ON THE MEANING OF "THE READER WILL EASILY VERIFY"

By John McCarthy

Logicians occasionally complain that the proofs given by mathematicians are incomplete almost to the point of non-existence. Mathematicians sometimes retort that a proof that would satisfy the logician would have to be fifty times as long as is customary. It seems desirable to find a way of writing proofs which will be completely rigorous in the sense that they can be algorithmically verified and yet will be as concise or even more so than the proofs customarily given by mathematicians.

If the theory T in which the theorem $\vdash$ occurs has a decision procedure P the proof can simply say $\vdash$: by the decision procedure P or more simply $\vdash$: P. However, the more interesting theories do not have decision procedures. Nevertheless, perhaps any theory whose proofs are made from a finite number of axioms and rules of inference can be divided into a number of subtheories T_1, ... T_k with decision procedures P_1, ..., P_k such that any proof can be written: $S_1 : P_{i_1}$

$S_2 : P_{i_2}$

.

.

.

$\vdash = S_n : P_{i_n}$

where the jth step means that S_i follows from the axioms and rules of inference of the subtheory T_{i_j} and the S_{1_j} ..., S_{j-1} by means of the decision procedure P_{i_j}.

If one admits pseudo-subtheories on which the length of proofs are bounded then it is trivial that the decision prodedures can be found, in fact if the pseudo-theories consist of a single application of a rule of inference, then any proof is of that form.

The interest of the ideas depends on two things:

1. That the decision procedures should be good enough so that they will decide whether a conjecture follows from an

arbitrary number of applications of the axioms and rules of inference of the subtheory. This can be assured if the rules of inference either only shorten or only lengthen formulas.

2. There are a small number of subtheories and the interesting theorems turn out to be not excessively deep. We define the depth of a theorem with respect to a collection of subtheories to be the length of the shortest sequence $S_1 : P_{i_1}$, $S_2 : P_{i_2}$, ..., $S_n : P_{i_n}$, $S = \top$ which constitutes a proof.

It is not necessary that the various subtheories be independent. In fact one suspects that many of the subtheories used in mathematics will consist mainly of derived theorems.

The length of a proof will as described above be the number of terms in the S:P sequence, but the length alone of the sequence does not characterize the difficulty of verifying a proof. If we regard the decision procedure as constituting a program on some fixed computer, the number of computer steps may be taken as measure of the size of each step of the proof. Frequently, even though an S_j follows from the previous S_j's by one of the decision procedures the insertion of an intermediate step may reduce the size of the proof.

To return to the subject of the title we suggest that a mathematical reader may be regarded as a finite collection of decision procedures by subtheories, of the theory in which the author is working. Since there are only a finite number of such procedures the author does not need to say which one is to be applied to a step of the proof although the reader can usually guess which one is meant. "The reader will easily verify" is an assertion that one of the reader's decision procedures will justify the proof.

In the conculsion we wish to express the conviction that a number of interesting branches of mathematics such as elementary number theory, the theory of finite groups, and to take a more esoteric example, the theory of the category of

finitely generated abelian groups and their homomorphisms can be divided into decidable subtheories with profit. If this can be done it should make them easy to expound and give even the most nervous logician full confidence in the proofs.

June 28, 1956