Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 27 (1981)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SPECKER'S MATHEMATICAL WORK FROM 1949 TO 1979
Autor: Wang, Hao
Kapitel: Complexity of algorithms
DOI: https://doi.org/10.5169/seals-51741

THEOREM 5. To every model M of Peano arithmetic, there is a proper elementary extension N of M such that all elements in $N - M$ are greater than all elements of M.

COMPLEXITY OF ALGORITHMS

In recent years under the leadership of Specker (at the E.T.H.) and Volker Strassen (at the Universität), Zürich has become a center for studies in computational complexity. One result is the volume edited by them with their lucid introduction (1976*a*). The center of interest in this volume is to consider whether each of a wide range of problems requires exponential algorithms or can be done in polynomial time. In particular, there is the famous open problem whether $P = NP$. In the Specker-Strassen volume $P \neq NP$ is called Cook's hypothesis (*Proc. of 3rd ACM Sym. on Theory of Computing*, 1971, pp. 151-158). Specker and Strassen who feel that the hypothesis is plausible present the following considerations. For example, most of the algorithmic problems in classical number theory can be interpreted as decision problems of the *NP* class and yet so far only special cases of such problems have been solved by special methods which are of the polynomial kind. Moreover, Cook's hypothesis is implied by the "spectrum hypothesis" which says that there is some spectrum whose complement is not a spectrum (the spectrum of a first-order formula F is the set of integers n such that F has an n-membered model).

The paper 1976*b* gives an illustration of the situation that sometimes what seems at first sight to require an exponential algorithm may upon closer analysis be seen to possess a polynomial one. Generalizing a result of M. Hall (1956), Specker gives a polynomial algorithm for finding distinct "independent" representations from a finite number of finite sets. (A set U of subsets of a finite set M is an independence structure over M if each subset of a member of U is a member of U, and whenever A, B belong to U and $|A| = |B| + 1$, there is some c in $A - B$ such that $A \cup \{c\}$ belongs to U. A set of representatives of M is independent if it belongs to U).

Both 1968 and 1976*c* study the question of determining the length of formulas in terms of different primitive connectives for representing each function. Essentially the concern is with Boolean functions. The formulas are built up from 0, 1 and the variables, with Boolean connectives. A central concern is to find "intrinsic properties" of functions which make

every representing formula of such a function long. In the 1968 paper one of the early lower bounds in complexity theory is established.

The results of 1968 are illustrated in a familiar manner. Let F_1 be the set of Boolean formulas with negation and conjunction as the only connectives, F_2 uses in addition also biconditional, F_3 extends F_2 by allowing also quantification over Boolean variables. It is proved that for every c, there is a formula G in F_{i+1} such that for every formula H in F_i $(i=1, 2)$ equivalent to G, the following holds:

$$\text{length of } H \geqslant c \cdot (\text{length of } G) .$$

The two parts of 1976*c* both study the problem of estimating the value of $L(f)$, giving the length of a shortest formula which represents the Boolean function f. The basic tool is the concept of subfunctions contained in a function. Let f be a Boolean function. Then g is a subfunction of f if it is obtained from f by fixing some subset of the variables of f to constants.

The second half of 1976*c* reformulates the ideas of 1968 and brings out the following corollary for symmetric functions. There is a function $t(n)$, $\lim (t(n)/n) = \infty$, such that for symmetric functions f of n variables (except 16 simple functions for each n), $L(f) > t(n)$.

Based on the kind of technique introduced in 1968, Fisher, Meyer and Paterson (in paper presented at the 7th ACM Symp. on Theory of Computing, May 1975) have proved lower bounds of up to $n \log n$ for a more restricted class of symmetric functions.

The first half of 1976*c* sharpens a result of E. E. Neciporuk (*Soviet math. dokl.*, vol. 7, 1966, pp. 999-1000) and makes three applications. The main result gives a lower bound to $L(f)$ by counting up subfunctions of f:

Roughly speaking, if f is a Boolean function of m variables, and G is a formula representing f with $L(G)$ defined as the number of occurrences of the m variables, then $L(G) > (\Sigma \log e_i)/\log 5$, where e_i is the number of subfunctions over X_i $(i=1, ..., j$ for some $j)$, and $X_1, ..., X_j$ make up a partition of the m variables of the function f.

Specker's most recent publication is 1979*a* which is apparently still in galley proofs. This relates more directly to the $P = \text{NP}$ problem in the central case of the tautology problem. Let F be a formula in the conjunctive normal form (CNF). It is said to be 2-satisfiable if any two clauses are simultaneously satisfiable. For example, $p, q, \bar{p} \vee \bar{q}, p \vee q$ is 2-satisfiable but not satisfiable. Let h be the "golden ratio" $(\sqrt{5}-1)/2 \doteq 0.618$, which is the positive solution of $h^2 + h - 1 = 0$.

It is shown that for 2-satisfiable F in CNF, there exists a satisfiable subset of the clauses $C_1, \ldots, C_n$ in F which has hn members. Moreover, there is a polynomial algorithm to find such a set. On the other hand, for any $h' > h$, there is some 2-satisfiable F which contains no satisfiable subset of at least $h' \mid F \mid$ members ($\mid F \mid$ being the number of clauses in F).

Let $Z(a)$ be the set of CNF's such that each F in CNF has an interpretation satisfying $a \mid F \mid$ clauses. The construction problem of $Z(a)$ is to compute for each F in $Z(a)$ an interpretation which satisfies at least $a \mid F \mid$ clauses. In this terminology it is well-known that $P = \text{NP}$ iff the construction problem of $Z(1)$ is in P. The result mentioned above shows that the construction problem for 2-satisfiable CNF's in $Z(h)$ is in P. Let now h' be an algebraic number such that $1 \geqslant h' > h$. A somewhat mysterious result is then given: the construction problem for all 2-satisfiable CNF's in $Z(h')$ is in P, iff $P = \text{NP}$. In other words, the set of 2-satisfiable CNF's which belong to $Z(h')$ is NP-complete.

Specker and his coauthor remark that under Cook's hypothesis (i.e., $P \neq \text{NP}$), there is a "quantum jump" at h, because at this point, the complexity of computation passes over from P to NP which is no longer polynomial under Cook's hypothesis. They do not mention whether they consider their result to be positive or negative evidence for Cook's conjecture. Over the years I have asked several experts why they believe in the conjecture and have failed to be convinced by the reasons they give. I continue to feel that our state of ignorance today is such that nothing is known to make $P \neq \text{NP}$ seem more plausible than $P = \text{NP}$.

According to Specker, the most important implication of 1979*a* is to draw attention to the golden ratio: we should not expect to fulfill more than 61.8% of our wishes.

Specker's Mathematical Publications (1949-79)

1. 1949*a*. Die erste Cohomologiegruppe von Überlagerungen und Homotopieeigenschaften dreidimonsionaler Mannigfaltigkeiten. *Commentarii Mathematici Helvetici*, vol. 23, pp. 303-333. Promotionsarbeit for Doctor of Mathematics at ETH, June, 1948.
2. 1949*b*. Nicht konstruktiv beweisbare Sätze der Analysis. *Journal of symbolic logic*, vol. 14, pp. 145-158.
3. 1949*c*. Sur un problème de Sikorski. *Colloquium Mathematicum*, vol. 2, pp. 9-12.
4. 1950*a*. Endenverbände von Räumen und Gruppen. *Math. Annalen*, vol. 122, pp. 167-174.