Typical ambiguity and model theory

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **27 (1981)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **10.08.2024**

Typical ambiguity and model theory

The commonly accepted cumulative or iterative concept of set can be viewed as an extension of the simple theory of types to the transfinite. It is often helpful first to confine attention to this simple theory both for exposition and for finding out new facts. For example, Gödel apparently studied the independence of the axiom of choice and the continuum hypothesis in this framework in the 1940s. A tempting question is to look for other extensions of the simple theory of types.

The family of structures intended by the theory is altogether familiar and natural. Let T_0 be a (nonempty) set; elements of T_0 are elements of type 0. T_1 is the set of subsets of T_0; T_2 is the set of subsets of T_1; and in general T_{n+1} is the set of subsets of T_n. We have variables $x_1^0, x_2^0, \ldots, x_1^1, x_2^1, \ldots$, etc. and prime formulas of two kinds such as $x_4^3 = x_2^3$ and $x_6^2 \in x_6^3$. In this way the language is determined in the obvious way. The intended structure $(T_0, T_1, \ldots, \in, =)$ has $\in$ and $=$ interpreted in the usual way and T_{k+1} taken as the power set of T_k. The axioms are of two groups and they make up the axiom system T $(n=0, 1, 2, \ldots)$:

T1. Extensionality. $\forall x_1^n (x_1^n \in x_1^{n+1} \leftrightarrow x_1^n \in x_2^{n+1}) \rightarrow x^{n+1} = x_2^{n+1}$.

T2. Comprehension. $\exists x_1^{n+1} \forall x_2^n (x_2^n \in x_1^{n+1} \leftrightarrow C(x_2^n))$.

Let F^+ be obtained from F by raising the superscripts of every variable in F by 1. A direct result on the system T is:

Theorem 1. If F is a theorem of T, so is F^+.

The converse is certainly not true. Since T_0 is nonempty, we can easily prove there are at least 2^n objects of type n. E.g., we can prove:

$$\exists x_1^1 \exists x_2^1 (x_1^1 \neq x_2^1),$$

call it S^+. But we cannot prove S in T. Once I suggested an extension N of T to include negative types (*Mind*, vol. 61, 1952, pp. 366-368), with the axioms T1 and T2 reconstrued so that n may also take negative integers as values. It could then be shown that, for every n and every given positive k_0, there are more than k_0 sets of type n. Yet it can also be shown in elementary number theory that N is consistent. Hence, for no fixed type n can one prove in N an axiom of infinity (i.e., there are infinitely many sets of type n).

Specker considers a theory T' obtained from T by adding the rule: if $\vdash S^+$, then $\vdash S$. He shows that T' is consistent and every model of N yields one of T'. The more difficult question is whether the system T^+ obtained from T by adding the axiom (scheme) "$S \leftrightarrow S^+$" is consistent. In the paper 1958 (=13), Specker proves the following theorem:

THEOREM 2. The system NF is consistent if and only if T^+ is.

In this way one gets a more natural characterization of NF in terms of "typical ambiguity", because T^+ may be said to be the result of taking typical ambiguity seriously.

In the paper 1962 (=17), Specker further proves:

THEOREM 3. If T^+ is consistent, then there exists a model $(M_0, M_1, ..., \in, =)$ which admits an isomorphism mapping M_k onto M_{k+1}.

In 1969, Ronald Jensen combined Specker's way of constructing models with an interesting use of Ramsey's theorem to get yet another surprising result about NF: If the extensionality axiom is weakened to allow individuals (urelements), then the resulting system NFU can be proved consistent in elementary number theory so that the axiom of infinity is not provable in NFU (*Words and objections*, pp. 278-291).

This contrasts with Specker's result of 1953 (=6):

THEOREM 4. The axiom of choice is refutable in NF and so the axiom of infinity is a theorem of NF.

Some time before this, I had remarked on a possible application of Skolem's theorem on countable models. Since NF is known to have a finite axiomatization (T. Hailperin, *Journal of symbolic logic*, vol. 9, 1945, pp. 1-19), I thought that by applying the axiom of choice, one can introduce in NF a set which essentially enumerates a countable model of NF, so that by the diagonal argument a new set and a contradiction can be derived. But my enumeration used an unstratified formula and I do not know whether one can remedy this by some trick to get an alternative proof of Theorem 4.

In regard to the construction of models, jointly with MacDowell, Specker has proved the following well-known theorem (1961*a* = 15; compare also *Handbook of mathematical logic*, p. 79):

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