

Lecture Notes in Computer Science

53

**Mathematical Foundations
of Computer Science 1977**

**Proceedings, 6th Symposium, Tatranská Lomnica
September 5-9, 1977**

Edited by J. Gruska

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

53

Mathematical Foundations of Computer Science 1977

Proceedings, 6th Symposium, Tatranská Lomnica
September 5-9, 1977

Edited by J. Gruska



Springer-Verlag
Berlin · Heidelberg · New York 1977

Editorial Board

P. Brinch Hansen D. Gries C. Moler G. Seegmüller
J. Stoer N. Wirth

Editor

Jozef Gruska
Computing Research Centre
Dúbravská 3
885 31 Bratislava
Czechoslovakia

Library of Congress Cataloging in Publication Data

Main entry under title:

Mathematical foundations of computer science, 1977.

(Lecture notes in computer science ; 53)

Bibliography: p.

Includes index.

1. Machine theory--Congresses. 2. Formal languages
--Congresses. 3. Programming (Electronic computers)--
Congresses. I. Gruska, Jozef. II. Series.
QA267.M37 001.6¹⁴ 77-10135

AMS Subject Classifications (1970): 02B25, 02D99, 02E10, 02E15,
02F10, 02F15, 02F20, 18B20, 68A05, 68A10, 68A20, 68A25, 68A30,
68A45, 68A50, 94A20, 94A30, 94A35

CR Subject Classifications (1974): 3.61, 3.79, 4.12, 4.20, 4.33, 5.14, 5.21,
5.22, 5.23, 5.24, 5.25, 5.26, 5.27, 5.28, 5.5

ISBN 3-540-08353-7 Springer-Verlag Berlin · Heidelberg · New York
ISBN 0-387-08353-7 Springer-Verlag New York · Heidelberg · Berlin

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, re-printing, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks.

Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to the publisher, the amount of the fee to be determined by agreement with the publisher.

© by Springer-Verlag Berlin · Heidelberg 1977

Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.

2145/3140-543210



FOREWORD

This volume contains papers which were contributed for presentation at the 6th Symposium on Mathematical Foundations of Computer Science - MFCS'77, held at Tatranská Lomnica, Czechoslovakia, September 5-9, 1977.

The symposium was organized by the Computing Research Centre in Bratislava. The following institutions have cooperated in providing their support: The Faculty of Mathematics and Physics of the Charles University, Prague; the Faculty of Natural Sciences of the Šafárik University, Košice; the Faculty of Natural Sciences of the Komenský University, Bratislava; the Institute of Computing Technique of the Technical University, Prague; Institute of Technical Cybernetics of the Slovak Academy of Sciences; the Association of Slovak Mathematicians and Physicists and the Slovak Cybernetical Society.

The title of the symposium, "Mathematical Foundations of Computer Science" was chosen six years ago by the Polish organizers for the first meeting in the series and in 1974 it was used also for a seminar held at the International Banach Centre in Warsaw. In subsequent years it became a widely accepted designation for this new and important branch of science. It is understandable that this designation, or its close variants, will be used for other scientific events in the same areas, such as some of the recent symposia and seminars, held both in the United States and in Europe.

The present Proceedings include 15 invited papers and 46 short communications, the latter having been selected by the Program Committee from among

the 117 submitted papers on the basis of, originality and relevance to the following principal areas of interest: automata and formal languages, computability theory, analysis and complexity of algorithms, theoretical aspects of programming and of programming languages, theoretical aspects of operating systems and mathematical approaches to artificial intelligence.

The papers in these Proceedings were not formally refereed. It is anticipated that most of them will appear in a more polished and complete form in scientific journals.

The organizers of the symposium are much indebted to all of the contributors to this program, especially to the authors of the papers. Thanks are also due to all the above mentioned cooperating institutions for their valuable and all round assistance and to all people who helped in the organization of the Symposium.

Special thanks are due to Professor A. Klas, director of the Computing Research Centre in Bratislava for his generous support of not only MFCS '77 but of all MFCS symposia held in Czechoslovakia.

The Program Committee of MFCS '77 consisted of the following members: I.M. Havel /chairman/, J. Bečvář, J. Gruska, J. Hořejš, I. Korec, M. Novotný, B. Rován and J. Šturf. A number of referees helped the Program Committee evaluate the submitted papers.

The organization was done mainly by the following members of the Organizing Committee: G. Andrejková, Z. Durayová, R. Filustek, J. Gruska /Symposium Chairman/, A. Guráňová, I.M. Havel, M. Chytil, A. Jelínková, M. Markusová, P. Mikulecký, I. Prívára, B. Rován /Organizing Secretary/, and I. Šujan.

The help of Springer-Verlag, which has published these Proceedings, is also highly appreciated.

Bratislava, May 1977

Jozef Gruska

CONTENTS

INVITED LECTURES

G. Ausiello

On the structure and properties of NP - complete problems
and their associated optimization problems 1

A. Blikle

A comparative review of some program verification methods 17

L. Boasson

Classification of the context-free languages 34

C.C. Elgot

Finite automaton from a flowchart scheme point of view 44

E. Engeler

A new type of models of computation 52

A.P. Ershov and V.E. Itkin

Correctness of mixed computation in Algol-like programs 59

F. Gécseg and P.E.-Tóth

Algebra and logic in theoretical computer science 78

B. Kacewicz and H. Woźniakowski	
A survey of recent problems and results in analytic computational complexity	93
H.A. Maurer and Th. Ottmann	
Tree-structures for set manipulation problems	108
A. Salwicki	
Applied algorithmic logic	122
C.P. Schnorr	
Improved lower bounds on the number of multiplications/divi- sions which are necessary to evaluate polynomials	135
B.A. Trakhtenbrot	
Frequency algorithms and computations	148
L.G. Valiant	
Graph-theoretic arguments in low-level complexity	162
G. Wechsung	
Properties of complexity classes-A short survey	177
J.B. Wright, E.G. Wagner and J.W. Thatcher	
A uniform approach to inductive posets and inductive closure	192
COMMUNICATIONS	
V.N. Agafonov	
Generalized probabilistic grammars	213

G. Ausiello, A.D' Atri, M. Gaudiano and M. Protasi	
Classes of structurally isomorphic NP-optimization problems	222
J.M. Autebert	
Pushdown-automata and families of languages generating cylinders	231
J.W. de Bakker	
Semantics of infinite processes using generalized trees	240
V. Benda and K. Bendová	
Characterization of recognizable families by means of regular languages	247
A. Bertoni, G. Mauri and M. Torelli	
An algebraic approach to problem solution and problem semantics	253
A. Černý	
Complexity and minimality of context-free grammars and languages	263
M.P. Chytil	
Comparison of the active visiting and the crossing complexities	272
P. Hájek	
Arithmetical complexity of some problems in computer science	282
F.W. von Henke	
Formal transformations and the development of programs	288

S. Horváth	
Optimal RASP programs for arbitrarily complex 0-1 valued functions	297
T.M.V. Janssen and P. van Emde Boas	
The expressive power of intensional logic in the semantics of programming languages	303
M.I. Kanovič	
On the complexity of equivalent transformations in programming languages	312
V.N. Kasyanov and S.B. Pokrovsky	
Schematology in a multi-language optimizer	315
I. Korec	
Decidability /undecidability/ of equivalence of Mińsky machines with components consisting of at most seven /eight/ instructions	324
J. Král	
A top-down no backtrack parsing of general context-free languages	333
I. Kramosil	
A probabilistic restriction of branching plans	342
M. Kudlek and M. Novotný	
Reducing operators for normed general formal systems	350
L.A. Levin and V.V. V'jugin	
Invariant properties of informational bulks	359

M. Linna	
Two decidability results for deterministic pushdown automata	365
W. Lipski, Jr.	
On the logic of incomplete information	374
A. De Luca and S. Termini	
Measures of ambiguity in the analysis of complex systems	382
R. Meersman and G. Rozenberg	
Two-level meta-controlled substitution grammars	390
P.A. Miglioli and M. Ornaghi	
A calculus to build up correct programs	398
P.A. Ng and S.Y. Bang	
Another approach for proving program correctness	410
A. Nijholt	
Cover results and normal forms	420
J. Peckel	
On a deterministic subclass of context-free languages	430
J. Pittl	
Exponential optimization for the LLP (k) parsing method	435
F.P. Preparata	
The medial axis of a simple polygon	443

P. Raulefs	
Semantics and proof rules for coroutine hierarchies in block-structured programming languages	451
G. Rozenberg and D. Vermeir	
Acceptors for iteration languages	460
P. Ružička and J. Wiedermann	
How good is the adversary lower bound ?	465
S. Sokołowski	
Total correctness for procedures	475
J. Štunc	
A model for retrieval systems and some mathematical problems behind	484
I. H. Sudborough	
Time and tape bounded auxiliary pushdown automata	493
O. Sýkora	
A fast non-commutative algorithm for matrix multiplication	504
J. Tiuryn	
Fixed-points and algebras with infinitely long expressions, I	513
V. Trnková and J. Adámek	
On languages, accepted by machines in the category of sets	523

M. K. Valiev	
Real time computations with restrictions on tape alphabet	532
V. Vianu	
The Bodnarchuk metric space of languages and the topology of the learning space	537
K. Wagner and G. Wechsung	
Complexity hierarchies of oracles	543
H. Wedde and J. Winkowski	
Determining processes by violations	549
R. Weicker	
The influence of the machine model on the time complexity of context-free language recognition.....	560
K. Weihrauch	
A generalized computability thesis	570
R. Wiehagen	
Identification of formal languages	571
APPENDIX	
J. A. Goguen and J. Meseguer	
Correctness of recursive flow diagram programs	580

ON THE STRUCTURE AND PROPERTIES OF NP-COMPLETE PROBLEMS AND THEIR ASSO-
CIATED OPTIMIZATION PROBLEMS

Giorgio Ausiello
CSSCCA-CNR, Roma, Italy

SUMMARY

1. INTRODUCTION
2. ON THE ISOMORPHISM OF NP-COMPLETE COMBINATORIAL PROBLEMS
3. NP OPTIMIZATION PROBLEMS AND THEIR APPROXIMATION
4. CHARACTERIZATIONS OF CLASSES OF OPTIMIZATION PROBLEMS

1. INTRODUCTION

Since the early work of Cook (1971) and Karp (1972) the research work on the properties of NP-complete problems has been intensive and widespread. The class of NP-complete problems contains all those problems which are in NP, that is which can be decided by a nondeterministic Turing machine in polynomial time, and to which all other problems in the class NP can be reduced in polynomial time. The characterization of the complexity of NP-complete problems leads to one of the most important (may be "the" most important) open questions in theoretical computer science: does there exist any Turing machine which decides any NP-complete problem in deterministic polynomial time? In that case, from the properties of the class NP, we would deduce that all NP-complete problems would be solvable within polynomial time and the two classes P and NP would coincide.

Even if it has been proved by Baker, Gill and Solovay (1975) that the question $P = NP?$ can be positively answered in a relativized class of machines and negatively in another class of machines with different relativization and actually Hartmanis and Hopcroft (1976) have shown that there are relativized classes of machines for which the question $P = NP?$ is independent from the axioms of set theory, the practical relevance of the issue and of its possible answers in the theory of algorithms is obvious and there is a wide belief that a solution will even-

tually be achieved.

Problems which have been recognized to be NP-complete problems belong to the widest variety of fields: among them we have combinatorial problems (such as the chromatic number or the node covering of a graph and the existence of hamiltonian circuits), scheduling problems, integer 0-1 programming, satisfiability of formulae of propositional calculus, solvability of quadratic Diophantine equations, inequivalence of simple programs with only one level of iteration. For any of these problems it would have important practical consequences to know whether the backtracking algorithms of polynomial depth that we should use for deterministically solving it could ever be replaced by an efficient deterministic polynomial time algorithm.

Beside the interest related to the solution of the question of whether P is equal to NP the research activities in this area of computational complexity have brought a new light on some of the most interesting properties of combinatorial problems. The results which have been obtained can very roughly be grouped into three classes. On one side (see Simon (1975), Hartmanis and Simon (1976), Hartmanis and Berman (1976, 1977)), there has been a successful attempt to strengthening the reductions among NP-complete problems in order to point out a deep similarity among these problems. The result of showing that all known NP-complete problems are isomorphic under a polynomial time mapping and the conjecture that this is the case with all infinite NP-complete problems seem to suggest that all these problems are very similar and that they actually are polynomial time permutations of the same problem.

From another point of view optimization problems related to NP-complete combinatorial problems have been considered. The literature in this field is overwhelmingly rich because this is the direction which is the most relevant for practical purposes and whose origin is certainly antecedent to the definition of NP-completeness. An extended annotated bibliography on approximate algorithms for combinatorial NP-complete problems is provided by Garey and Johnson (1976b). The general tendency in this area, analogously to what happens in concrete computational complexity, has been to consider one problem at a time and to look for the "best" approximate algorithm, that is the approximate algorithm with the best performance either from the point of view of efficiency or from the point of view of proximity to the exact solution or both.

Among those papers which have more particular interest there are also some papers with a deep methodological insight, such as those by Johnson (1974), Sahni and Gonzales (1976), Sahni (1976), Garey and Johnson (1976a); in these papers intrinsic differences among various optimization problems appear. While in some problems like knapsack and job sequencing

we can reach any desired level of accuracy with polynomial time approximation algorithms, in some other problems, such as graph colouring, for example, any algorithm that comes too close to the optimal solution has the same complexity of the algorithms which give the optimal solution itself.

This type of results introduce a clear element of distinction among optimization problems and hence even if two NP-complete combinatorial problems are isomorphic, their isomorphism cannot be always extended to the associated optimization problems. The search for structural isomorphism among optimization problems and for classes of problems which are structurally isomorphic becomes, hence, an issue of great interest and this is the third kind of results that we want to consider in this introduction. Clearly when such a result can be proven, for those problems which are shown to be structurally isomorphic the same approximation algorithm can be used and good approximate solutions which have been found for an input in one problem can be mapped into good approximate solutions for the equivalent input in another problem. Beside these practical aspects, to be able of finding structural characterizations of classes of optimization problems and to relate their structural properties with the "degree of approximability" is certainly a relevant issue in the theory of computational complexity. Results in this direction have been achieved by Paz and Moran (1977) and Ausiello, D'Atri, Gaudiano and Protasi (1977a, 1977b).

2. ON THE ISOMORPHISM OF NP-COMPLETE COMBINATORIAL PROBLEMS

Let us first briefly review the basic terminology and notation.

Let Σ^* be the set of all words over a finite alphabet Σ . A language $L \subseteq \Sigma^*$ is said to be recognizable in time $t(n)$ by a Turing Machine (TM) M if for all $n \geq 0$, for every input x of length n M takes less than $t(n)$ steps either to accept or to reject x . If the TM is non deterministic we will consider the number of steps of the shortest accepting computation (if x is accepted) or the number of steps of the longest rejecting computation (if x is rejected).

DEFINITION 1. $NP = \{L \mid L \text{ is recognizable by a non-deterministic TM in time bounded by some polynomial } p\}$.

DEFINITION 2. A set $A \subseteq \Sigma^*$ is said to be *p-reducible* to a set $B \subseteq \Gamma^*$ (denoted $A \leq B$) if there is a mapping $f: \Sigma^* \rightarrow \Gamma^*$ which is computable in polynomial time on a deterministic TM and such that for every $x \in \Sigma^*$ $f(x) \in B$ if and only if $x \in A$.

DEFINITION 3. A set B is said to be *complete* for some class of sets C (denoted C-complete) if $B \in C$ and, for every $A \in C$, $A \leq B$.

Well known examples of NP-complete sets (problems) are:

SATISFIABILITY = {w | w is a formula of propositional calculus in CNF and there exists a truth assignment that satisfies it}.

CLIQUE = {⟨g, K⟩ | g is the encoding of a graph G, K is an integer and G has a complete subgraph of K nodes}.

CHROMATIC-NUMBER = {⟨g, K⟩ | g is the encoding of a graph G, K is an integer and G can be coloured with K colours with no two adjacent nodes equally coloured}.

DIOPH = {⟨a, b, c⟩ | a, b, c ≥ 0 are integers and the quadratic diophantine equation $ax^2 + by - c = 0$ can be solved with x, y positive integers}.

SUBSET-SUM = {⟨a₁, ..., a_n, b⟩ | there is a subsequence i₁, ..., i_m such that $\sum_{j=1}^m a_{i_j} = b$ }

JOB-SEQUENCING-WITH-DEADLINES = {⟨t₁, ..., t_n, d₁, ..., d_n, p₁, ..., p_n, k⟩ | there exists a permutation π such that $\sum_{j=1}^n (if \sum_{i=1}^j t_{\pi(i)} \leq d_j \text{ then } p_j \text{ else } 0) \geq k$.

DEFINITION 4. Two sets $A \subseteq \Sigma^*$ and $B \subseteq \Gamma^*$ are said to be *p-isomorphic* if there is a mapping $f: \Sigma^* \rightarrow \Gamma^*$ such that

- f is 1-1 and onto
- f is a p-reduction of A to B and f^{-1} is a p-reduction of B to A.

The following two theorems are both due to Hartmanis and Berman (1976) and are very important because they establish necessary conditions for two sets to be p-isomorphic; in the first case this fact can be derived from the properties of the p-reductions that hold among the two sets:

RESULT 1. Let p and q be length increasing invertible p-reductions of A to B and B to A respectively. Then A and B are p-isomorphic.

PROOF. Let us define

$$R_1 = \bigcup_{k=0}^{\infty} (q \circ p)^k \overline{\text{RANGE}(q)}$$

$$R_2 = q(S_1)$$

$$S_1 = \bigcup_{k=0}^{\infty} (p \circ q)^k \overline{\text{RANGE}(p)}$$

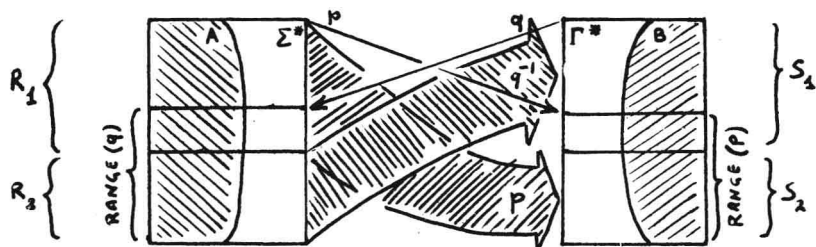
$$S_2 = p(R_1)$$

$$\varphi(z) = \begin{cases} p(z) & \text{if } z \in R_1 \\ q^{-1}(z) & \text{if } z \in R_2 \end{cases}$$

$$\varphi^{-1}(z) = \begin{cases} p^{-1}(z) & \text{if } z \in S_2 \\ q(z) & \text{if } z \in S_1 \end{cases}$$

By the properties of p and q it follows that φ and φ^{-1} are inverses and:

- φ and φ^{-1} are computable in polynomial time;
- φ is 1-1 and onto and is a p -reduction of A to B . QED



The second theorem shows instead that the existence of a p -isomorphism to SATISFIABILITY is a consequence of intrinsic properties of some NP-complete sets:

RESULT 2. An NP-complete set B is p -isomorphic to SATISFIABILITY if and only if there exists a polynomial time computable length increasing padding function S_B for B such that

- for any x and y , $S_B(x, y) \in B$ iff $x \in B$
- the padding can be obtained back by a polynomial time computable function D_B and for every x, y $D_B(S_B(x, y)) = y$.

PROOF. Let us first prove that if there is any reduction p from SATISFIABILITY to B then there is also a reduction p' which is length increasing one-one and invertible in polynomial time.

For $x \in \text{SATISFIABILITY}$ let us define

$$p'(x) = S_B(p(x), x)$$

and $t(x) = \text{if } x = S_B(p(D(x)), D(x)) \text{ then } D(x) \text{ else undefined.}$

Clearly $p'(x) = p'(y)$ implies $x = y$ and besides $t = (p')^{-1}$ and $|p'(x)| > |x|$.

In order to prove that we can also find a length increasing one-one and invertible reduction q' from B to SATISFIABILITY we only have to prove (once and forever) that also SATISFIABILITY has a padding function S and a function D with the properties stated in the theorem. Once we have proved the existence of such reductions p' and q' which are length increasing, one-one and invertible, we are in the conditions of theorem 1 to prove the p -isomorphism between B and SATISFIABILITY. QED

The intuitive meaning of theorem 2 is shown in the figure.