, y)$. The truncation $f^T(\tilde{x}_k)$ of a function $f(\tilde{x}_k)$ belonging to the set

M_n is defined by the following equation

$$f^T(\tilde{x}_k) = \min(f(\tilde{x}_k) + |f(\tilde{x}_k)|, 1)\cdot\min(f(\tilde{x}_k), n)$$

where $(\tilde{x}_k) = (x_1, \ldots, x_k)$, $k \geqq 0$, and the variables $x_1, \ldots, x_k$ range over the set $\{0, 1, \ldots, n\}$. The author shows that the set of truth-functions generated by C and N in the Łukasiewicz $(n+1)$-valued propositional calculus with the truth-values $0, 1, \ldots, n$ is the same as the set of the truncations of the functions in M_n. The proof is based upon simple arithmetical facts. ARTO SALOMAA

ARTO SALOMAA. ***Some completeness criteria for sets of functions over a finite domain. II.*** Annales Universitatis Turkuensis, Series AI, no. 63. Turun Yliopisto, Turku 1963, 19 pp.

This is a continuation of XXVII 247(2). The latter contains sections 1 and 2 of the investigation and sections 3 and 4 constitute the present paper.

The author uses E_n to denote the set of all k-place n-valued functions (n finite and $n \geqq 2$). He calls a subset of E_n *complete* (or a *Sheffer set*) if its members can generate, by finite composition, all the members of E_n. Further, a k-place n-valued function is said to satisfy *Słupecki conditions* if "it depends essentially on at least two variables and assumes all n values." In section 1, the following theorem is proved:

THEOREM 1. Assume that $n \geqq 5$ and F is a subset of E_n containing the alternating group A_n and an arbitrary function $f(x_1, \ldots, x_k)$ satisfying Słupecki conditions. Then F is complete.

The present paper investigates sets E_n where n is prime and E_p is used to denote such sets. In particular, stronger completeness criteria are obtained for E_p than for E_n. A function $f(x_1, \ldots, x_k)$ is now said to satisfy *strong Słupecki conditions* if "it depends essentially on at least two variables and, furthermore, there are numbers i and u_j, $j = 1, \ldots, i-1, i+1, \ldots, k$, such that $f_1(x_i) = f(u_1, \ldots, u_{i-1}, x_i, u_{i+1}, \ldots, u_k)$ is a permutation of the numbers $1, 2, \ldots, n$." The following theorem is proved:

THEOREM 3. Let F be a subset of E_p containing (1) a circular permutation $c(x)$, (2) a one-place function $g(x)$ which is not linear with respect to $c(x)$, (3) a function $f(x_1, \ldots, x_k)$ satisfying strong Słupecki conditions. Then F is complete.

This theorem is next applied to the theory of Sheffer functions of E_p. The following two alternative formulations give the chief results obtained:

THEOREM 4. A function $f(x_1, \ldots, x_k)$ belonging to E_p is a Sheffer function if (and only if) it generates a circular permutation $c(x)$ and a function $g(x)$ which is not a power of $c(x)$.

THEOREM 4′. A function $f(x_1, \ldots, x_k)$ belonging to E_p is a Sheffer function if (and only if) it generates a circular permutation $c(x)$ and is not self-conjugate under $c(x)$.

Given a function $f(x_1, \ldots, x_k)$, the function $f(x, \ldots, x)$ is called the *main diagonal* of f. Theorems 4 and 4′ enable the author to write a formula for the huge number of k-place Sheffer functions in E_p whose main diagonal is a circular permutation. With this number determined, the paper is concluded by formulating the following interesting problem:

"The question arises: what is the minimum number a of values of a k-place function f which have to be fixed in order to be sure that f always is a Sheffer function, no matter how the remaining $n^k - a$ values of f are defined?"

ATWELL R. TURQUETTE

M. J. GHAZALA (Gazalé). *Irredundant disjunctive and conjunctive forms of a Boolean function.* ***IBM journal of research and development,*** vol. 1 (1957), pp. 171–176.

T. RADO. *Comments on the presence function of Gazalé.* Ibid., vol. 6 (1962), pp. 268–269.

In XVIII 280 and XXI 328 Quine showed that any irredundant disjunctive normal

Arto Salomaa
”On an axiomatic system of the infinitely many-valued threshold logics”
”On the infinitely many-valued threshold logics and von Wright’s system M””
”A note on truth-value functions in the infinitely many-valued logics”
”On a simple axiomatic system of the infinitely many-valued logic based on $A, \to$”
”On an axiomatic system of the infinitely many-valued threshold predicate calculi”
”Truth-value stipulations for the von Wright’s system M' and the Heyting system”
by Akira Nakamura
The Journal of Symbolic Logic, Vol. 30, No. 3, September 1965, 374-375.

sense, but not adequate. As a result of Henkin's theorem (XXIII 362(2), §54), this calculus is adequate in the weaker sense called *quasi-adequate*.

In the first paper, Bayart shows that both calculi (S5, 2) and (S5, 1) are correct. The paper proceeds as follows: first the second-order pure modal functional calculus L is formulated, then for a proposition (sentence) of L, the notions *true*, *false*, *valid*, *realizable*, etc. are defined semantically.

A symbol Z (which operates as an abstraction symbol in place of the more usual λ) is introduced and some syntactical terms such as *abstractor*, *abstraction*, *primary* and *secondary parapropositions* are defined.

Following the method of sequents (*Sequenzen*) of Gentzen, the author defines (S5, 2), giving one axiom scheme and twenty-five deduction rules upon L.

The correctness of (S5, 2) and (S5, 1) is then established, by showing first that each axiom is valid and then for each rule that validity of premiss or premisses implies validity of the conclusion.

In the second paper, the author defines the notions *quasi-correct* and *quasi-adequate* as weakened notions of correctness and adequacy respectively.

And for (S5, 2) he establishes the quasi-correctness and quasi-adequacy. The method of the proof is quite analogous to that of the first paper. Furthermore he shows the non-adequacy of (S5, 2) as a direct result of the incompleteness theorem of Gödel.

The adequacy of (S5, 1) is also proved, by the standard method.

Kazuo Matsumoto

Akira Nakamura. *On an axiomatic system of the infinitely many-valued threshold logics.* ***Zeitschrift für mathematische Logik und Grundlagen der Mathematik,*** vol. 8 (1962), pp. 71–76.

Akira Nakamura. *On the infinitely many-valued threshold logics and von Wright's system M''.* Ibid., pp. 147–164.

Akira Nakamura. *A note on truth-value functions in the infinitely many-valued logics.* Ibid., vol. 9 (1963), pp. 141–144.

Akira Nakamura. *On a simple axiomatic system of the infinitely many-valued logic based on* $\wedge$, $\rightarrow$. Ibid., pp. 251–263.

Akira Nakamura. *On an axiomatic system of the infinitely many-valued threshold predicate calculi.* Ibid., pp. 321–239.

Akira Nakamura. *Truth-value stipulations for the von Wright system M' and the Heyting system.* Ibid., vol. 10 (1964), pp. 173–183.

The papers under review deal with infinitely many-valued propositional calculi except the fifth paper where an infinitely many-valued predicate calculus is considered. There are essential differences among the various systems presented, especially with respect to the truth-functions corresponding to implication. The first and the fifth papers are closely interrelated, and so are the third and the fourth as well as the second and the sixth papers. Some of the basic notions and ideas are credited to M. Itoh.

The operations characteristic for the system A_1 considered in the first paper are called "threshold operations" by the author. The set of truth-values equals the set R of all real numbers in the interval [0, 1], the value 1 being the only designated value. The primitive connectives of A_1 are disjunction with the truth-function $\max(x, y)$, conjunction with the truth-function $\min(x, y)$, and a set $\{T_\alpha \mid \alpha \in R\}$ of threshold operations with truth-functions $t_\alpha(x)$ where $t_\alpha(x) = 1$ for $x < \alpha$ and $t_\alpha(x) = 0$ for $x \geqq \alpha$. The author gives a complete axiomatization for the system A_1. The axiomatization consists of two parts: the former is identical with the axiomatization for the ordinary two-valued propositional calculus and the latter takes care of the threshold operations. The latter part consists of an infinite number (in fact, a continuum) of axiom schemata. The completeness proof is very simple: a reduction to the two-valued case and conjunctive normal forms are used. This reduction is possible because of the definition of the threshold operations and the definition of the implication: $P \rightarrow Q = (T_1P) \vee Q$. (Thus, the implication $P \rightarrow Q$ always assumes the value 1 when the value for P is less than 1.) The independence of the axiom schemata is not discussed.

It is easy to see that the same axiomatization is complete for any system $A_1(R')$ obtained from A_1 by replacing the set of truth-values R by some subset R' which contains the numbers 0 and 1. If R' is finite then the threshold operations can be expressed as disjunctions of the J-functions of Rosser and Turquette.

The system A_1 (where R' is denumerably infinite) is extended to an infinitely many-valued predicate calculus in the fifth paper. An axiomatization which follows the line of Rosser and Turquette is given. A completeness proof which uses Skolem normal forms is sketched.

The system A_2 presented in the third paper does not contain threshold operations. The set of truth-values is R where 1 is the only designated value and the primitive connectives are conjunction with the truth-function $\min(x, y)$ and implication with the truth-function $f(x, y)$, where $f(x, y) = 1$ for $x \leqq y$ and $f(x, y) = y$ for $x > y$. (Note that the implication of A_1 always assumes a designated value when the implication of A_2 does, but not conversely.) The decision problem of A_2 is solved in the third paper. For this purpose, a normal form for the well-formed formulas is introduced such that the validity of a formula can be decided by considering the constituents of the normal form. A complete axiomatization for A_2 is given in the fourth paper.

The threshold operations characteristic for the system A_3 considered in the second paper are different from those of A_1. The set of truth-values in A_3 is the Boolean lattice consisting of infinite sequences of 0's and 1's where the lattice operations are defined pointwise in the natural way. The sequence $(1, 1, 1, \ldots)$ is the only designated value. The primitive connectives are disjunction $\vee$ and negation $\neg$ whose truth-functions are the join and the complement of the lattice and, in addition, an infinite sequence of threshold operations T_i, $i = 1, 2, \ldots$, with truth-functions $t_i(x)$ where $t_i(x) = (0, 0, 0, \ldots)$ if the number of 1's in x is less than i and $t_i(x) = (1, 1, 1, \ldots)$ otherwise. (Note that threshold operations thus defined resemble those considered in automata theory.) A complete axiomatization for A_3 is given. As in connection with A_1, the axiomatization consists of a two-valued part and a part for the threshold operations. Implication is defined as in the two-valued case: $P \rightarrow Q = \neg P \vee Q$. (Note that, in A_3, $(T_iP) \rightarrow (T_jP)$ is assertable if $i \geqq j$. In A_1, $(T_iP) \rightarrow (T_jP)$ is assertable if $i \leqq j$.) It would be an interesting problem to establish an interconnection between A_1 and A_3. Let A_3' be the system with the primitive connectives $\vee$, $\neg$, and T_1. The axiomatization of A_3' results from that of A_3 by omitting superfluous axioms. The author shows that A_3' is equivalent to von Wright's system M'' in the sense that both systems contain the same provable formulas.

The approach of the sixth paper is converse to that of the other papers: the author begins with an axiomatic stipulation, namely, von Wright's system M' and constructs an equivalent truth-value stipulation. The latter is too complicated to be restated here. Using well-known interconnections between M' and the Heyting system, the author finally gives a truth-value stipulation for the latter.

The reader should be alert to some inaccuracies in the definitions as well as to some typographical errors. ARTO SALOMAA

BURTON DREBEN. *Relation of m-valued quantificational logic to 2-valued quantificational logic.* ***Summaries of talks presented at the Summer Institute for Symbolic Logic, Cornell University, 1957,*** 2nd edn., Communications Research Division, Institute for Defense Analyses, Princeton, N.J., 1960, pp. 303–304.

Arto Salomaa
”On the infinitely many-valued double-threshold logic” by Akira Nakamura
The Journal of Symbolic Logic, Vol. 31, No. 4, December 1966, 665.

(T) $CCQPCQR \equiv CCPQCPQ$ provable from Łukasiewicz's first three axioms (A1–A3) with modus ponens (R1)? This is done by assigning a four-valued truth-function to C, under which all theorems deducible from A1–A3, R1, always take value 1, while Łukasiewicz's axiom A4 does not. Since Meredith has shown that A4 is deducible from A1–A3, T, R1, it follows that T is not deducible from A1–A3, R1. The author indicates that the four truth-values used in the proof cannot be replaced by a smaller number.

LOUISE HAY

ATWELL R. TURQUETTE. *Independent axioms for infinite-valued logic.* ***The journal of symbolic logic,*** vol. 28 no. 3 (for 1963, pub. 1964), pp. 217–221.

In this paper, the author refers to Łukasiewicz's $\mathrm{L}_{\aleph_0}$, with the (dependent) fourth axiom deleted, as A^{λ}; A^{λ}_{4} is thus the negation axiom. He establishes minimality (i.e., independence of axioms and rules) by truth-table methods using three-valued logic and shows two-valued logic to be insufficient for this purpose. The author then considers the possibility of "simplifying" A^{λ} by a change of syntax, as follows: Let O be a statement constant with associated truth-value 0. Let $\mathrm{A}^{\alpha} = \mathrm{A}^{\lambda}$ with NP replaced by CPO, $\mathrm{A}^{\beta} = \mathrm{A}^{\lambda}$ with A^{λ}_{4} replaced by $CCCPOOP$, and $\mathrm{A}^{\gamma} = \mathrm{A}^{\lambda}$ with A^{λ}_{4} replaced by CPO. Using results of Rose and Rosser (XXIV 248), the author proves that A^{α}, A^{β}, and A' define the same class of theorems, and that all theorems of A^{λ} are expressible and provable in A^{α}, A^{β}, and A^{γ} (though not conversely; this fact is merely stated in a footnote, and could perhaps have been expanded upon). Of the four systems, A^{λ} thus appears to be the "simplest" axiomatization of $\mathrm{L}_{\aleph_0}$. The author also shows that four- and three-valued logic respectively are needed to establish the minimality of A^{β} and A^{γ}, in spite of the equivalence of the systems.

LOUISE HAY

AKIRA NAKAMURA. *On the infinitely many-valued double-threshold logic.* ***Zeitschrift für mathematische Logik und Grundlagen der Mathematik,*** vol. 11 (1965), pp. 93–101.

AKIRA NAKAMURA. *On a certain system of modal logic.* Ibid., pp. 203–207.

In the first paper, the author gives a modification of one of his earlier systems of infinitely many-valued logic. The modification is obtained by regarding infinite matrices of 0's and 1's (instead of infinite sequences of 0's and 1's) as truth-values. The truth-functions are defined analogously. In particular, there are two types of threshold operations, namely, those operating on rows and those operating on columns of the matrices. A decision method, which uses reduction to normal forms, is given for the validity of well-formed formulas. An interesting interconnection between the author's system and a certain dyadic predicate logic is established.

A formal system for a binary operation T, called the temporal valuation, is presented in the second paper. It is shown that this system, which is similar to a system considered by Prior, is an intermediate system between the von Wright systems M' and M''.

ARTO SALOMAA

A. N. PRIOR. *The theory of implication.* Ibid., vol. 9 (1963), pp. 1–6.

A. N. PRIOR. *The theory of implication: two corrections.* Ibid., vol. 11 (1965), pp. 381–382.

BOLESŁAW SOBOCIŃSKI. *A note on Prior's systems in "The theory of deduction."* ***Notre Dame journal of formal logic,*** vol. 5 no. 2 (1964), pp. 139–140.

This group of papers has to do with delicate questions concerning syntactical formulations of the Lewis systems S4 and S5, together with quantificational extensions thereof. In the first, Prior offers a formulation of S4 and S5 in terms of the primitives ⥽, $\supset$, and a constant impossible proposition 0. Necessity and negation are defined: $\Box A = (A ⥽ A) ⥽ A$, $\sim A = A \supset 0$; and other connectives are defined in the

Arto Salomaa
”Some problems of synthesis of digital automata” by V. M. Gluskov
”On an algorithm of synthesis of abstract automata” by V. M. Gluskov
The Journal of Symbolic Logic, Vol. 33, No. 4, December 1968, 629.

jedem Automaten $\mathfrak{A} \in \mathfrak{M}$ ein Programm $\mathfrak{P}_{\mathfrak{A}}$ für $M(\Delta, \mathfrak{J})$ gibt, so daß für alle $w \in \Theta(\Delta)$ (= Menge aller Wörter über Δ) gilt $\mathfrak{P}_{\mathfrak{A}}(w) = u_1$, falls $w \in T(\mathfrak{A})$, oder u_2, falls $w \notin T(\mathfrak{A})$, wobei u_1, u_2 zwei verschiedene Wörter aus $\Theta(\Delta)$ sind und $T(\mathfrak{A})$ das durch $\mathfrak{A}$ repräsentierte reguläre Ereignis bezeichnet.

In der ersten Arbeit wird zunächst gezeigt, daß sich die Klasse $\mathfrak{M}$ aller endlichen Automaten mit dem Eingabealphabet Δ in einer Einregister-Maschine $M(\Delta, \mathfrak{J}_1)$ simulieren läßt, deren Befehlsliste $\mathfrak{J}_1$ aus zwei sehr einfachen Typen von Befehlen besteht, die allerdings wesentlich von dem verwendeten Alphabet Δ abhängen. Daher wird in einem zweiten Theorem eine Simulierbarkeit aller endlichen Automaten über Δ in einer "arithmetischen" Einregister-Maschine $M(\{1\}, \mathfrak{J}_2)$ bei passender Kodierung der Wörter aus $\Theta(\Delta)$ in $\Theta(\{1\})$ gezeigt.

In der zweiten Arbeit wird bewiesen, daß auch die Klasse aller *real-time* Turing-Maschinen von Rabin (XXXI 657) in einer geeigneten Art von (unbeschränkten) Register-Maschinen simulierbar ist.

GÜNTER ASSER

O. P. KUZNÉCOV. *Ob odnom klassé régulárnyh sobytij* (On a class of regular events). ***Strukturnáa téoriá reléjnyh ustrojstv,*** Izdatél'stvo Akadémii Nauk, SSSR, Moscow, 1963, pp. 100–109.

The following synthesis problem of definite languages is considered: given finitely many definite languages $L_1, \cdots, L_n$, to construct a finite automaton A (without any specified final state set) such that, for any L_i, there is a set of states S_i in A which represents the language L_i in A (i.e., A with the final state set S_i accepts L_i). This problem is solved and an upper bound for the number of states in A is obtained by a simple indexing technique through the finite languages determining the languages L_i. The upper bound is much sharper than the bound obtained in case the languages L_i are regular. The result is illustrated by two examples. *Erratum.* Page 101, line 7 from the bottom: for "ba[2]," read "aba[2]."

ARTO SALOMAA

V. M. GLUŠKOV. *Nékotoryé problémy sintéza cifrovyh avtomatov* (Some problems of synthesis of digital automata). ***Žurnal vyčislitél'noj matématiki i matématičéskoj fiziki,*** vol. 1 (1961), pp. 371–411.

V. M. GLUŠKOV. *Ob odnom algoritmé sintéza abstraktnyh avtomatov* (*On an algorithm of synthesis of abstract automata*). ***Ukrainskij matématičéskij žurnal,*** vol. 12 (1960), pp. 147–156.

Since the essential contents of the second paper are covered by §4 of the first paper, the review is restricted to the first paper.

In §1 and §2, the author gives an introduction to the basic notions of automata and sequential machines, including infinite-state machines. Special emphasis is laid on the formalism of regular expressions. The author then proceeds to the analysis and synthesis problems of finite automata. The algorithms presented are similar in spirit (although somewhat different in form) to those given by McNaughton and Yamada in XXXII 390. The synthesis is also carried further than by McNaughton and Yamada in the sense that the result is in general better as regards the number of states and that it is applicable to the simultaneous synthesis of several languages.

The analysis procedure described in §3 is based on an inductive characterization of paths through k states in terms of paths through $k - 1$ states. An immediate consequence is that the star-height of a language representable in an n-state automaton (or sequential machine of Mealy or Moore type) cannot exceed n. In §4, the synthesis problem is considered in the following form: given finitely many regular expressions $R_1, \cdots, R_n$, to construct a finite automaton A (without any specified final state set) such that, for any R_i, there is a set of states S_i in A such that A with the final state set S_i accepts the language denoted by R_i. The synthesis algorithm is based on an indexing through the regular expressions R_i, which procedure gives the correct transitions of the automaton. An upper bound (which is an exponential function of the number of letters appearing in R_i) for the number of states in A is obtained. Finally, in §5 and §6, the author discusses the minimization technique based on experiments and a variant of the state assignment problem.

The reviewer would like to point out that the first paper (in somewhat shortened form) appears also in German translation as Appendices 1–4 of W. M. Gluschkow's XXXIII 634(2).

ARTO SALOMAA

Arto Salomaa
”On a class of regular events” by O. P. Kuznecov
The Journal of Symbolic Logic, Vol. 33, No. 4, December 1968, 629.

jedem Automaten $\mathfrak{A} \in \mathfrak{M}$ ein Programm $\mathfrak{P}_{\mathfrak{A}}$ für $M(\Delta, \mathfrak{J})$ gibt, so daß für alle $w \in \Theta(\Delta)$ (= Menge aller Wörter über Δ) gilt $\mathfrak{P}_{\mathfrak{A}}(w) = u_1$, falls $w \in T(\mathfrak{A})$, oder u_2, falls $w \notin T(\mathfrak{A})$, wobei u_1, u_2 zwei verschiedene Wörter aus $\Theta(\Delta)$ sind und $T(\mathfrak{A})$ das durch $\mathfrak{A}$ repräsentierte reguläre Ereignis bezeichnet.

In der ersten Arbeit wird zunächst gezeigt, daß sich die Klasse $\mathfrak{M}$ aller endlichen Automaten mit dem Eingabealphabet Δ in einer Einregister-Maschine $M(\Delta, \mathfrak{J}_1)$ simulieren läßt, deren Befehlsliste $\mathfrak{J}_1$ aus zwei sehr einfachen Typen von Befehlen besteht, die allerdings wesentlich von dem verwendeten Alphabet Δ abhängen. Daher wird in einem zweiten Theorem eine Simulierbarkeit aller endlichen Automaten über Δ in einer "arithmetischen" Einregister-Maschine $M(\{1\}, \mathfrak{J}_2)$ bei passender Kodierung der Wörter aus $\Theta(\Delta)$ in $\Theta(\{1\})$ gezeigt.

In der zweiten Arbeit wird bewiesen, daß auch die Klasse aller *real-time* Turing-Maschinen von Rabin (XXXI 657) in einer geeigneten Art von (unbeschränkten) Register-Maschinen simulierbar ist.

GÜNTER ASSER

O. P. KUZNÉCOV. *Ob odnom klassé régulárnyh sobytij* (On a class of regular events). ***Strukturnáa téoriá réléjnyh ustrojstv,*** Izdatél'stvo Akadémii Nauk, SSSR, Moscow, 1963, pp. 100–109.

The following synthesis problem of definite languages is considered: given finitely many definite languages $L_1, \cdots, L_n$, to construct a finite automaton A (without any specified final state set) such that, for any L_i, there is a set of states S_i in A which represents the language L_i in A (i.e., A with the final state set S_i accepts L_i). This problem is solved and an upper bound for the number of states in A is obtained by a simple indexing technique through the finite languages determining the languages L_i. The upper bound is much sharper than the bound obtained in case the languages L_i are regular. The result is illustrated by two examples. *Erratum.* Page 101, line 7 from the bottom: for "ba[2]," read "aba[2]."

ARTO SALOMAA

V. M. GLUŠKOV. *Nékotoryé problémy sintéza cifrovyh avtomatov* (Some problems of synthesis of digital automata). ***Žurnal vyčislitél'noj matématiki i matématičéskoj fiziki,*** vol. 1 (1961), pp. 371–411.

V. M. GLUŠKOV. *Ob odnom algoritmé sintéza abstraktnyh avtomatov* (*On an algorithm of synthesis of abstract automata*). ***Ukrainskij matématičéskij žurnal,*** vol. 12 (1960), pp. 147–156.

Since the essential contents of the second paper are covered by §4 of the first paper, the review is restricted to the first paper.

In §1 and §2, the author gives an introduction to the basic notions of automata and sequential machines, including infinite-state machines. Special emphasis is laid on the formalism of regular expressions. The author then proceeds to the analysis and synthesis problems of finite automata. The algorithms presented are similar in spirit (although somewhat different in form) to those given by McNaughton and Yamada in XXXII 390. The synthesis is also carried further than by McNaughton and Yamada in the sense that the result is in general better as regards the number of states and that it is applicable to the simultaneous synthesis of several languages.

The analysis procedure described in §3 is based on an inductive characterization of paths through k states in terms of paths through $k - 1$ states. An immediate consequence is that the star-height of a language representable in an n-state automaton (or sequential machine of Mealy or Moore type) cannot exceed n. In §4, the synthesis problem is considered in the following form: given finitely many regular expressions $R_1, \cdots, R_n$, to construct a finite automaton A (without any specified final state set) such that, for any R_i, there is a set of states S_i in A such that A with the final state set S_i accepts the language denoted by R_i. The synthesis algorithm is based on an indexing through the regular expressions R_i, which procedure gives the correct transitions of the automaton. An upper bound (which is an exponential function of the number of letters appearing in R_i) for the number of states in A is obtained. Finally, in §5 and §6, the author discusses the minimization technique based on experiments and a variant of the state assignment problem.

The reviewer would like to point out that the first paper (in somewhat shortened form) appears also in German translation as Appendices 1–4 of W. M. Gluschkow's XXXIII 634(2).

ARTO SALOMAA

Arto Salomaa
”O raspoznavanii zamšèamosti v rkursivnyh zykah” by A. V. Gladkij
”On the recognition of replaceability in recursive languages” by A. V. Gladkij,
(English translation of the paper by Gladkij by M. Greendlinger in
Amer. Math. Soc. translations, Ser. 2, Vol. 64, 1967, 81-96.)
The Journal of Symbolic Logic, Vol. 35, No. 2, June 1970, 340.

as follows. The language $\phi_x(L)$ consists of all words y such that, for all words z_1 and z_2, $z_1xz_2 \in L$ implies $z_1yz_2 \in L$. The language $\psi_x(L)$ is defined similarly, with "implies" replaced by "if and only if." (According to customary terminology, $\psi_x(L)$ consists of all words congruent to x with respect to the congruence induced by L.) For each recursive language L, the languages $\phi_x(L)$ and $\psi_x(L)$ are complements of recursively enumerable languages. Gladkij shows that there is a context-free language L such that among the sets $\phi_x(L)$ there is the complement of a recursively enumerable language with an arbitrary degree of unsolvability. This leads also to several other unsolvability results.

In his auxiliary constructions, Gladkij considers Turing machines whose external alphabet consists of the blank symbol a_0, one letter a_1, and a boundary marker a_2. The instructions of the machine include operations with the boundary marker. For instance, the instantaneous description $a_0\, a_2\, q_m\, a_t$ may yield directly the instantaneous description $a_2\, q_t\, a_0\, a_t$. Computations are defined in the usual fashion, with these additional instructions allowed. If the instantaneous descriptions are written one after the other, then a terminating computation may be considered as a word over the alphabet $\{a_0, a_1, a_2\}$. Thus, all terminating computations of a Turing-machine T constitute a language $C(T)$ over the alphabet mentioned. Gladkij shows that the complement of $C(T)$ (with respect to the set of non-empty words) is a linear context-free language and, furthermore, the generating grammar may be effectively constructed.

This machine construction is used also in the proof of the undecidability of inherent ambiguity. Moreover, the following auxiliary notion is introduced. A context-free grammar G determines a "unique decomposition" of the language $L(G)$ if the following condition is satisfied. Consider a word x in $L(G)$ and two subwords x_1 and x_2 of x such that both x_1 and x_2 are derived from a non-terminal in a derivation of x. Then either the words x_1 and x_2 do not intersect, or one of them is a subword of the other. An unambiguous grammar determines a unique decomposition. (The reader is referred to the aforementioned book by Ginsburg for a very clear treatment of the undecidability of inherent ambiguity, as well as related problems.)

The discussion above deals with the first two papers. The remaining three papers under review investigate the notion of a "configuration." A configuration of degree 1 with respect to a language L is a word X of length greater than 1 such that there is a letter x in the language $\psi_X(L)$. Assume that configurations of degree $i < r$ have been defined. Then a configuration of degree r with respect to L is a word X of length greater than 1 such that there is a letter x with the property that, for any words x_1 and x_2, (i) if $x_1xx_2 \in L$ then $x_1Xx_2 \in L$, and (ii) if $x_1Xx_2 \in L$ and contains no occurrences of configurations of degree $< r$ which intersect with but are not contained in the indicated occurrence of X, then $x_1xx_2 \in L$. Properties of configurations pertinent to characterization of language families and several questions of undecidability, as well as upper bounds for the degrees, are studied. Arto Salomaa

A. V. Gladkij. *O raspoznavanii zaméščaémosti v rékursivnyh ázykah.* Ibid., vol. 2 no. 3 (1963), pp. 5–22.

A. V. Gladkii. *On the recognition of replaceability in recursive languages.* English translation of the above by M. Greendlinger. ***American Mathematical Society translations,*** ser. 2 vol. 64 (1967), pp. 81–96.

Given a language L and a word x, the languages $\phi_x(L)$ and $\psi_x(L)$ are defined as in the preceding review. Furthermore, $\phi(L)$ is the set of ordered pairs (x, y) such that $x \in \phi_y(L)$. $\psi(L)$ is defined similarly. The author shows by an example that L may be recursive, with neither $\phi(L)$ nor $\psi(L)$ being recursively enumerable. Also the opposite situation is possible: $\phi(L)$ and $\psi(L)$ are recursive but L is not recursive. The examples are over an alphabet with at least two letters, but similar considerations hold for one-letter alphabets. There is no algorithm for constructing $\phi(L)$ or $\psi(L)$, given L. Finally, the author considers context-sensitive grammars. He shows that, for any given degree of unsolvability, there is a context-sensitive grammar G such that the language $g(\psi_xL(G))$ possesses the given degree of unsolvability. Here x is a fixed given word and $g(L)$ denotes the set of Gödel words of the words in L. Arto Salomaa

C. R. J. Clapham. *An embedding theorem for finitely generated groups.* ***Proceedings of the London Mathematical Society,*** ser. 3 vol. 17 (1967), pp. 419–430.

The author's introduction is an admirable summary: "Our aim is to show that any finitely

Arto Salomaa
”Algebraic and automata-theoretic properties of formal languages”
by Seymour Ginsburg
The Journal of Symbolic Logic, Vol. 41, No. 4, December 1976, 788-789.

the theory of word transformations constructed in the 1968 paper and some of the ideas used in the proofs of the sequels.

This, then, is a book which, at first sight, consists of miscellaneous papers thrown together, but turns out in the end to give a fair indication of both the unity and diversity of work done under the over-all heading "word problems." C. R. J. Clapham

Seymour Ginsburg. ***Algebraic and automata-theoretic properties of formal languages.*** Fundamental studies in computer science, vol. 2. North-Holland Publishing Company, Amsterdam and Oxford, and American Elsevier Publishing Company, Inc., New York, 1975, xii + 313 pp.

A formal language is a set of strings of letters from a finite alphabet. Finite specifications of languages either by generative devices (grammars) or accepting devices (automata) have been the object of an intensive study during the past twenty years. A device of some specific type, such as a finite automaton or a context-free grammar, determines a family of languages, consisting of all languages definable by devices of this type. Quite a few such language families have been introduced and investigated from various points of view. One important aspect in this has been the study of closure properties. It has turned out that many of the most important language families are closed under regular operations (union, catenation, and Kleene star or Kleene plus) and transductions (corresponding to the operations of homomorphism, inverse homomorphism, and intersection with regular languages).

In the late sixties, the author originated the theory of "abstract families of languages" (AFL's) as an attempt to unify the treatment of different language families. The work under review is the first comprehensive treatment of AFL theory in book form. By definition, a full AFL is a family of languages (with some trivial cases excluded) closed under regular operations and transductions. An AFL differs from a full AFL in that, as regards homomorphism, closure only under non-erasing homomorphisms is required. (Kleene star is used for full AFL's, Kleene plus for AFL's.) The book studies AFL's and related structures, the most important of which is a "trio." By definition, a full trio is a family of languages closed under transductions. The notion of a trio is obtained by the same modification as before.

Some terminological differences between the Ginsburg school and some other, notably French, authors should be pointed out. According to the latter authors, full AFL, AFL, full trio, trio, are called (in that order) FAL, faithful FAL, cone, faithful cone.

A brief description of the contents of the book follows. After two chapters with introduction and preliminaries, all basic results concerning trios and AFL's are established in Chapter 3. They include the characterization of transductions in terms of the three operations listed above, substitution, dependencies among the AFL operations, and taking the AFL and trio closure of an arbitrary family. This part also contains a proof of the (perhaps most interesting general AFL theory) theorem to the effect that the AFL closure of a family of languages is obtained by closing the family first with transductions and then the resulting family with regular operations. The next chapter deals with "abstract families of acceptors" (AFA's). Basically, an AFA is a family of automata with a fixed mode of reading and writing information on the storage. Various ways of "squeezing out" language families from AFA's are introduced, and one-to-one correspondences between these language families and (full) AFL's are obtained. Since AFL's may include languages not recursively enumerable, AFA's may also contain devices not effective in any sense. To this reviewer, the main reason for introducing acceptors in formal language theory is to provide intuition to understand certain phenomena. It is not clear that AFA's satisfy this requirement, as in fact they lead into very complicated considerations.

Chapter 5 deals with principal AFL's and trios, i.e., those generated with respect to the operations involved by a family consisting of one language only. (It turns out that a principal trio is always closed under union, i.e., is a semi-AFL in the terminology of the author.) Results concerning the representation of principal families in different ways, including several AFA characterizations, are given. The technique of proper ascending chains for showing non-principality is also discussed. Chapter 6 returns to the discussion of substitution: AFA representation, substitution closure, and the problem of how principality is preserved under substitution. The final chapter deals with trios and AFL's generated by families of bounded languages.

The whole book has a feature which certainly the readers of this Journal will find important:

the definitions and proofs are reliable, written in the thorough "Ginsburgian" style. This reviewer has given a course based on the book and could find very few errors of any kind, including printing errors. The motivation and background mateiial is scarce but to the point. It is always more pleasant to give more of the latter material during the lectures and rely on the proofs in a book, than the other way round. Unfortunately, most of the books in the area of automata and formal languages have very bad proofs.

On the other hand, the book is by no means easy to read and requires also previous knowledge concerning automata and languages. Some of the proofs are impossible to understand if one has not seen analogous proofs before. For instance, in the proof of the crucial Lemma 3.2.2, page 26, the notation used makes it very difficult to see that R_1 keeps track of the right sequence of states.

On the critical side, the following points should be mentioned. Although the proofs are correct, in many cases simpler and more polished arguments can be given. The author has not made full use of the decomposition theorem for the operator M, Theorem 3.2.1. For instance, the very long proof concerning closure under inverse homomorphism in the important Lemma 3.6.1 can be entirely avoided. The only thing needed is reference to Theorem 3.2.1 and the short sentence "For note that ..." in brackets in the middle of page 63. A use of the associativity law would simplify some arguments in the chapter dealing with substitution. It also seems to this reviewer that at least half of the arguments deal with difficulties caused only by the empty word. Sometimes it is very difficult to find out what is the main line of reasoning and what is only a side issue caused by the empty word. Sometimes a convention to the effect that languages differing by the empty word only are considered equal would have been very helpful.

The book covers a lot of ground, and additional material and references are given in the exercises. There is just one topic that I would have liked to see given more coverage: generators of language families, especially important families like context-free languages. Principality is discussed in detail but not the question of what are the requirements for a generator. How does a language family have to look if every AFL generator for it is also a trio generator for it? Contrary to his usual practice, the author states without proof some things regarding this topic that are basic even for context-free languages; e.g. the equation $h^{-1}(W_2) = U$ in Example 5.1.1 on page 139.

It should be apparent from what has been already said that, in spite of a few critical remarks, my over-all impression of the book is positive. The book is recommended for mathematicians, computer scientists, and linguists as a useful source and reference book about this special area of language theory. ARTO SALOMAA

FREDERIC B. FITCH. ***Elements of combinatory logic.*** Yale University Press, New Haven and London 1974, viii + 162 pp.

What is combinatory logic about? Fifty years after Schönfinkel proposed the combinators as the "building blocks" of mathematical logic, there is still no really convincing answer. Yet, like a natural phenomenon, the combinators keep reappearing, to be used and to be explained.

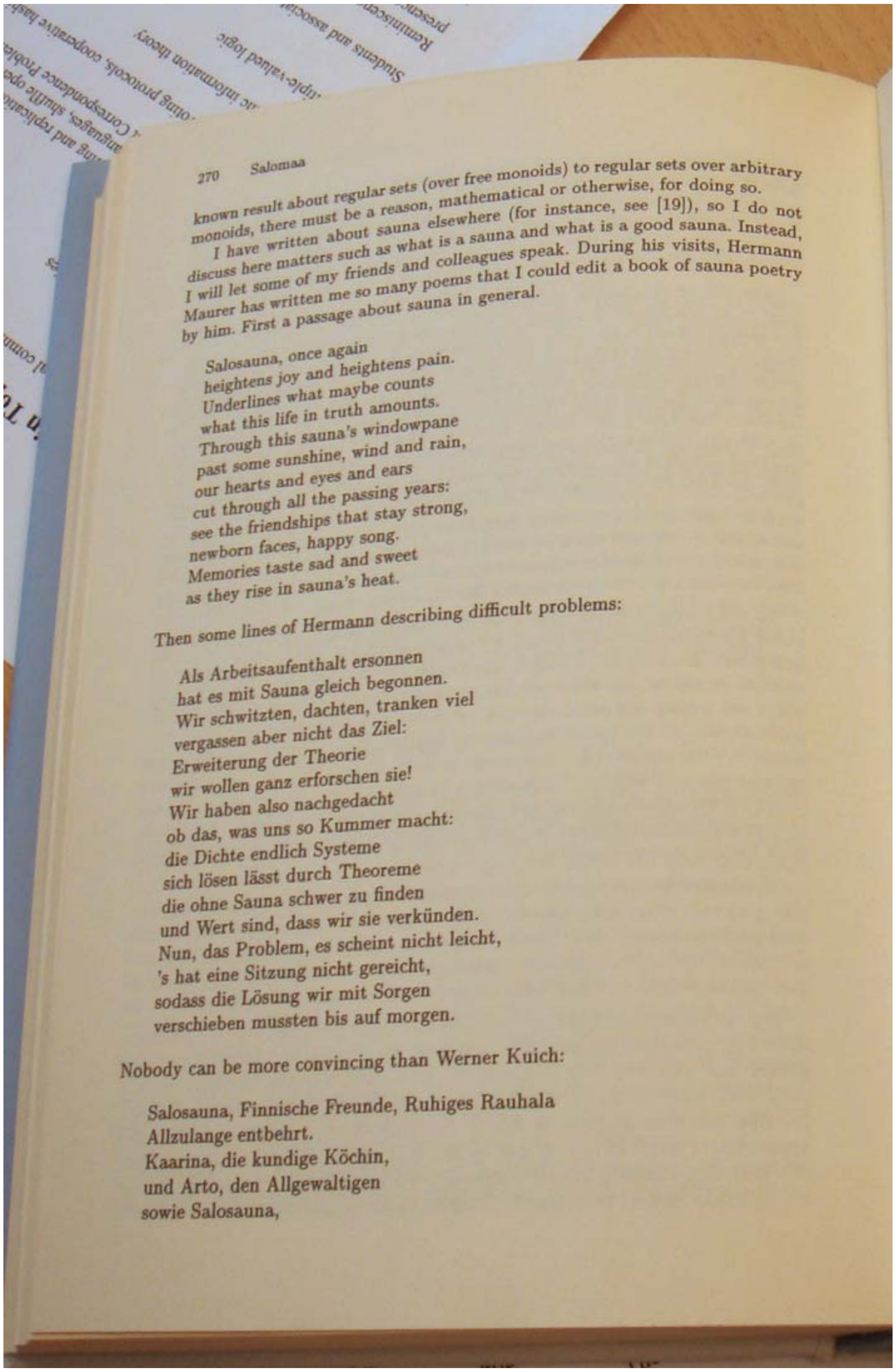
In the past few years, combinatory logic seems to have broken out of its age of exploration in which the main activity was to test the strength and consistency of various ways of adding logical or mathematical notions to the combinators. This type of research should and will continue, but the face of combinatory logic has been changed by Scott's discovery of models of combinatory logic in which the combinators are interpreted as genuine mathematical functions. There have also been some striking recent results not dependent on Scott's models, such as Böhm's theorem on the separability of combinators in normal form, Plotkin's proof of ω-incompleteness, and the proof by Sanchis and by Tait independently that in the combinatory theory of the primitive recursive functions of finite types, every term has a normal form.

The reader looking for a survey of the current status of combinatory logic, an introduction that also provides an indication of the main results and lines of research, will not, however, find it in Fitch's new book. Instead, and appropriately enough for one of the grand old men of combinatory logic (the 1975 Rome symposium on lambda-calculus and computer science theory was dedicated to Church, Curry, and Fitch), the present book is an exposition of some of Fitch's own thinking — the development of a particular system of combinatory logic.

From the preface: "The system of combinatory logic presented in this book is called the system Q. It contains not only the usual combinatory operators and sentential connectives, but also

8 Salosauna

Salomaa, A., ”What computer scientists should know about sauna?”,
European Association for Theoretical Computer Science Bulletin,
Vol. 15, 1981, 8-21.



270 Salomaa

known result about regular sets (over free monoids) to regular sets over arbitrary monoids, there must be a reason, mathematical or otherwise, for doing so.

I have written about sauna elsewhere (for instance, see [19]), so I do not discuss here matters such as what is a sauna and what is a good sauna. Instead, I will let some of my friends and colleagues speak. During his visits, Hermann Maurer has written me so many poems that I could edit a book of sauna poetry by him. First a passage about sauna in general.

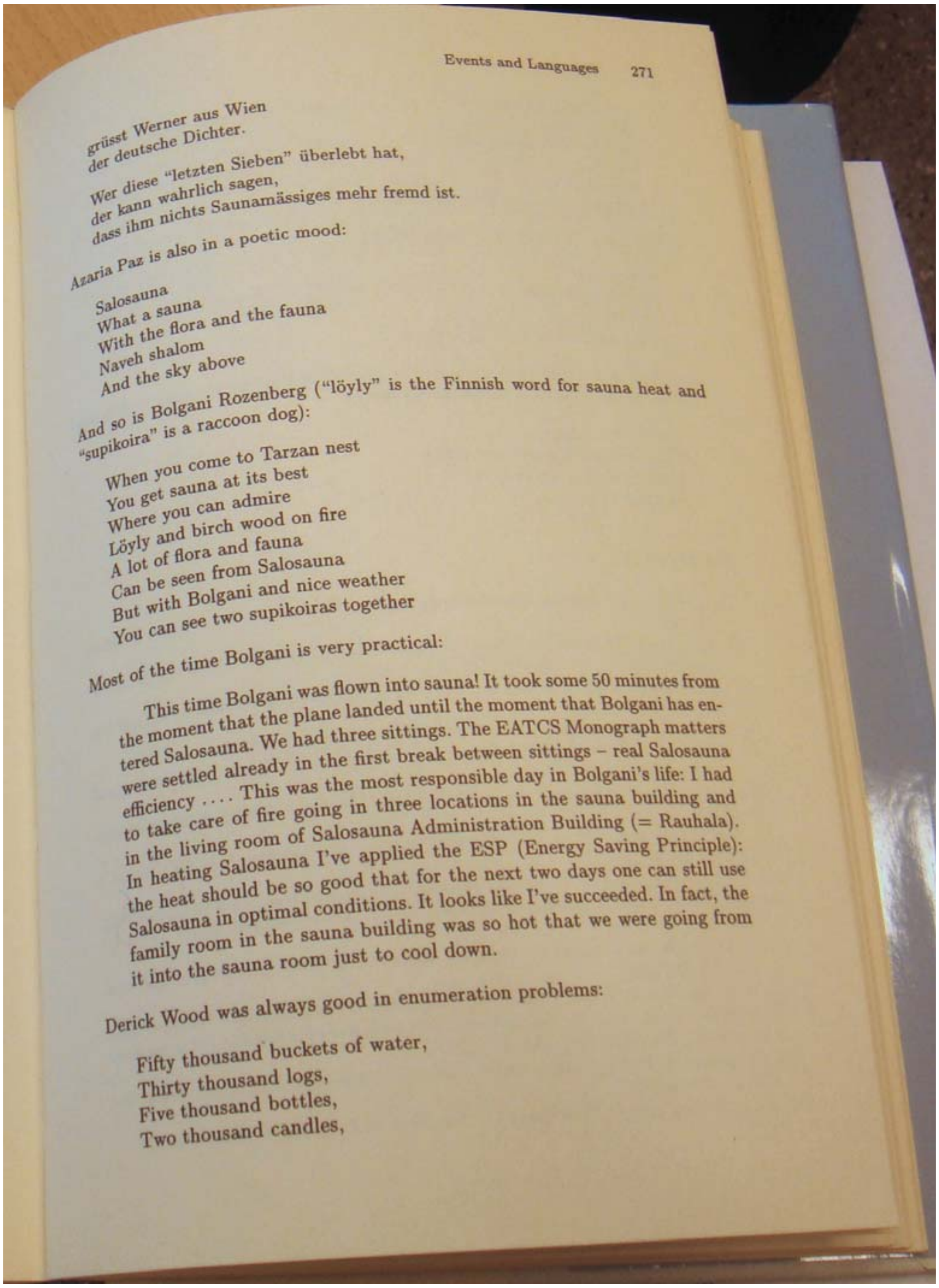
Salosauna, once again
heightens joy and heightens pain.
Underlines what maybe counts
what this life in truth amounts.
Through this sauna's windowpane
past some sunshine, wind and rain,
our hearts and eyes and ears
cut through all the passing years:
see the friendships that stay strong,
newborn faces, happy song.
Memories taste sad and sweet
as they rise in sauna's heat.

Then some lines of Hermann describing difficult problems:

Als Arbeitsaufenthalt ersonnen
hat es mit Sauna gleich begonnen.
Wir schwitzten, dachten, tranken viel
vergassen aber nicht das Ziel:
Erweiterung der Theorie
wir wollen ganz erforschen sie!
Wir haben also nachgedacht
ob das, was uns so Kummer macht:
die Dichte endlich Systeme
sich lösen lässt durch Theoreme
die ohne Sauna schwer zu finden
und Wert sind, dass wir sie verkünden.
Nun, das Problem, es scheint nicht leicht,
's hat eine Sitzung nicht gereicht,
sodass die Lösung wir mit Sorgen
verschieben mussten bis auf morgen.

Nobody can be more convincing than Werner Kuich:

Salosauna, Finnische Freunde, Ruhiges Rauhala
Allzulange entbehrt.
Kaarina, die kundige Köchin,
und Arto, den Allgewaltigen
sowie Salosauna,



grüsst Werner aus Wien
der deutsche Dichter.

Wer diese "letzten Sieben" überlebt hat,
der kann wahrlich sagen,
dass ihm nichts Saunamässiges mehr fremd ist.

Azaria Paz is also in a poetic mood:

Salosauna
What a sauna
With the flora and the fauna
Naveh shalom
And the sky above

And so is Bolgani Rozenberg ("löyly" is the Finnish word for sauna heat and "supikoira" is a raccoon dog):

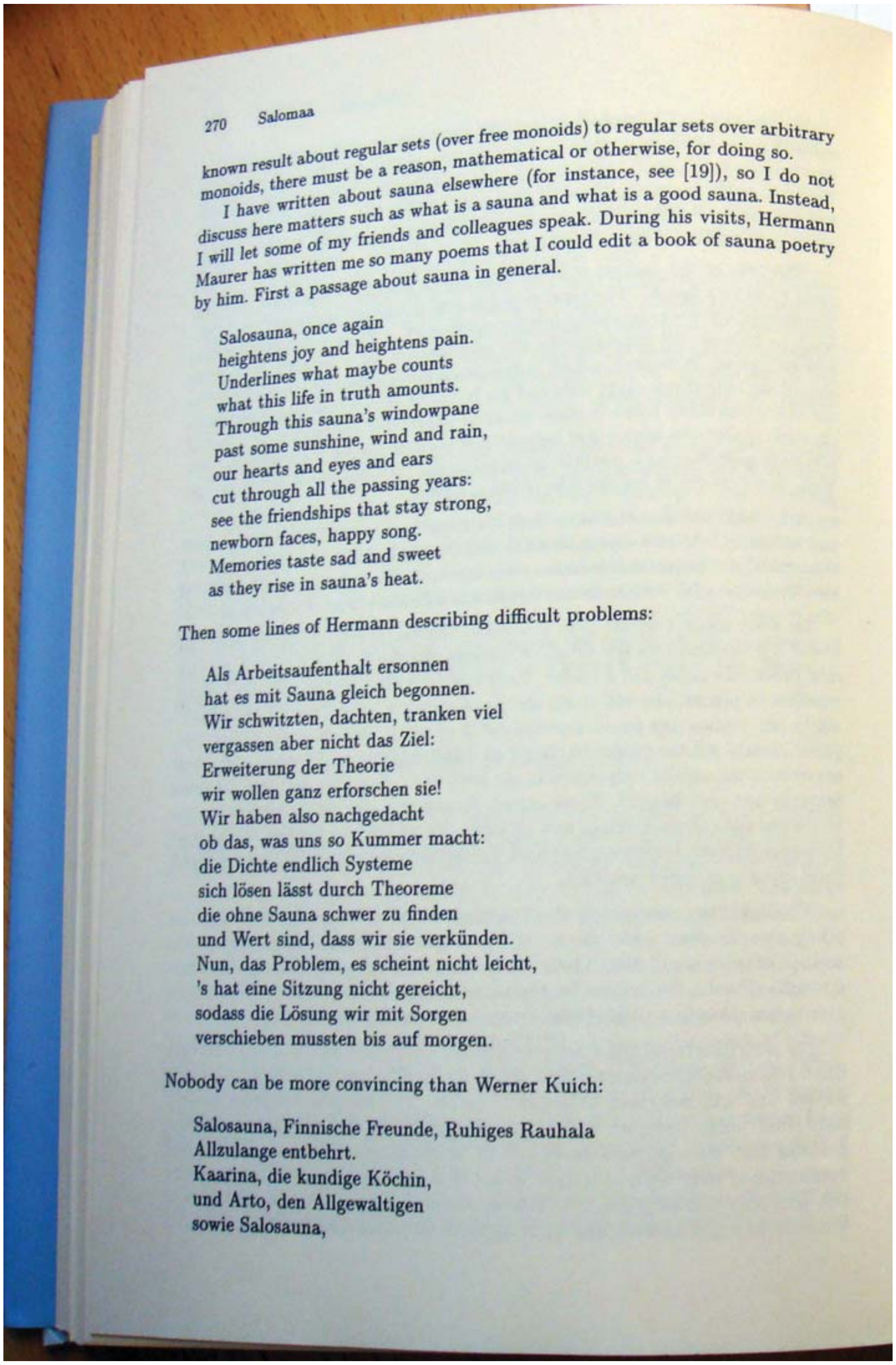
When you come to Tarzan nest
You get sauna at its best
Where you can admire
Löyly and birch wood on fire
A lot of flora and fauna
Can be seen from Salosauna
But with Bolgani and nice weather
You can see two supikoiras together

Most of the time Bolgani is very practical:

> This time Bolgani was flown into sauna! It took some 50 minutes from the moment that the plane landed until the moment that Bolgani has entered Salosauna. We had three sittings. The EATCS Monograph matters were settled already in the first break between sittings – real Salosauna efficiency .... This was the most responsible day in Bolgani's life: I had to take care of fire going in three locations in the sauna building and in the living room of Salosauna Administration Building (= Rauhala). In heating Salosauna I've applied the ESP (Energy Saving Principle): the heat should be so good that for the next two days one can still use Salosauna in optimal conditions. It looks like I've succeeded. In fact, the family room in the sauna building was so hot that we were going from it into the sauna room just to cool down.

Derick Wood was always good in enumeration problems:

Fifty thousand buckets of water,
Thirty thousand logs,
Five thousand bottles,
Two thousand candles,



known result about regular sets (over free monoids) to regular sets over arbitrary monoids, there must be a reason, mathematical or otherwise, for doing so.

I have written about sauna elsewhere (for instance, see [19]), so I do not discuss here matters such as what is a sauna and what is a good sauna. Instead, I will let some of my friends and colleagues speak. During his visits, Hermann Maurer has written me so many poems that I could edit a book of sauna poetry by him. First a passage about sauna in general.

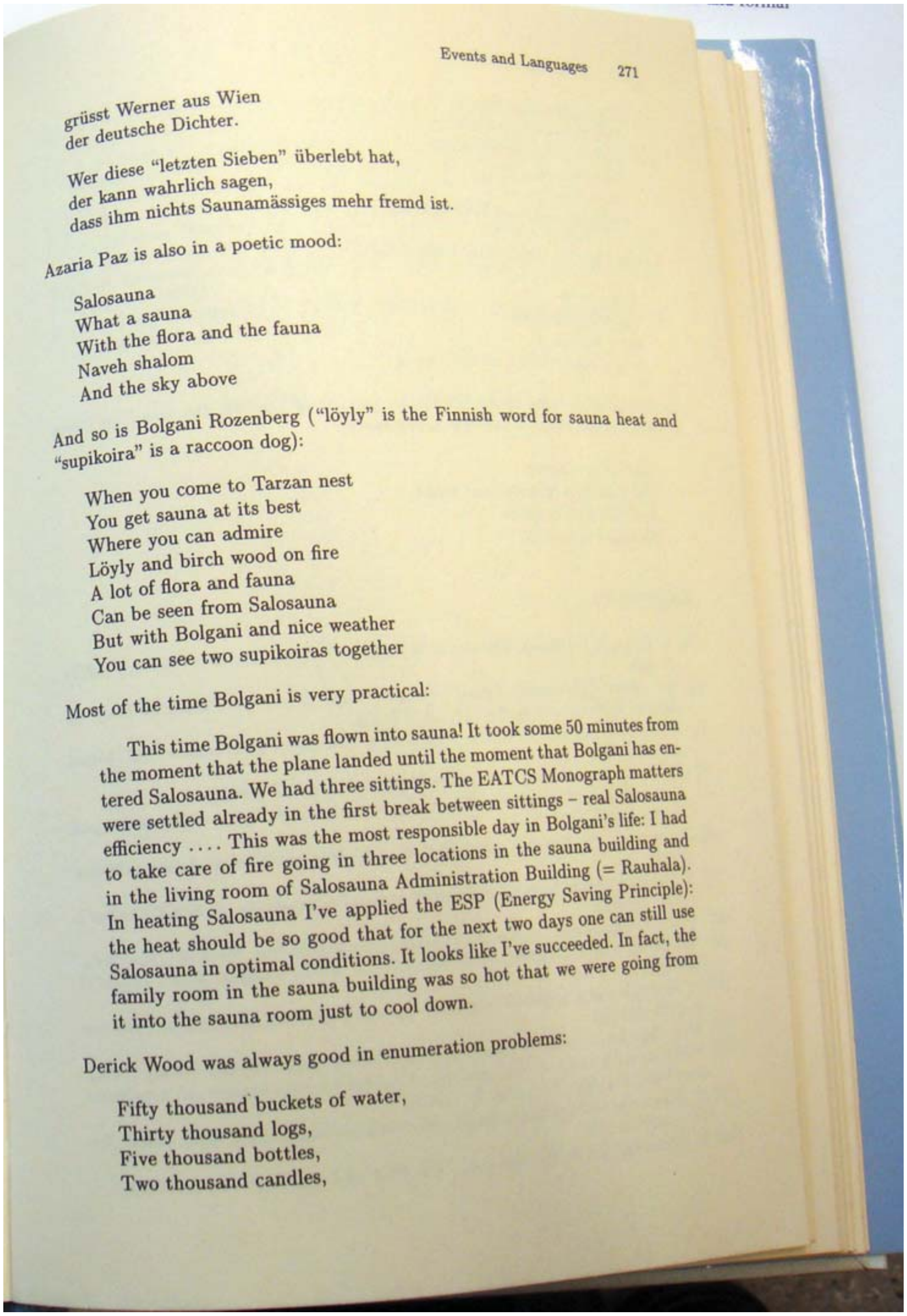
Salosauna, once again
heightens joy and heightens pain.
Underlines what maybe counts
what this life in truth amounts.
Through this sauna's windowpane
past some sunshine, wind and rain,
our hearts and eyes and ears
cut through all the passing years:
see the friendships that stay strong,
newborn faces, happy song.
Memories taste sad and sweet
as they rise in sauna's heat.

Then some lines of Hermann describing difficult problems:

Als Arbeitsaufenthalt ersonnen
hat es mit Sauna gleich begonnen.
Wir schwitzten, dachten, tranken viel
vergassen aber nicht das Ziel:
Erweiterung der Theorie
wir wollen ganz erforschen sie!
Wir haben also nachgedacht
ob das, was uns so Kummer macht:
die Dichte endlich Systeme
sich lösen lässt durch Theoreme
die ohne Sauna schwer zu finden
und Wert sind, dass wir sie verkünden.
Nun, das Problem, es scheint nicht leicht,
's hat eine Sitzung nicht gereicht,
sodass die Lösung wir mit Sorgen
verschieben mussten bis auf morgen.

Nobody can be more convincing than Werner Kuich:

Salosauna, Finnische Freunde, Ruhiges Rauhala
Allzulange entbehrt.
Kaarina, die kundige Köchin,
und Arto, den Allgewaltigen
sowie Salosauna,



grüsst Werner aus Wien
der deutsche Dichter.

Wer diese "letzten Sieben" überlebt hat,
der kann wahrlich sagen,
dass ihm nichts Saunamässiges mehr fremd ist.

Azaria Paz is also in a poetic mood:

Salosauna
What a sauna
With the flora and the fauna
Naveh shalom
And the sky above

And so is Bolgani Rozenberg ("löyly" is the Finnish word for sauna heat and "supikoira" is a raccoon dog):

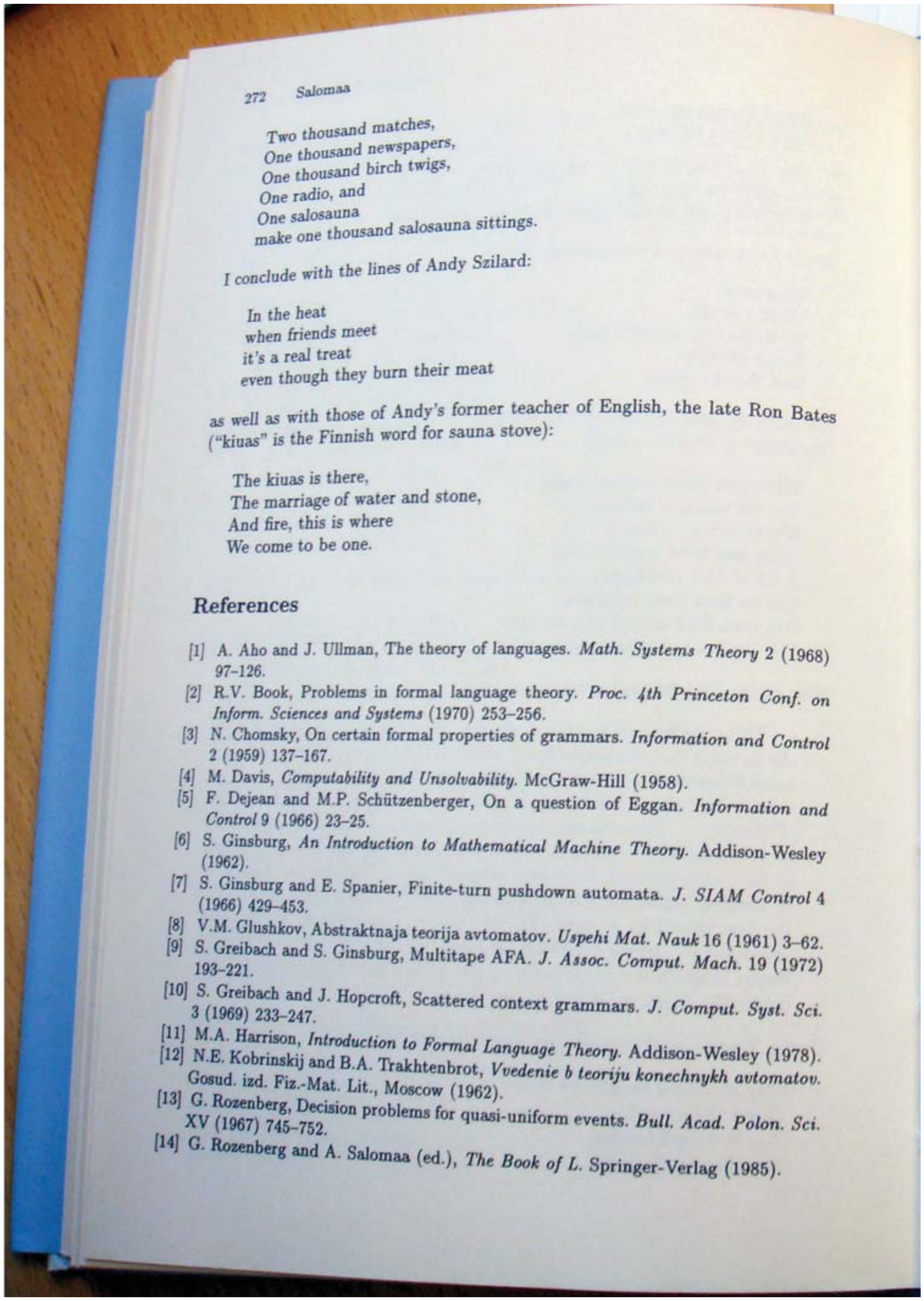
When you come to Tarzan nest
You get sauna at its best
Where you can admire
Löyly and birch wood on fire
A lot of flora and fauna
Can be seen from Salosauna
But with Bolgani and nice weather
You can see two supikoiras together

Most of the time Bolgani is very practical:

> This time Bolgani was flown into sauna! It took some 50 minutes from the moment that the plane landed until the moment that Bolgani has entered Salosauna. We had three sittings. The EATCS Monograph matters were settled already in the first break between sittings – real Salosauna efficiency .... This was the most responsible day in Bolgani's life: I had to take care of fire going in three locations in the sauna building and in the living room of Salosauna Administration Building (= Rauhala). In heating Salosauna I've applied the ESP (Energy Saving Principle): the heat should be so good that for the next two days one can still use Salosauna in optimal conditions. It looks like I've succeeded. In fact, the family room in the sauna building was so hot that we were going from it into the sauna room just to cool down.

Derick Wood was always good in enumeration problems:

Fifty thousand buckets of water,
Thirty thousand logs,
Five thousand bottles,
Two thousand candles,



Two thousand matches,
One thousand newspapers,
One thousand birch twigs,
One radio, and
One salosauna
make one thousand salosauna sittings.

I conclude with the lines of Andy Szilard:

In the heat
when friends meet
it's a real treat
even though they burn their meat

as well as with those of Andy's former teacher of English, the late Ron Bates ("kiuas" is the Finnish word for sauna stove):

The kiuas is there,
The marriage of water and stone,
And fire, this is where
We come to be one.

References

[1] A. Aho and J. Ullman, The theory of languages. *Math. Systems Theory* 2 (1968) 97–126.

[2] R.V. Book, Problems in formal language theory. *Proc. 4th Princeton Conf. on Inform. Sciences and Systems* (1970) 253–256.

[3] N. Chomsky, On certain formal properties of grammars. *Information and Control* 2 (1959) 137–167.

[4] M. Davis, *Computability and Unsolvability.* McGraw-Hill (1958).

[5] F. Dejean and M.P. Schützenberger, On a question of Eggan. *Information and Control* 9 (1966) 23–25.

[6] S. Ginsburg, *An Introduction to Mathematical Machine Theory.* Addison-Wesley (1962).

[7] S. Ginsburg and E. Spanier, Finite-turn pushdown automata. *J. SIAM Control* 4 (1966) 429–453.

[8] V.M. Glushkov, Abstraktnaja teorija avtomatov. *Uspehi Mat. Nauk* 16 (1961) 3–62.

[9] S. Greibach and S. Ginsburg, Multitape AFA. *J. Assoc. Comput. Mach.* 19 (1972) 193–221.

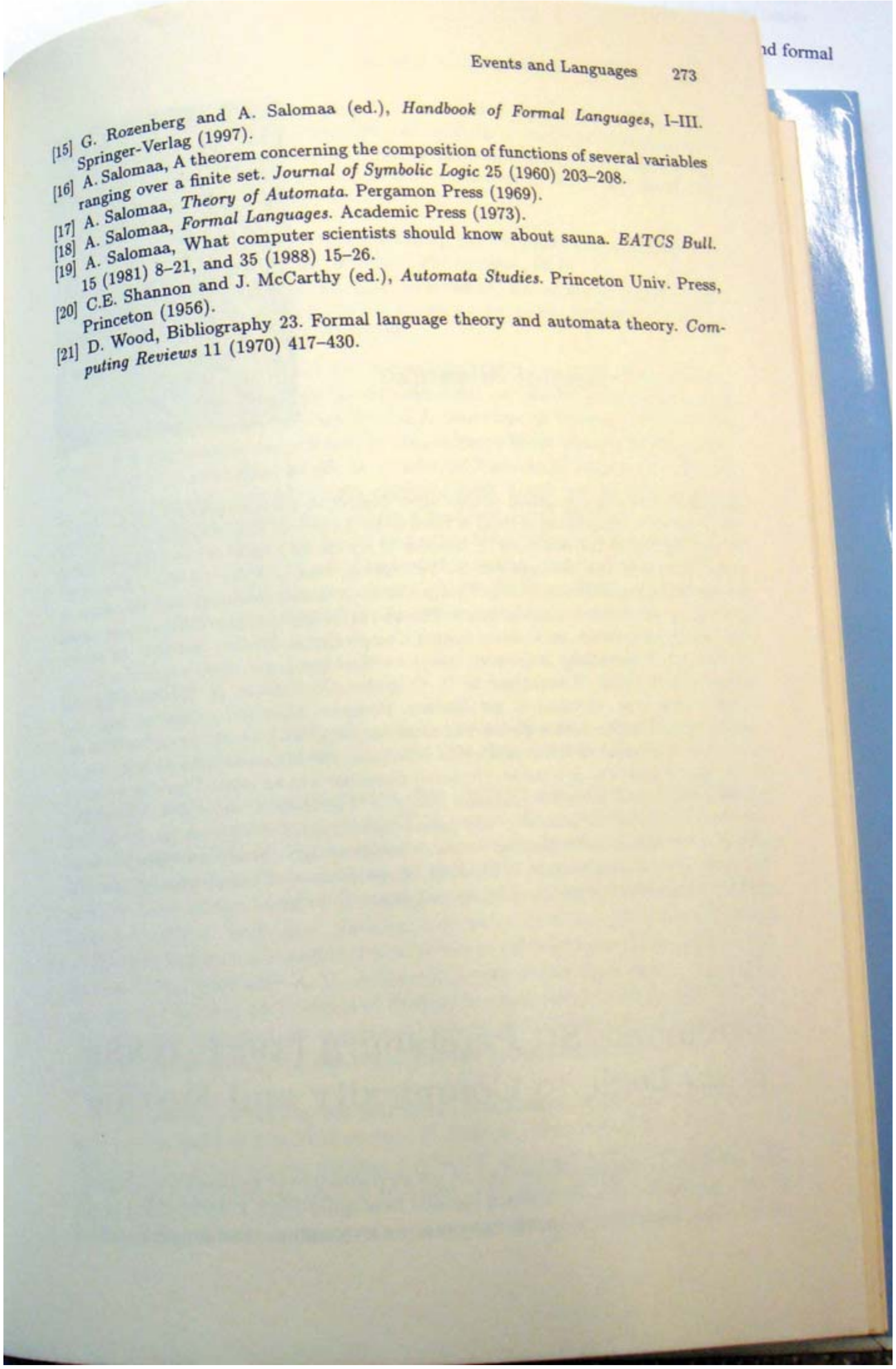
[10] S. Greibach and J. Hopcroft, Scattered context grammars. *J. Comput. Syst. Sci.* 3 (1969) 233–247.

[11] M.A. Harrison, *Introduction to Formal Language Theory.* Addison-Wesley (1978).

[12] N.E. Kobrinskij and B.A. Trakhtenbrot, *Vvedenie b teoriju konechnykh avtomatov.* Gosud. izd. Fiz.-Mat. Lit., Moscow (1962).

[13] G. Rozenberg, Decision problems for quasi-uniform events. *Bull. Acad. Polon. Sci.* XV (1967) 745–752.

[14] G. Rozenberg and A. Salomaa (ed.), *The Book of L.* Springer-Verlag (1985).



[15] G. Rozenberg and A. Salomaa (ed.), *Handbook of Formal Languages*, I–III. Springer-Verlag (1997).

[16] A. Salomaa, A theorem concerning the composition of functions of several variables ranging over a finite set. *Journal of Symbolic Logic* 25 (1960) 203–208.

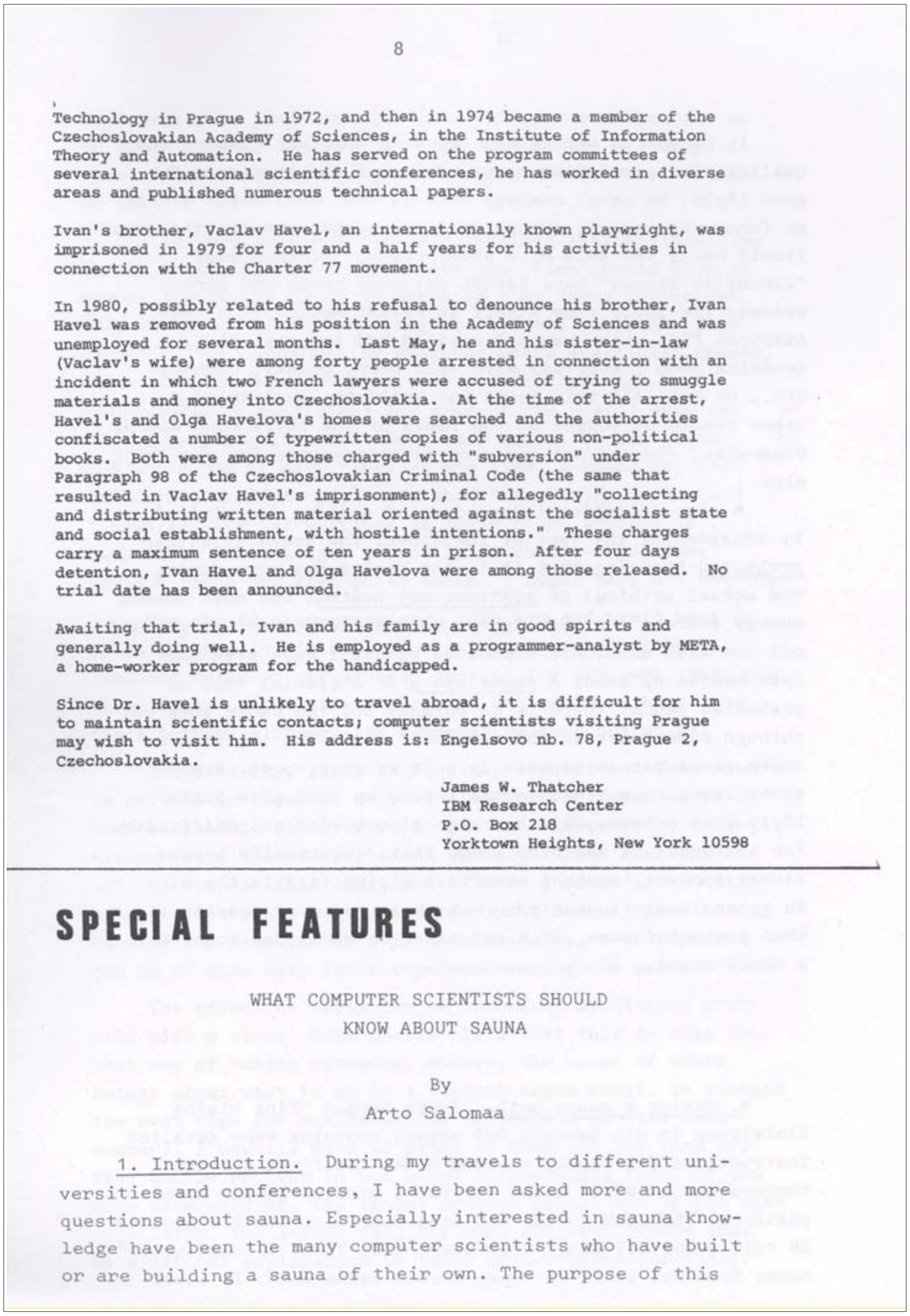
[17] A. Salomaa, *Theory of Automata*. Pergamon Press (1969).

[18] A. Salomaa, *Formal Languages*. Academic Press (1973).

[19] A. Salomaa, What computer scientists should know about sauna. *EATCS Bull.* 15 (1981) 8–21, and 35 (1988) 15–26.

[20] C.E. Shannon and J. McCarthy (ed.), *Automata Studies*. Princeton Univ. Press, Princeton (1956).

[21] D. Wood, Bibliography 23. Formal language theory and automata theory. *Computing Reviews* 11 (1970) 417–430.



Technology in Prague in 1972, and then in 1974 became a member of the Czechoslovakian Academy of Sciences, in the Institute of Information Theory and Automation. He has served on the program committees of several international scientific conferences, he has worked in diverse areas and published numerous technical papers.

Ivan's brother, Vaclav Havel, an internationally known playwright, was imprisoned in 1979 for four and a half years for his activities in connection with the Charter 77 movement.

In 1980, possibly related to his refusal to denounce his brother, Ivan Havel was removed from his position in the Academy of Sciences and was unemployed for several months. Last May, he and his sister-in-law (Vaclav's wife) were among forty people arrested in connection with an incident in which two French lawyers were accused of trying to smuggle materials and money into Czechoslovakia. At the time of the arrest, Havel's and Olga Havelova's homes were searched and the authorities confiscated a number of typewritten copies of various non-political books. Both were among those charged with "subversion" under Paragraph 98 of the Czechoslovakian Criminal Code (the same that resulted in Vaclav Havel's imprisonment), for allegedly "collecting and distributing written material oriented against the socialist state and social establishment, with hostile intentions." These charges carry a maximum sentence of ten years in prison. After four days detention, Ivan Havel and Olga Havelova were among those released. No trial date has been announced.

Awaiting that trial, Ivan and his family are in good spirits and generally doing well. He is employed as a programmer-analyst by META, a home-worker program for the handicapped.

Since Dr. Havel is unlikely to travel abroad, it is difficult for him to maintain scientific contacts; computer scientists visiting Prague may wish to visit him. His address is: Engelsovo nb. 78, Prague 2, Czechoslovakia.

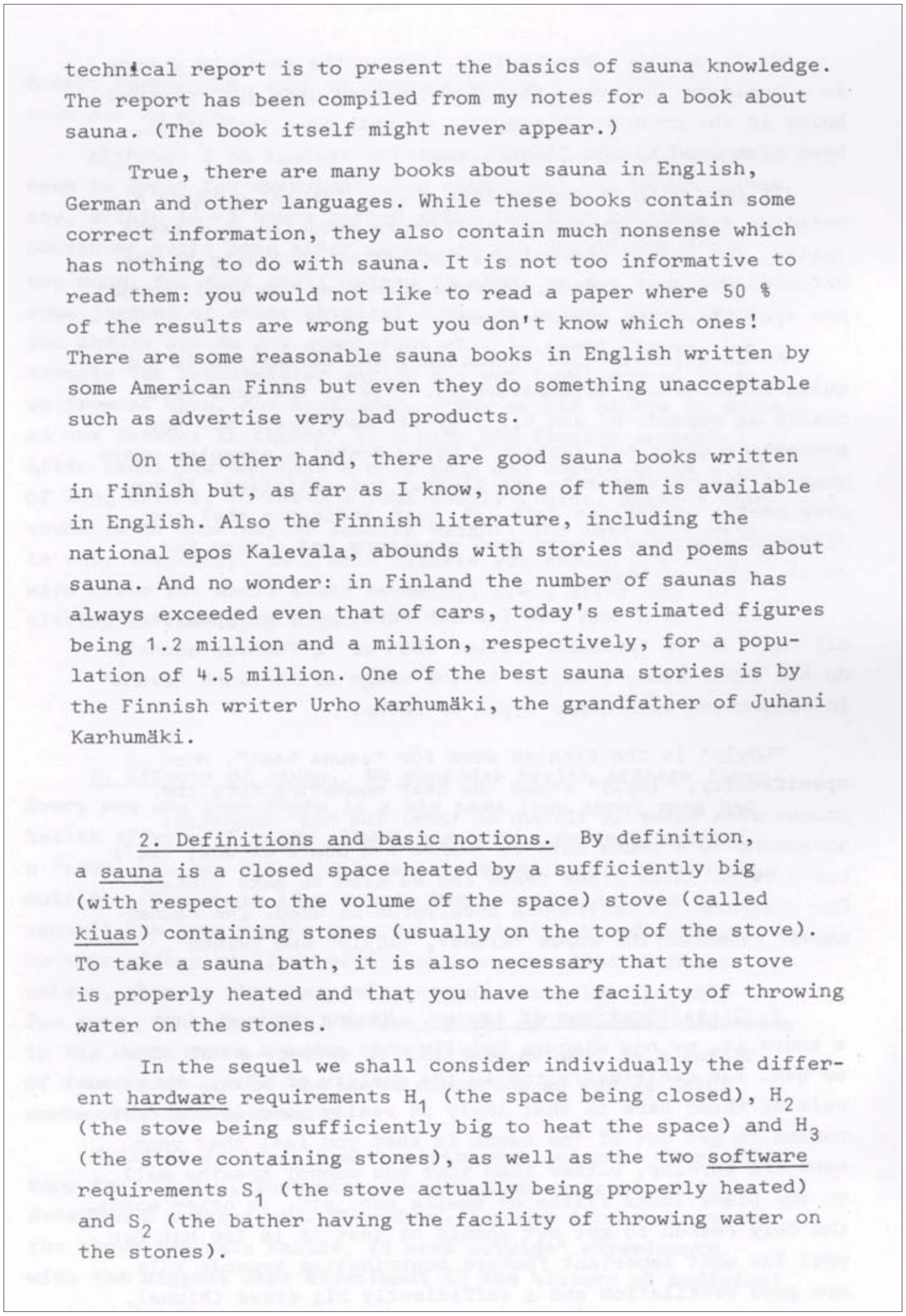
James W. Thatcher
IBM Research Center
P.O. Box 218
Yorktown Heights, New York 10598

SPECIAL FEATURES

WHAT COMPUTER SCIENTISTS SHOULD KNOW ABOUT SAUNA

By
Arto Salomaa

1. Introduction. During my travels to different universities and conferences, I have been asked more and more questions about sauna. Especially interested in sauna knowledge have been the many computer scientists who have built or are building a sauna of their own. The purpose of this



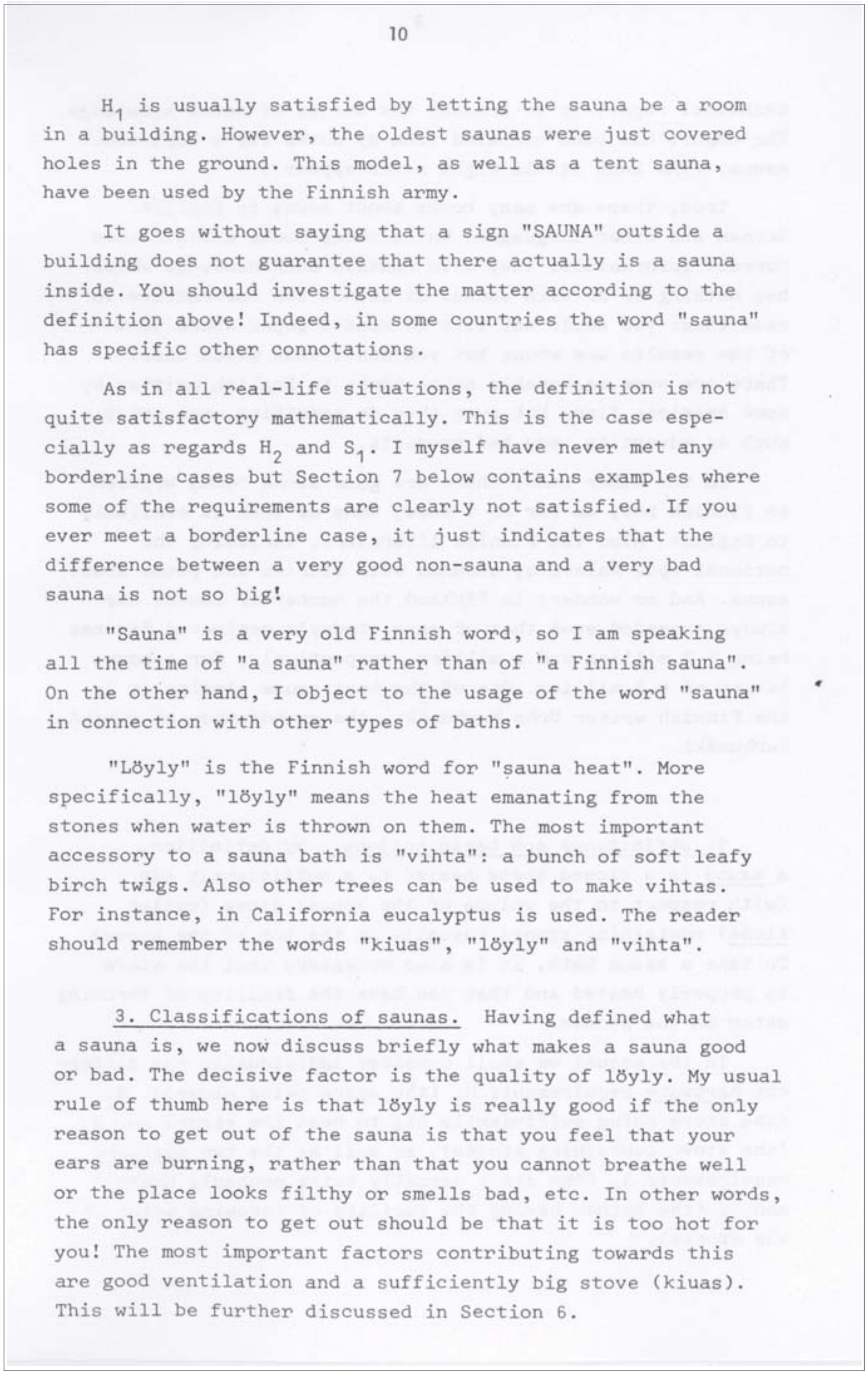
technical report is to present the basics of sauna knowledge. The report has been compiled from my notes for a book about sauna. (The book itself might never appear.)

True, there are many books about sauna in English, German and other languages. While these books contain some correct information, they also contain much nonsense which has nothing to do with sauna. It is not too informative to read them: you would not like to read a paper where 50 % of the results are wrong but you don't know which ones! There are some reasonable sauna books in English written by some American Finns but even they do something unacceptable such as advertise very bad products.

On the other hand, there are good sauna books written in Finnish but, as far as I know, none of them is available in English. Also the Finnish literature, including the national epos Kalevala, abounds with stories and poems about sauna. And no wonder: in Finland the number of saunas has always exceeded even that of cars, today's estimated figures being 1.2 million and a million, respectively, for a population of 4.5 million. One of the best sauna stories is by the Finnish writer Urho Karhumäki, the grandfather of Juhani Karhumäki.

2. Definitions and basic notions. By definition, a sauna is a closed space heated by a sufficiently big (with respect to the volume of the space) stove (called kiuas) containing stones (usually on the top of the stove). To take a sauna bath, it is also necessary that the stove is properly heated and that you have the facility of throwing water on the stones.

In the sequel we shall consider individually the different hardware requirements H_1 (the space being closed), H_2 (the stove being sufficiently big to heat the space) and H_3 (the stove containing stones), as well as the two software requirements S_1 (the stove actually being properly heated) and S_2 (the bather having the facility of throwing water on the stones).



H_1 is usually satisfied by letting the sauna be a room in a building. However, the oldest saunas were just covered holes in the ground. This model, as well as a tent sauna, have been used by the Finnish army.

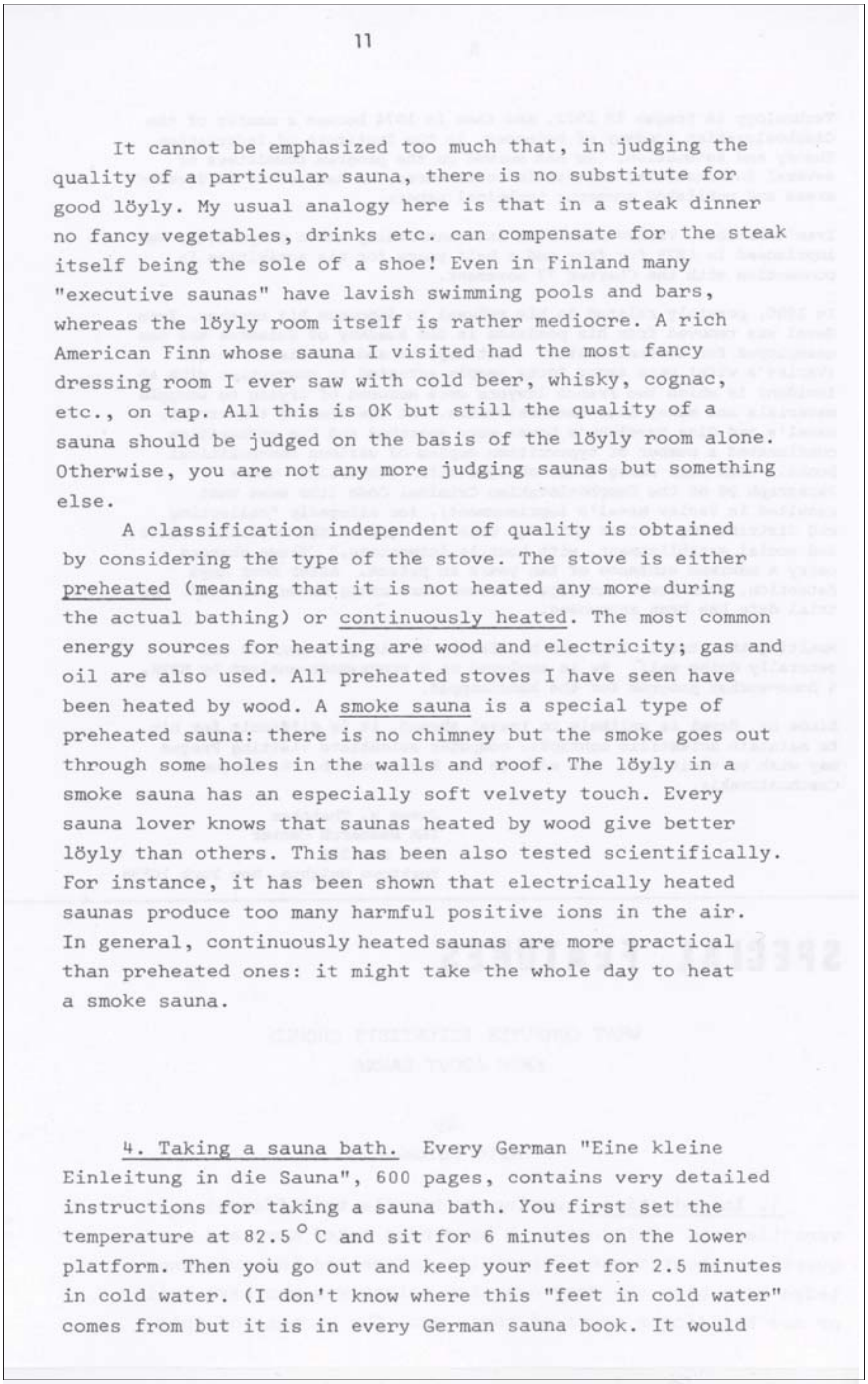
It goes without saying that a sign "SAUNA" outside a building does not guarantee that there actually is a sauna inside. You should investigate the matter according to the definition above! Indeed, in some countries the word "sauna" has specific other connotations.

As in all real-life situations, the definition is not quite satisfactory mathematically. This is the case especially as regards H_2 and S_1. I myself have never met any borderline cases but Section 7 below contains examples where some of the requirements are clearly not satisfied. If you ever meet a borderline case, it just indicates that the difference between a very good non-sauna and a very bad sauna is not so big!

"Sauna" is a very old Finnish word, so I am speaking all the time of "a sauna" rather than of "a Finnish sauna". On the other hand, I object to the usage of the word "sauna" in connection with other types of baths.

"Löyly" is the Finnish word for "sauna heat". More specifically, "löyly" means the heat emanating from the stones when water is thrown on them. The most important accessory to a sauna bath is "vihta": a bunch of soft leafy birch twigs. Also other trees can be used to make vihtas. For instance, in California eucalyptus is used. The reader should remember the words "kiuas", "löyly" and "vihta".

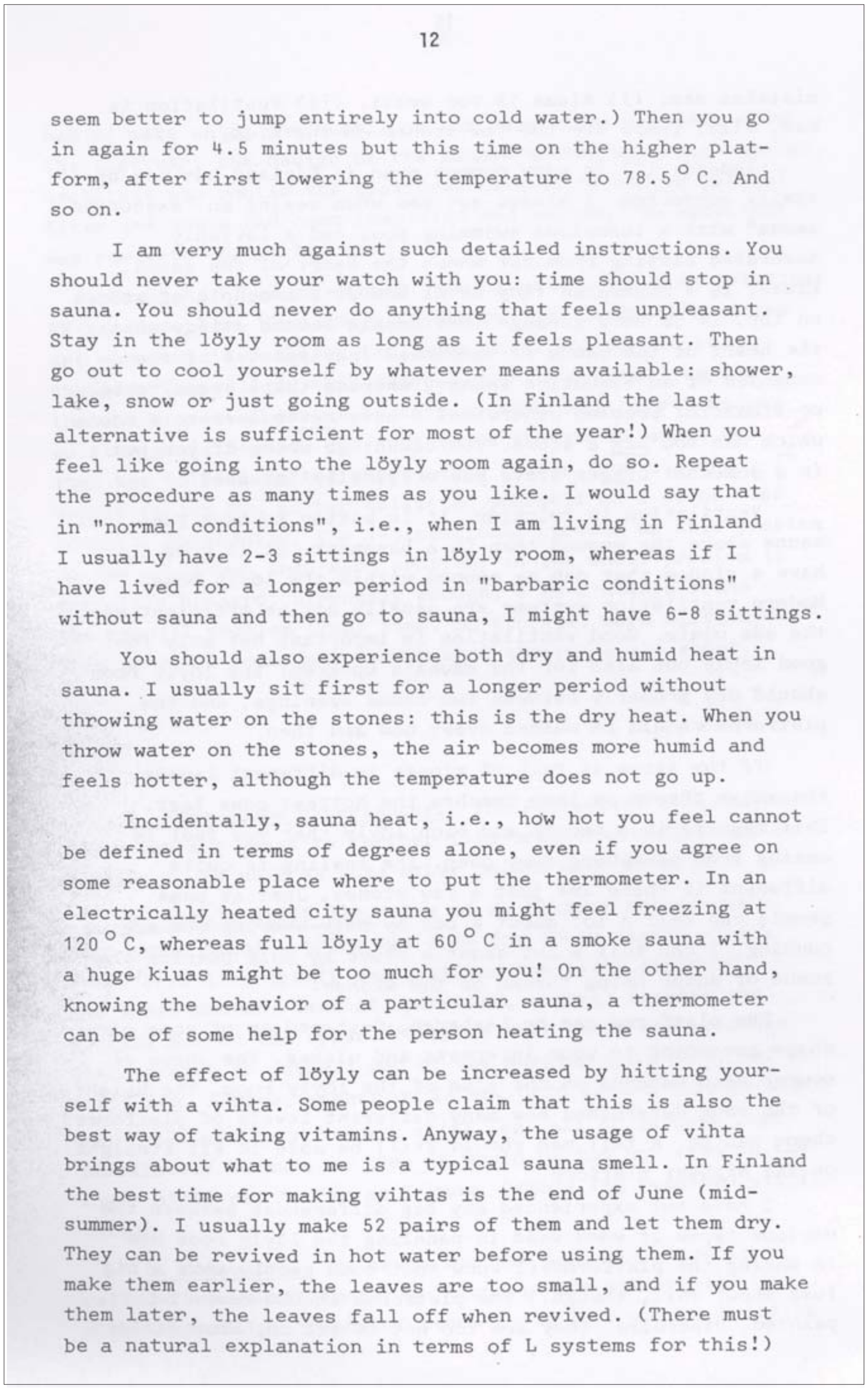
<u>3. Classifications of saunas.</u> Having defined what a sauna is, we now discuss briefly what makes a sauna good or bad. The decisive factor is the quality of löyly. My usual rule of thumb here is that löyly is really good if the only reason to get out of the sauna is that you feel that your ears are burning, rather than that you cannot breathe well or the place looks filthy or smells bad, etc. In other words, the only reason to get out should be that it is too hot for you! The most important factors contributing towards this are good ventilation and a sufficiently big stove (kiuas). This will be further discussed in Section 6.



It cannot be emphasized too much that, in judging the quality of a particular sauna, there is no substitute for good löyly. My usual analogy here is that in a steak dinner no fancy vegetables, drinks etc. can compensate for the steak itself being the sole of a shoe! Even in Finland many "executive saunas" have lavish swimming pools and bars, whereas the löyly room itself is rather mediocre. A rich American Finn whose sauna I visited had the most fancy dressing room I ever saw with cold beer, whisky, cognac, etc., on tap. All this is OK but still the quality of a sauna should be judged on the basis of the löyly room alone. Otherwise, you are not any more judging saunas but something else.

A classification independent of quality is obtained by considering the type of the stove. The stove is either preheated (meaning that it is not heated any more during the actual bathing) or continuously heated. The most common energy sources for heating are wood and electricity; gas and oil are also used. All preheated stoves I have seen have been heated by wood. A smoke sauna is a special type of preheated sauna: there is no chimney but the smoke goes out through some holes in the walls and roof. The löyly in a smoke sauna has an especially soft velvety touch. Every sauna lover knows that saunas heated by wood give better löyly than others. This has been also tested scientifically. For instance, it has been shown that electrically heated saunas produce too many harmful positive ions in the air. In general, continuously heated saunas are more practical than preheated ones: it might take the whole day to heat a smoke sauna.

4. Taking a sauna bath. Every German "Eine kleine Einleitung in die Sauna", 600 pages, contains very detailed instructions for taking a sauna bath. You first set the temperature at 82.5 °C and sit for 6 minutes on the lower platform. Then you go out and keep your feet for 2.5 minutes in cold water. (I don't know where this "feet in cold water" comes from but it is in every German sauna book. It would



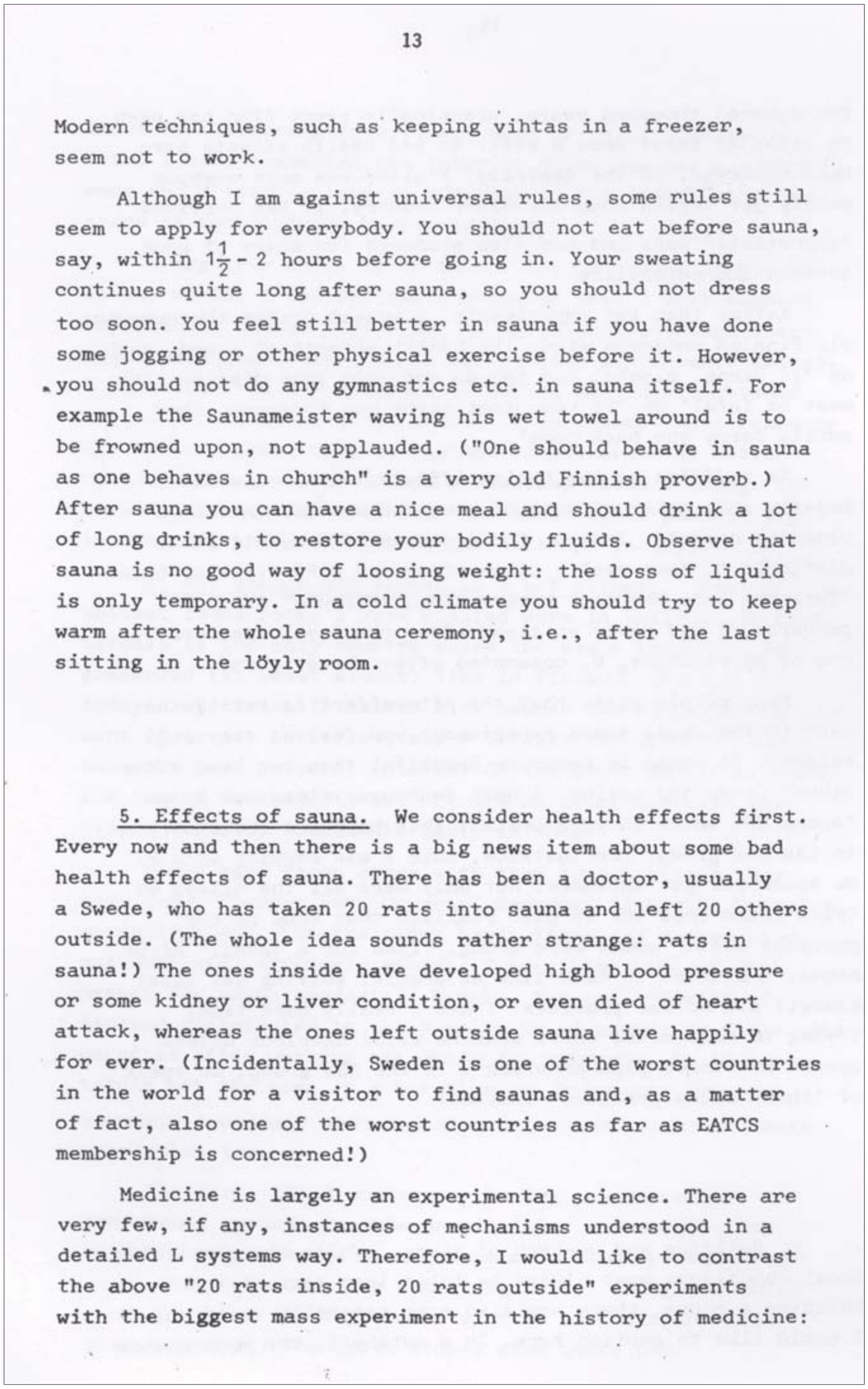
seem better to jump entirely into cold water.) Then you go in again for 4.5 minutes but this time on the higher platform, after first lowering the temperature to 78.5 ° C. And so on.

I am very much against such detailed instructions. You should never take your watch with you: time should stop in sauna. You should never do anything that feels unpleasant. Stay in the löyly room as long as it feels pleasant. Then go out to cool yourself by whatever means available: shower, lake, snow or just going outside. (In Finland the last alternative is sufficient for most of the year!) When you feel like going into the löyly room again, do so. Repeat the procedure as many times as you like. I would say that in "normal conditions", i.e., when I am living in Finland I usually have 2-3 sittings in löyly room, whereas if I have lived for a longer period in "barbaric conditions" without sauna and then go to sauna, I might have 6-8 sittings.

You should also experience both dry and humid heat in sauna. I usually sit first for a longer period without throwing water on the stones: this is the dry heat. When you throw water on the stones, the air becomes more humid and feels hotter, although the temperature does not go up.

Incidentally, sauna heat, i.e., how hot you feel cannot be defined in terms of degrees alone, even if you agree on some reasonable place where to put the thermometer. In an electrically heated city sauna you might feel freezing at 120 ° C, whereas full löyly at 60 ° C in a smoke sauna with a huge kiuas might be too much for you! On the other hand, knowing the behavior of a particular sauna, a thermometer can be of some help for the person heating the sauna.

The effect of löyly can be increased by hitting yourself with a vihta. Some people claim that this is also the best way of taking vitamins. Anyway, the usage of vihta brings about what to me is a typical sauna smell. In Finland the best time for making vihtas is the end of June (midsummer). I usually make 52 pairs of them and let them dry. They can be revived in hot water before using them. If you make them earlier, the leaves are too small, and if you make them later, the leaves fall off when revived. (There must be a natural explanation in terms of L systems for this!)

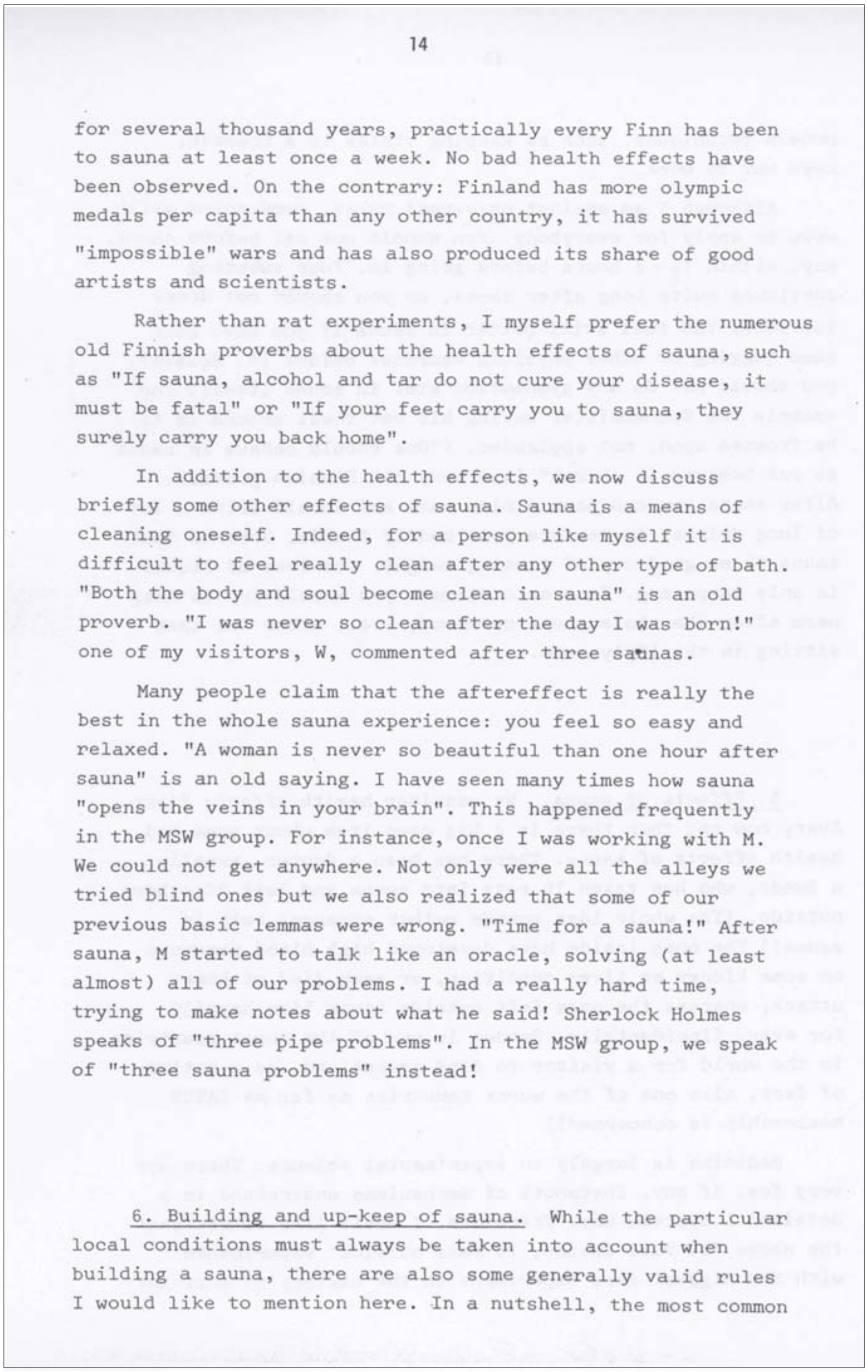


Modern techniques, such as keeping vihtas in a freezer, seem not to work.

Although I am against universal rules, some rules still seem to apply for everybody. You should not eat before sauna, say, within 1$\frac{1}{2}$ - 2 hours before going in. Your sweating continues quite long after sauna, so you should not dress too soon. You feel still better in sauna if you have done some jogging or other physical exercise before it. However, you should not do any gymnastics etc. in sauna itself. For example the Saunameister waving his wet towel around is to be frowned upon, not applauded. ("One should behave in sauna as one behaves in church" is a very old Finnish proverb.) After sauna you can have a nice meal and should drink a lot of long drinks, to restore your bodily fluids. Observe that sauna is no good way of loosing weight: the loss of liquid is only temporary. In a cold climate you should try to keep warm after the whole sauna ceremony, i.e., after the last sitting in the löyly room.

5. Effects of sauna. We consider health effects first. Every now and then there is a big news item about some bad health effects of sauna. There has been a doctor, usually a Swede, who has taken 20 rats into sauna and left 20 others outside. (The whole idea sounds rather strange: rats in sauna!) The ones inside have developed high blood pressure or some kidney or liver condition, or even died of heart attack, whereas the ones left outside sauna live happily for ever. (Incidentally, Sweden is one of the worst countries in the world for a visitor to find saunas and, as a matter of fact, also one of the worst countries as far as EATCS membership is concerned!)

Medicine is largely an experimental science. There are very few, if any, instances of mechanisms understood in a detailed L systems way. Therefore, I would like to contrast the above "20 rats inside, 20 rats outside" experiments with the biggest mass experiment in the history of medicine:



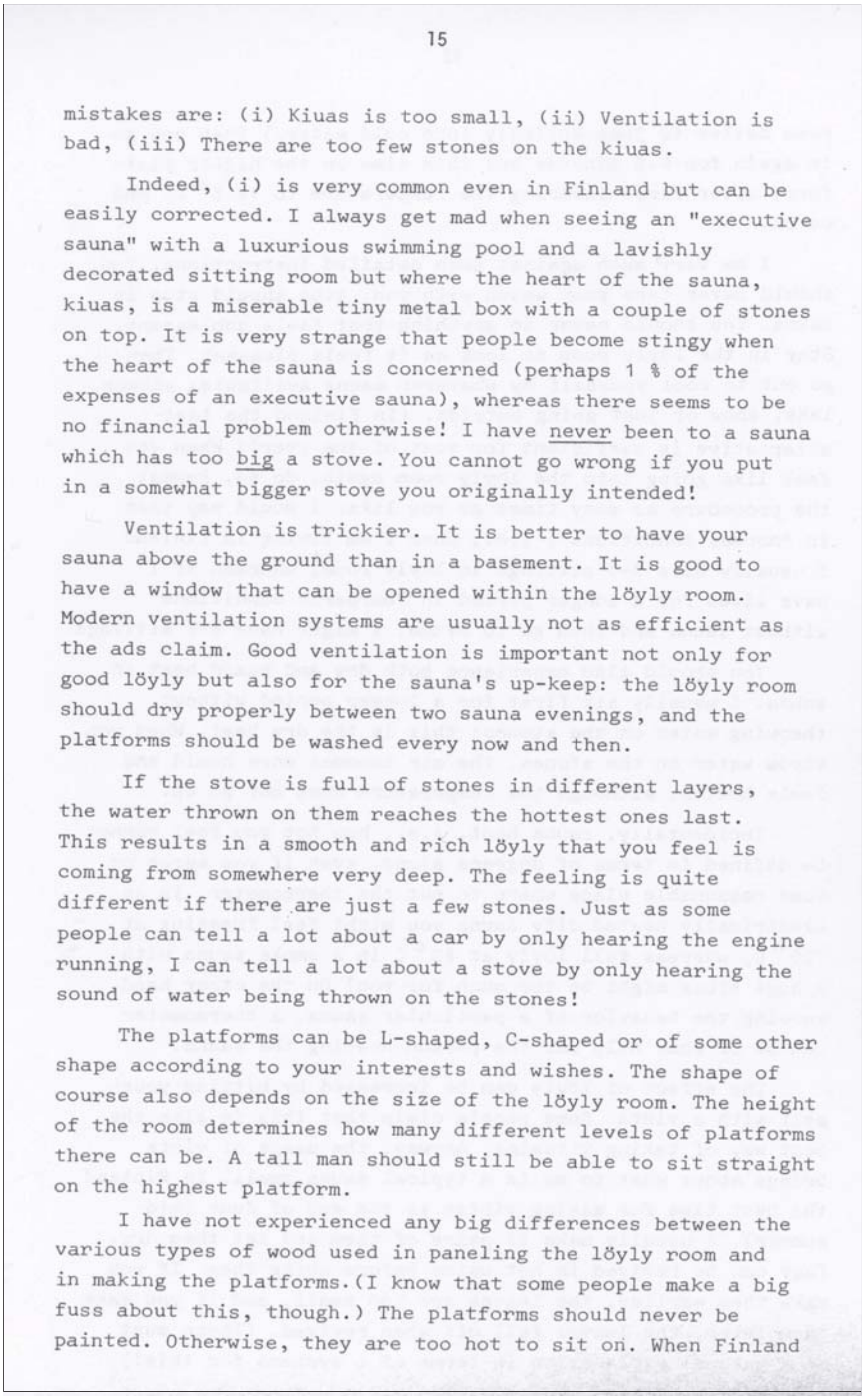
for several thousand years, practically every Finn has been to sauna at least once a week. No bad health effects have been observed. On the contrary: Finland has more olympic medals per capita than any other country, it has survived "impossible" wars and has also produced its share of good artists and scientists.

Rather than rat experiments, I myself prefer the numerous old Finnish proverbs about the health effects of sauna, such as "If sauna, alcohol and tar do not cure your disease, it must be fatal" or "If your feet carry you to sauna, they surely carry you back home".

In addition to the health effects, we now discuss briefly some other effects of sauna. Sauna is a means of cleaning oneself. Indeed, for a person like myself it is difficult to feel really clean after any other type of bath. "Both the body and soul become clean in sauna" is an old proverb. "I was never so clean after the day I was born!" one of my visitors, W, commented after three saunas.

Many people claim that the aftereffect is really the best in the whole sauna experience: you feel so easy and relaxed. "A woman is never so beautiful than one hour after sauna" is an old saying. I have seen many times how sauna "opens the veins in your brain". This happened frequently in the MSW group. For instance, once I was working with M. We could not get anywhere. Not only were all the alleys we tried blind ones but we also realized that some of our previous basic lemmas were wrong. "Time for a sauna!" After sauna, M started to talk like an oracle, solving (at least almost) all of our problems. I had a really hard time, trying to make notes about what he said! Sherlock Holmes speaks of "three pipe problems". In the MSW group, we speak of "three sauna problems" instead!

6. Building and up-keep of sauna. While the particular local conditions must always be taken into account when building a sauna, there are also some generally valid rules I would like to mention here. In a nutshell, the most common



mistakes are: (i) Kiuas is too small, (ii) Ventilation is bad, (iii) There are too few stones on the kiuas.

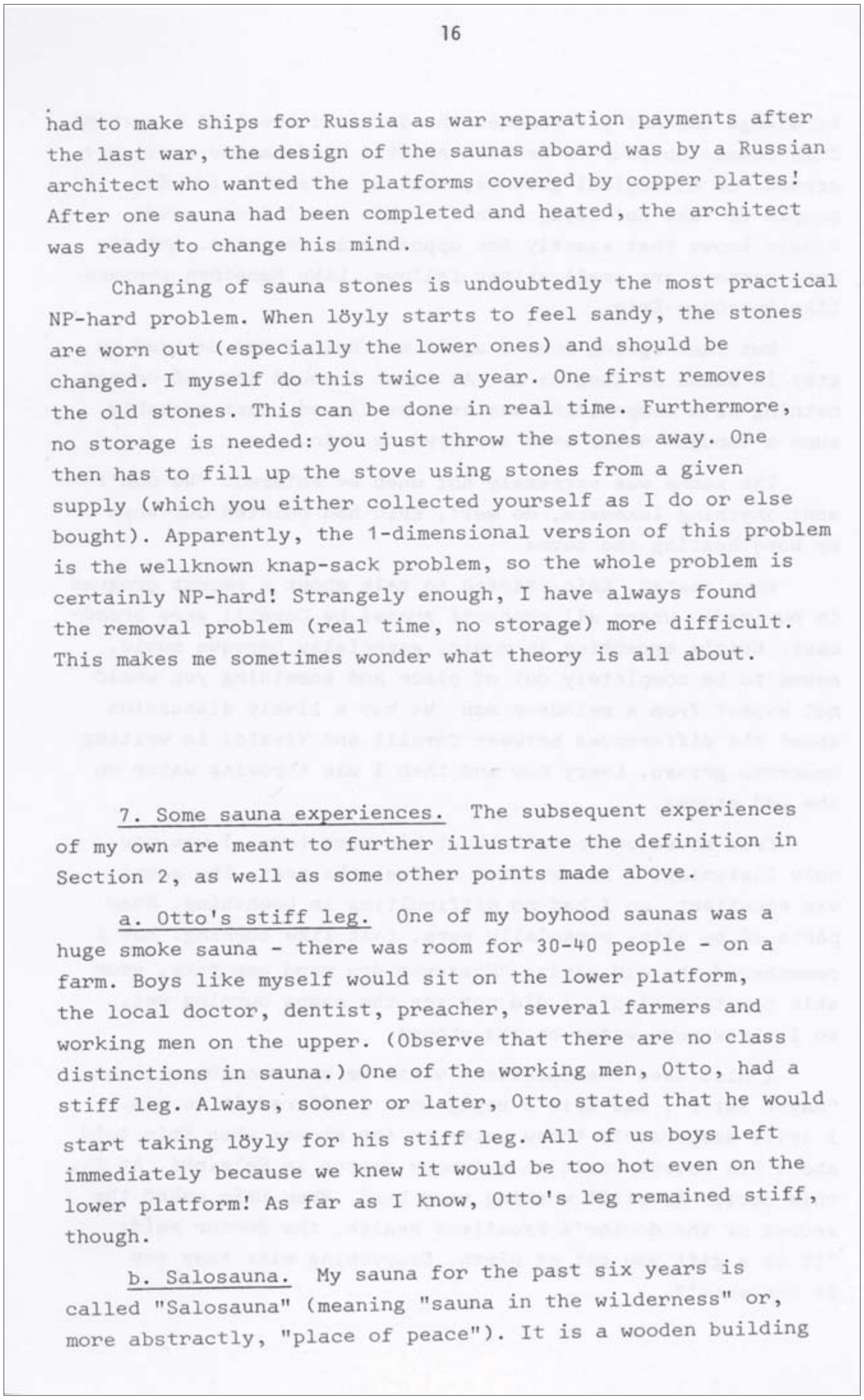
Indeed, (i) is very common even in Finland but can be easily corrected. I always get mad when seeing an "executive sauna" with a luxurious swimming pool and a lavishly decorated sitting room but where the heart of the sauna, kiuas, is a miserable tiny metal box with a couple of stones on top. It is very strange that people become stingy when the heart of the sauna is concerned (perhaps 1 % of the expenses of an executive sauna), whereas there seems to be no financial problem otherwise! I have *never* been to a sauna which has too *big* a stove. You cannot go wrong if you put in a somewhat bigger stove you originally intended!

Ventilation is trickier. It is better to have your sauna above the ground than in a basement. It is good to have a window that can be opened within the löyly room. Modern ventilation systems are usually not as efficient as the ads claim. Good ventilation is important not only for good löyly but also for the sauna's up-keep: the löyly room should dry properly between two sauna evenings, and the platforms should be washed every now and then.

If the stove is full of stones in different layers, the water thrown on them reaches the hottest ones last. This results in a smooth and rich löyly that you feel is coming from somewhere very deep. The feeling is quite different if there are just a few stones. Just as some people can tell a lot about a car by only hearing the engine running, I can tell a lot about a stove by only hearing the sound of water being thrown on the stones!

The platforms can be L-shaped, C-shaped or of some other shape according to your interests and wishes. The shape of course also depends on the size of the löyly room. The height of the room determines how many different levels of platforms there can be. A tall man should still be able to sit straight on the highest platform.

I have not experienced any big differences between the various types of wood used in paneling the löyly room and in making the platforms.(I know that some people make a big fuss about this, though.) The platforms should never be painted. Otherwise, they are too hot to sit on. When Finland



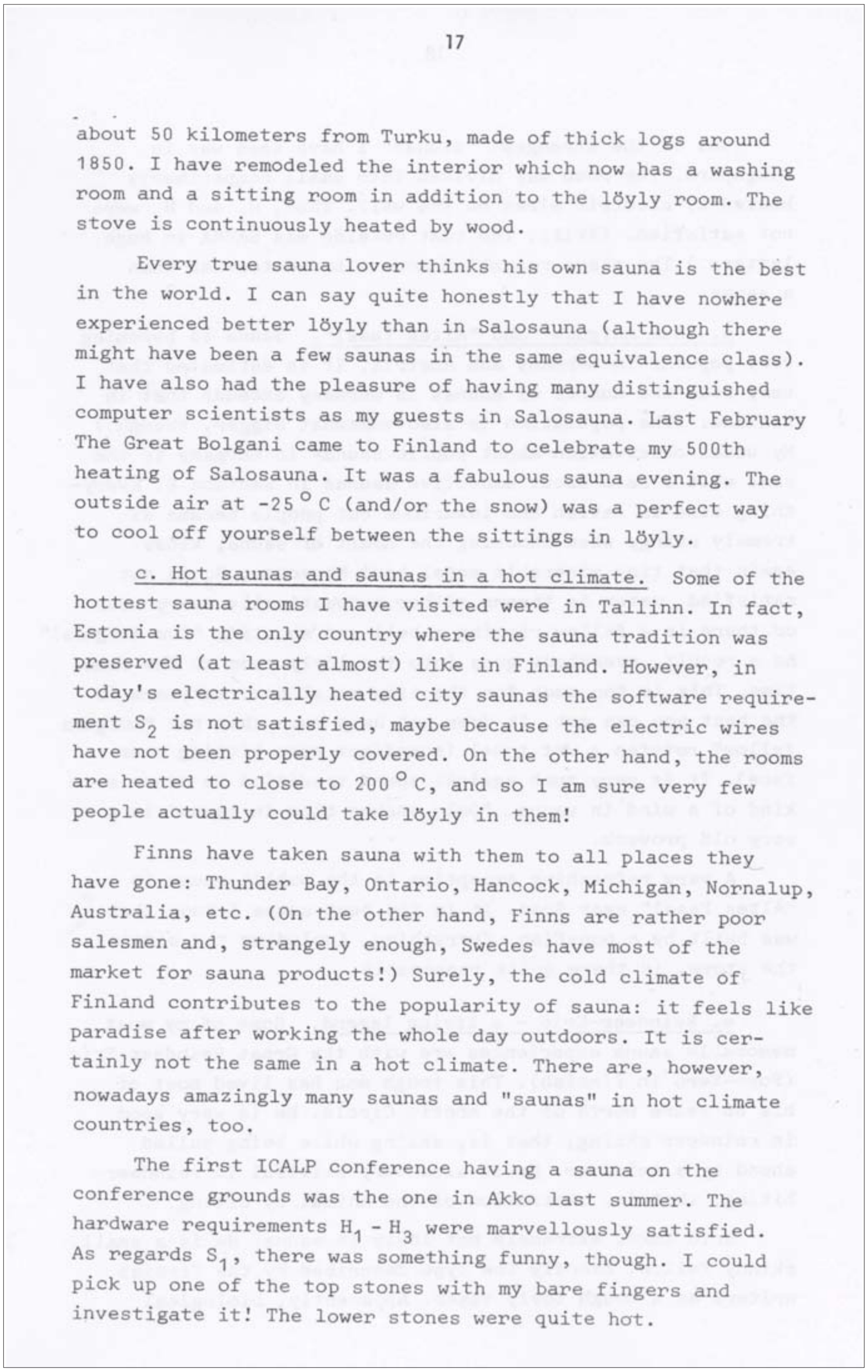
had to make ships for Russia as war reparation payments after the last war, the design of the saunas aboard was by a Russian architect who wanted the platforms covered by copper plates! After one sauna had been completed and heated, the architect was ready to change his mind.

Changing of sauna stones is undoubtedly the most practical NP-hard problem. When löyly starts to feel sandy, the stones are worn out (especially the lower ones) and should be changed. I myself do this twice a year. One first removes the old stones. This can be done in real time. Furthermore, no storage is needed: you just throw the stones away. One then has to fill up the stove using stones from a given supply (which you either collected yourself as I do or else bought). Apparently, the 1-dimensional version of this problem is the wellknown knap-sack problem, so the whole problem is certainly NP-hard! Strangely enough, I have always found the removal problem (real time, no storage) more difficult. This makes me sometimes wonder what theory is all about.

7. Some sauna experiences. The subsequent experiences of my own are meant to further illustrate the definition in Section 2, as well as some other points made above.

a. Otto's stiff leg. One of my boyhood saunas was a huge smoke sauna - there was room for 30-40 people - on a farm. Boys like myself would sit on the lower platform, the local doctor, dentist, preacher, several farmers and working men on the upper. (Observe that there are no class distinctions in sauna.) One of the working men, Otto, had a stiff leg. Always, sooner or later, Otto stated that he would start taking löyly for his stiff leg. All of us boys left immediately because we knew it would be too hot even on the lower platform! As far as I know, Otto's leg remained stiff, though.

b. Salosauna. My sauna for the past six years is called "Salosauna" (meaning "sauna in the wilderness" or, more abstractly, "place of peace"). It is a wooden building



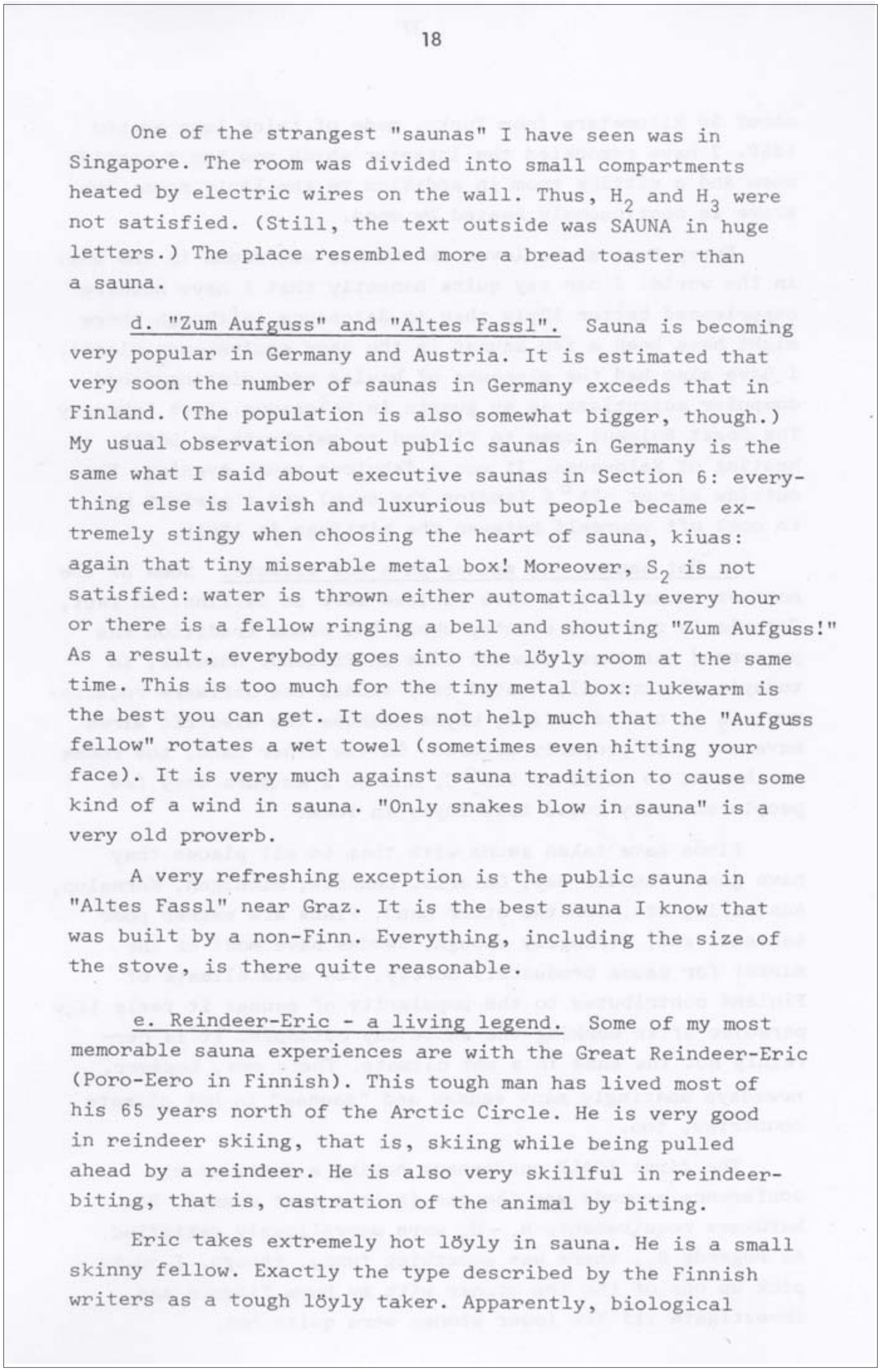
about 50 kilometers from Turku, made of thick logs around 1850. I have remodeled the interior which now has a washing room and a sitting room in addition to the löyly room. The stove is continuously heated by wood.

Every true sauna lover thinks his own sauna is the best in the world. I can say quite honestly that I have nowhere experienced better löyly than in Salosauna (although there might have been a few saunas in the same equivalence class). I have also had the pleasure of having many distinguished computer scientists as my guests in Salosauna. Last February The Great Bolgani came to Finland to celebrate my 500th heating of Salosauna. It was a fabulous sauna evening. The outside air at -25 ° C (and/or the snow) was a perfect way to cool off yourself between the sittings in löyly.

c. Hot saunas and saunas in a hot climate. Some of the hottest sauna rooms I have visited were in Tallinn. In fact, Estonia is the only country where the sauna tradition was preserved (at least almost) like in Finland. However, in today's electrically heated city saunas the software requirement S_2 is not satisfied, maybe because the electric wires have not been properly covered. On the other hand, the rooms are heated to close to 200 ° C, and so I am sure very few people actually could take löyly in them!

Finns have taken sauna with them to all places they have gone: Thunder Bay, Ontario, Hancock, Michigan, Nornalup, Australia, etc. (On the other hand, Finns are rather poor salesmen and, strangely enough, Swedes have most of the market for sauna products!) Surely, the cold climate of Finland contributes to the popularity of sauna: it feels like paradise after working the whole day outdoors. It is certainly not the same in a hot climate. There are, however, nowadays amazingly many saunas and "saunas" in hot climate countries, too.

The first ICALP conference having a sauna on the conference grounds was the one in Akko last summer. The hardware requirements $H_1 - H_3$ were marvellously satisfied. As regards S_1, there was something funny, though. I could pick up one of the top stones with my bare fingers and investigate it! The lower stones were quite hot.



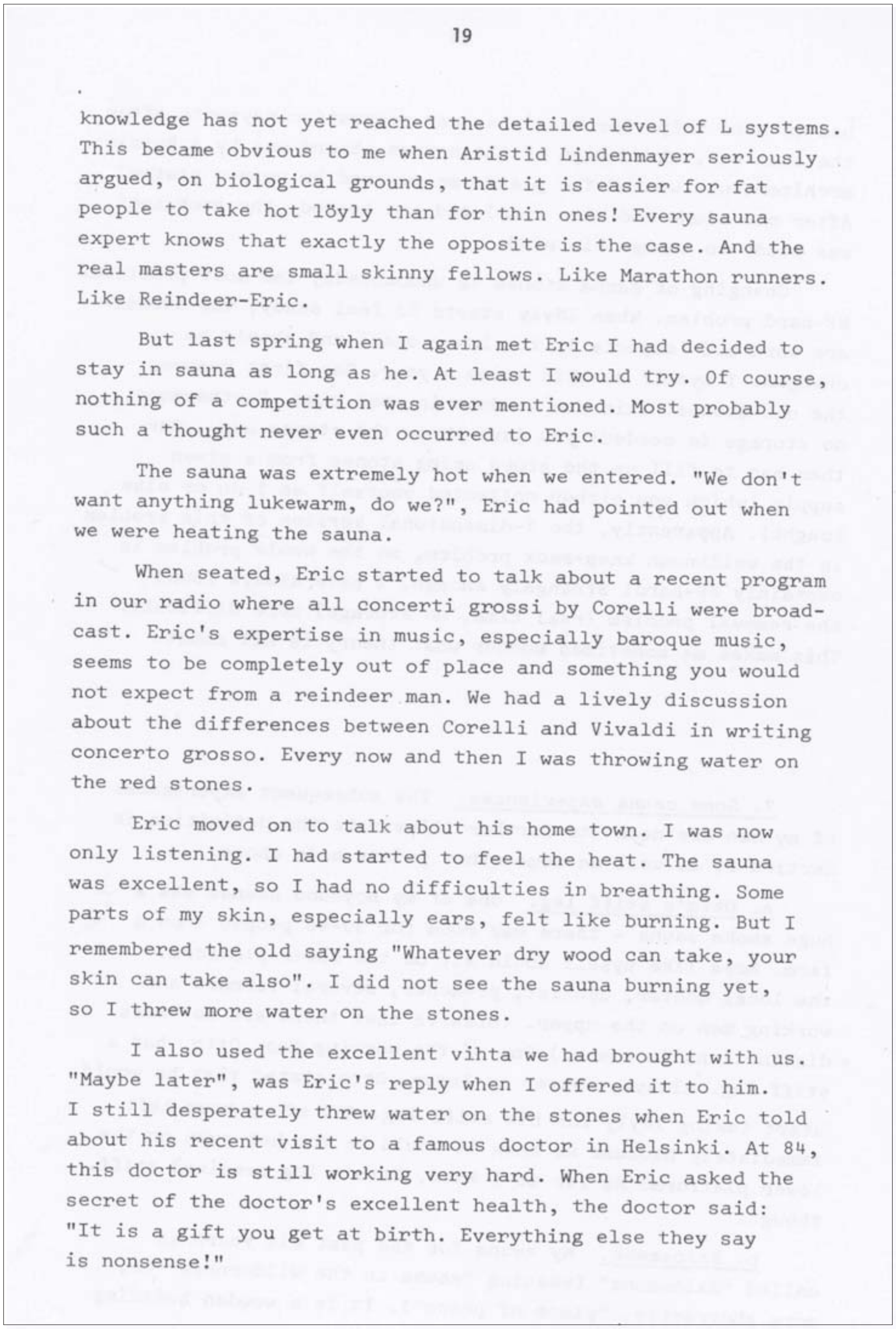
One of the strangest "saunas" I have seen was in Singapore. The room was divided into small compartments heated by electric wires on the wall. Thus, H_2 and H_3 were not satisfied. (Still, the text outside was SAUNA in huge letters.) The place resembled more a bread toaster than a sauna.

d. "Zum Aufguss" and "Altes Fassl". Sauna is becoming very popular in Germany and Austria. It is estimated that very soon the number of saunas in Germany exceeds that in Finland. (The population is also somewhat bigger, though.) My usual observation about public saunas in Germany is the same what I said about executive saunas in Section 6: everything else is lavish and luxurious but people became extremely stingy when choosing the heart of sauna, kiuas: again that tiny miserable metal box! Moreover, S_2 is not satisfied: water is thrown either automatically every hour or there is a fellow ringing a bell and shouting "Zum Aufguss!" As a result, everybody goes into the löyly room at the same time. This is too much for the tiny metal box: lukewarm is the best you can get. It does not help much that the "Aufguss fellow" rotates a wet towel (sometimes even hitting your face). It is very much against sauna tradition to cause some kind of a wind in sauna. "Only snakes blow in sauna" is a very old proverb.

A very refreshing exception is the public sauna in "Altes Fassl" near Graz. It is the best sauna I know that was built by a non-Finn. Everything, including the size of the stove, is there quite reasonable.

e. Reindeer-Eric - a living legend. Some of my most memorable sauna experiences are with the Great Reindeer-Eric (Poro-Eero in Finnish). This tough man has lived most of his 65 years north of the Arctic Circle. He is very good in reindeer skiing, that is, skiing while being pulled ahead by a reindeer. He is also very skillful in reindeer-biting, that is, castration of the animal by biting.

Eric takes extremely hot löyly in sauna. He is a small skinny fellow. Exactly the type described by the Finnish writers as a tough löyly taker. Apparently, biological



knowledge has not yet reached the detailed level of L systems. This became obvious to me when Aristid Lindenmayer seriously argued, on biological grounds, that it is easier for fat people to take hot löyly than for thin ones! Every sauna expert knows that exactly the opposite is the case. And the real masters are small skinny fellows. Like Marathon runners. Like Reindeer-Eric.

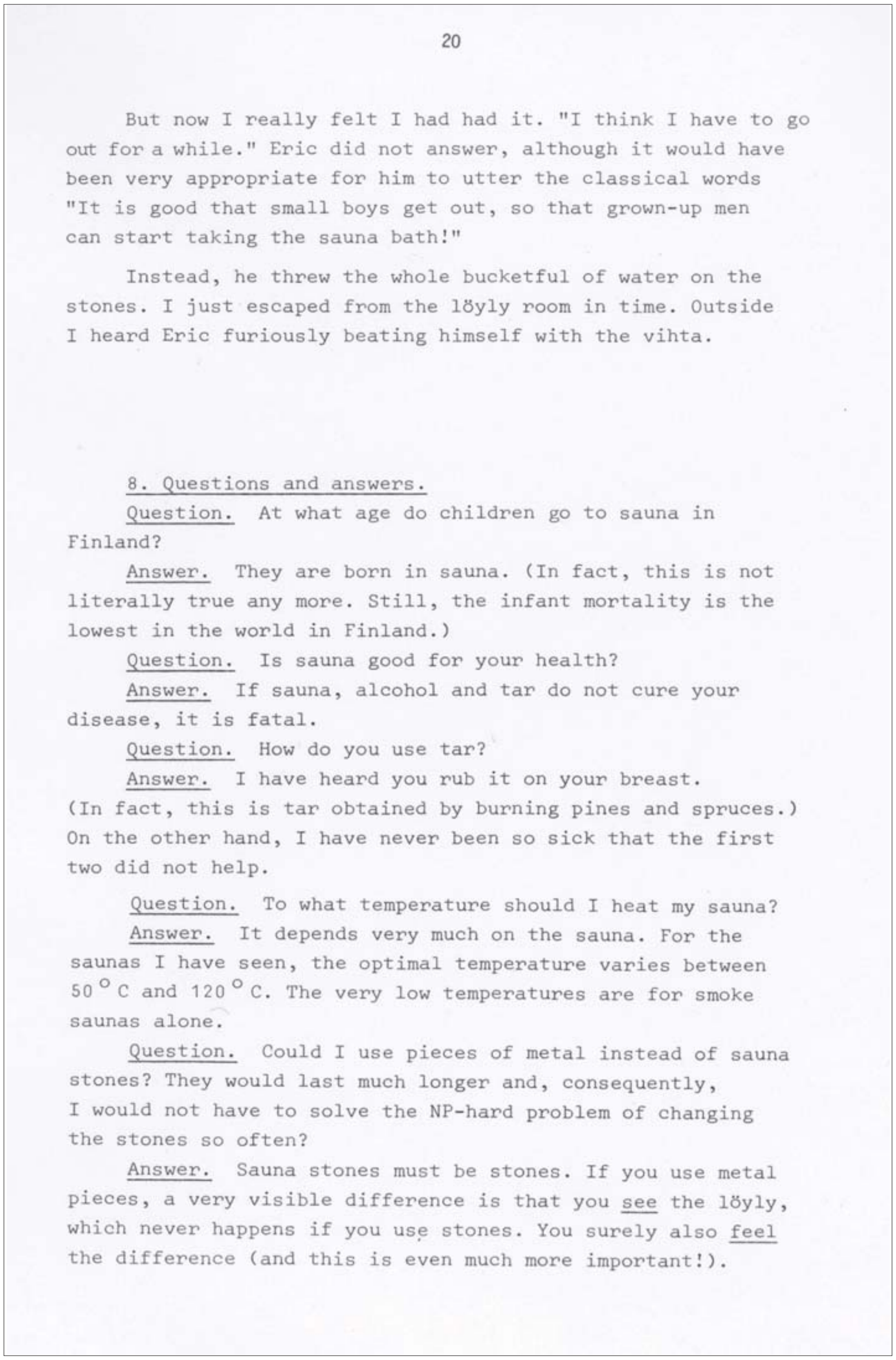
But last spring when I again met Eric I had decided to stay in sauna as long as he. At least I would try. Of course, nothing of a competition was ever mentioned. Most probably such a thought never even occurred to Eric.

The sauna was extremely hot when we entered. "We don't want anything lukewarm, do we?", Eric had pointed out when we were heating the sauna.

When seated, Eric started to talk about a recent program in our radio where all concerti grossi by Corelli were broadcast. Eric's expertise in music, especially baroque music, seems to be completely out of place and something you would not expect from a reindeer man. We had a lively discussion about the differences between Corelli and Vivaldi in writing concerto grosso. Every now and then I was throwing water on the red stones.

Eric moved on to talk about his home town. I was now only listening. I had started to feel the heat. The sauna was excellent, so I had no difficulties in breathing. Some parts of my skin, especially ears, felt like burning. But I remembered the old saying "Whatever dry wood can take, your skin can take also". I did not see the sauna burning yet, so I threw more water on the stones.

I also used the excellent vihta we had brought with us. "Maybe later", was Eric's reply when I offered it to him. I still desperately threw water on the stones when Eric told about his recent visit to a famous doctor in Helsinki. At 84, this doctor is still working very hard. When Eric asked the secret of the doctor's excellent health, the doctor said: "It is a gift you get at birth. Everything else they say is nonsense!"



But now I really felt I had had it. "I think I have to go out for a while." Eric did not answer, although it would have been very appropriate for him to utter the classical words "It is good that small boys get out, so that grown-up men can start taking the sauna bath!"

Instead, he threw the whole bucketful of water on the stones. I just escaped from the löyly room in time. Outside I heard Eric furiously beating himself with the vihta.

8. Questions and answers.

Question. At what age do children go to sauna in Finland?

Answer. They are born in sauna. (In fact, this is not literally true any more. Still, the infant mortality is the lowest in the world in Finland.)

Question. Is sauna good for your health?

Answer. If sauna, alcohol and tar do not cure your disease, it is fatal.

Question. How do you use tar?

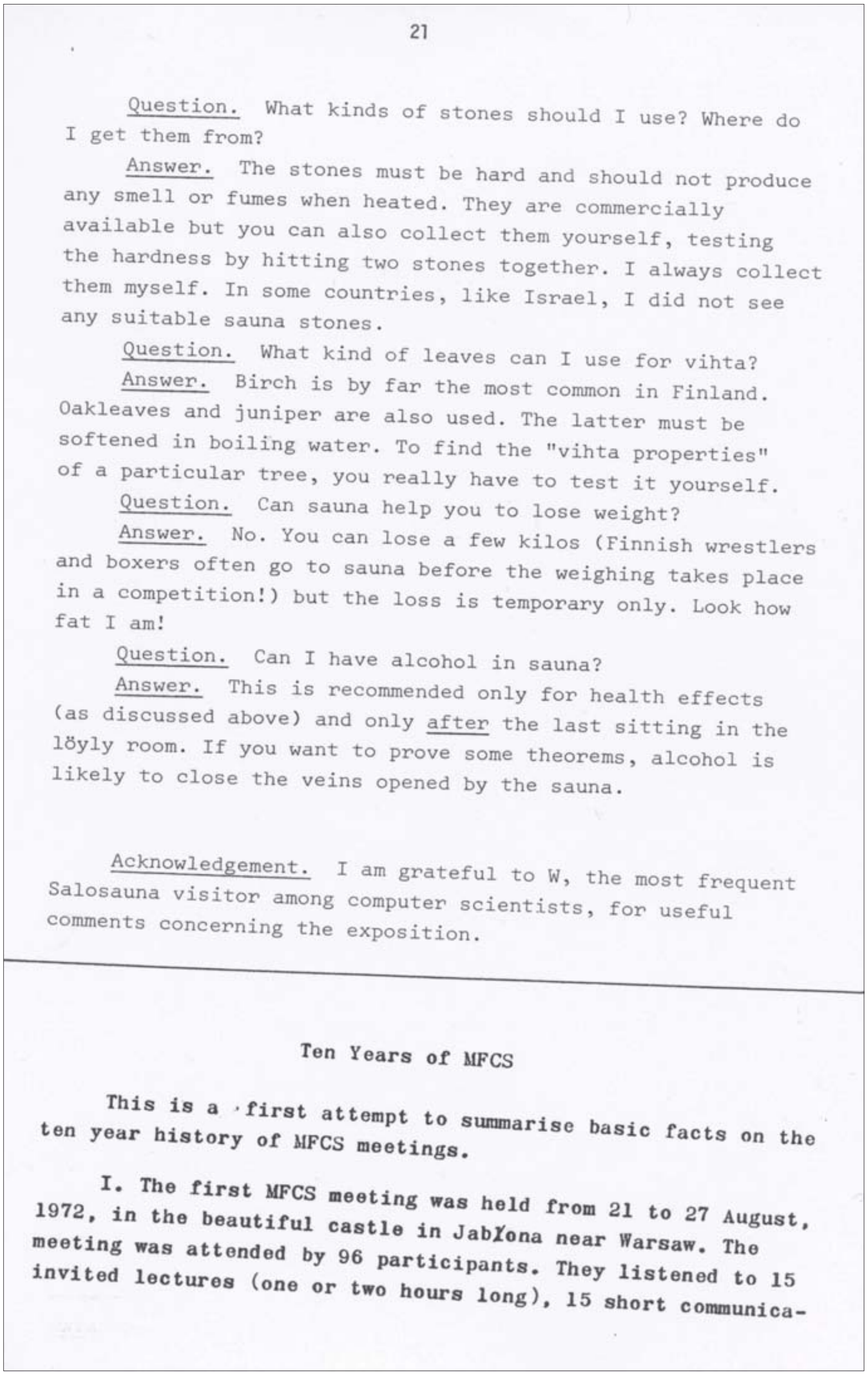
Answer. I have heard you rub it on your breast. (In fact, this is tar obtained by burning pines and spruces.) On the other hand, I have never been so sick that the first two did not help.

Question. To what temperature should I heat my sauna?

Answer. It depends very much on the sauna. For the saunas I have seen, the optimal temperature varies between 50 °C and 120 °C. The very low temperatures are for smoke saunas alone.

Question. Could I use pieces of metal instead of sauna stones? They would last much longer and, consequently, I would not have to solve the NP-hard problem of changing the stones so often?

Answer. Sauna stones must be stones. If you use metal pieces, a very visible difference is that you *see* the löyly, which never happens if you use stones. You surely also *feel* the difference (and this is even much more important!).



Question. What kinds of stones should I use? Where do I get them from?

Answer. The stones must be hard and should not produce any smell or fumes when heated. They are commercially available but you can also collect them yourself, testing the hardness by hitting two stones together. I always collect them myself. In some countries, like Israel, I did not see any suitable sauna stones.

Question. What kind of leaves can I use for vihta?

Answer. Birch is by far the most common in Finland. Oakleaves and juniper are also used. The latter must be softened in boiling water. To find the "vihta properties" of a particular tree, you really have to test it yourself.

Question. Can sauna help you to lose weight?

Answer. No. You can lose a few kilos (Finnish wrestlers and boxers often go to sauna before the weighing takes place in a competition!) but the loss is temporary only. Look how fat I am!

Question. Can I have alcohol in sauna?

Answer. This is recommended only for health effects (as discussed above) and only after the last sitting in the löyly room. If you want to prove some theorems, alcohol is likely to close the veins opened by the sauna.

Acknowledgement. I am grateful to W, the most frequent Salosauna visitor among computer scientists, for useful comments concerning the exposition.

Ten Years of MFCS

This is a first attempt to summarise basic facts on the ten year history of MFCS meetings.

I. The first MFCS meeting was held from 21 to 27 August, 1972, in the beautiful castle in Jabłona near Warsaw. The meeting was attended by 96 participants. They listened to 15 invited lectures (one or two hours long), 15 short communica-

Tampereen teknillinen yliopisto
PL 527
33101 Tampere

Tampere University of Technology
P.O. Box 527
FIN-33101 Tampere, Finland

ISBN 978-952-15-2290-1
ISSN 1456-2774