Зборник радова Математичког института, Нова серија, књ. 2 (10), 1977.
Recueil des travaux de l'Institut Mathématique, Nouvelle série, tome 2 (10), 1977,

Symposium: Set theory. Foundations of Mathematics, Beograd, 29.08 — 2.09. 1977.

FROM FOUNDATIONS TO SCIENCE: JUSTIFYING AND UNWINDING PROOFS

Georg KREISEL

Abstract. The first part of this paper recapitulates the general scheme of using techniques developed for discredited foundational aims; specifically, proof theoretic techniques developed for carrying out Hilbert's programme. Since this programme relies on formalization, that is, mechanization, an obvious use is in the mechanical 'handling' of proofs. — The second part of the paper considers three different kinds of 'handling:' finding, checking and unwinding (transforming) proofs. The principal, generally neglected conclusion is that mechanical unwinding presents the most promising application of proof theoretic techniques; particularly where the passage from the informal proof considered to a formalization of its *relevant* features is not particularly problematic. Examples of such cases are proposed.

I. Background

It is a commonplace that the notions and problems (formulated in terms of such notions) which occur to us when we know little about a subject are liable to lose their prominence when we know more. This shift occurs even when, realistically speaking, the notions are quite precise. Here are two examples from so to speak opposite extremes in the case of formulae and proofs.

1. When we know little, *length* of formulae (measured by the number of symbols) will occur to most of us as a subjct of study. It is quite precise for any given notation. But as we go into the subject, we find that length does not determine the mathematical 'behaviour' of formulae at all well; for example, in many decision procedures a bound on the number of quantifier alternations is much more significant. This kind of thing is familiar from the natural sciences: The (mechanical) behaviour of bodies is determined more by their weight and moments of inertia than by their colour or (details of) their shape though colour and shape strike the eye most.

2. When we know little, the first and often almost the only Yes-No question to ask about a proof is whether it is *valid* or, perhaps, whether it uses valid *principles*. Of course this question is meaningful (and often the answer is negative when we have little experience with the subject; for example, a hundred years ago

one applied the power set operation to what Cantor called a *Vielheit*, e.g. the universe). But as we go into the subject we often reach a stage when any analysis or — as one says — justification of the principles is unrewarding in a quite precise sense: any analysis (tacitly: in terms of current concepts) is less convincing than the recognition (=constatation, Konstatierung) of validity. This kind of thing is familiar from experience with children who learn only slowly when it is (intellectually) unrewarding to ask: Why? — The case-study in the Appendix illustrates in detail how experience with the subject matter affects the recognition of validity.

Perhaps the most famous attempt to pursue questions of validity to the bitter end is Hilbert's programme. Fairly recently, I have set out what I believe we have learned from work on this progamme [4]. The idea was to justify abstractly valid principles by the following kind of reduction. If an elementary statement has a proof π by such principles then it has also a proof π_e by elementary means. And if the principles are *formalized*, the reduction is, in turn, expressed by an elementary statement (for details, see [4]). The latter should be proved by elementary means, once and for all; cf. Hilbert's famous 'final solution' ([4], pp. 111—112).

As is well-known, the most striking so to speak legalistic defect of Hilbert's programme is established by Gödel's incompleteness theorem; naturally modulo second thoughts about abstract validity. A far more *specific*, and *therefore more convincing* defect is established by looking at particular abstract principles which have been reduced according to Hilbert's aim, and to see what is gained or lost by the reduction; cf. [4] pp. 116—117. Indeed, quite generally, defects of reductions are most easily seen in cases where they have been carried out, where Ockham's razor has been applied. Otherwise there is always a lingering doubt that we shall see something new and marvellous when 'unnecessary' growth has been removed.

Be that as it may, it is quite clear that the 'reductions' involve transformations of proofs: $\pi \to \pi_e$. And even if one has no doubts about (the validity of) π or less doubts about π than about π_e (for example, because π_e is more involved than π and so has a higher chance of containing copying errors), there remains the possibility that π_e *tells us something we want to know that* π *doesn't.* Finding that 'something' becomes a principal problem: it may need more imagination than the step from π to π_e.

Remarks. (a) The problem above, of exploiting work done for the sake of discredited aims, is familiar in the philosophy of science under the somewhat grandiose heading: *Logik der Forschung* (logic of scientific discovery). It is very popular among scientists working on cosmology or theories of evolution where such problems are the order of the day. (b) In particular, what were principal notions or principal results for the discredited aims turn into lemmas, of interest only when reformulated, and combined with other constructions. A good example is provided by so-called consistency proofs using ε_0-induction, reformulated as a formal equivalence between the logical principle of soundness (=reflection) and the mathematical principle of ε_0-induction ([4], p. 121, l. 7—8). This has recently been combined with combinatorial arguments by Paris and Harrington [7], who established an equivalence to a 'more' mathematical principle, namely their version of Ramsey's theorem, to which we return in the Appendix.

II. Mechanical Handling of Proofs

For familiar foundational reasons which were recalled above, *formalization* of the principles studied (of course not: of the metamathematical methods used) is needed for Hilbert's programme. Others tried to connect formalization with mathematical rigour, which requires metamathematical arguments to be formalized too. However far-fetched all this may be for the phenomena of mathematical reasoning itself, formalization or, equivalently, mechanization is an obviously essential element in the use of digital computers. since they operate only on formal data.[1] We consider here three kinds of uses: *finding* proofs, say for a given conjecture; *checking* proofs, of a given assertion; and *transforming* proofs, for example, a prima facie non-constructive proof of an existential theorem into a realization, an analytic proof of an algebraic theorem into an algebraic one, and the like.

1. *Past experience: computation and highbrow mathematics.* Of course, the huge bulk of computer uses in pure or applied mathematematies concerns computations or, more generally, classes of assertions A, for example, equations $t=t'$, for which decision methods are known that can be realistically implemented by a computer. So formulated, the uses *can* be regarded as examples of finding or checking proofs; for example, if we think we have an argument for A, but are not sure[2]. However, the only feature of the argument which is relevant to this use is the conclusion A itself. The computer checks the *result* of the argument, and does not look at its details. Put differently, given the result, the computer makes a fresh start. As a corollary, the third type of use mentioned above, the transformation of proofs, does not occur here at all.

In high-brow mathematics the situation is different. Finding and checking proofs are, at least generally, done without using mechanical rules. This is a commonplace as far as discovery is concerned. But also checking is rarely done mechanically, for example, by careful comparison with some given set of formal rules (mathematicians make logical inferences, but seldom remember rules of predicate calculus even after having seen them). By far the most efficient checking is done by comparing or confronting intermediate steps with what is known already, possibly in superficially quite different parts of mathematics. This is of course related to discovery where results from different areas of knowledge are combined. In short, for the phenomena of mathematical reasoning just mentioned the business of formalization seems quite far-fetched.

In contrast there is another part of high-brow mathematical activity which does have a mechanical look, namely the analysis or unwinding of proofs; it is mechanical, once one has decided *what* to read off the proof. As a matter of empirical fact (cf. p. 113—116 of [5]), though mechanical, this unwinding occasionally makes one's head spin, and one gets lost — as in computations with large numbers. From this point of view it is promising to use computers for such unwinding. And, as suggested by Part I, methods developed in traditional proof theory turn out to be relevant here.

[1] Many instruments which are called 'computers' are here thought of as combining a (central) digital computer and a (peripheral) analogue device; the latter may operate on, say, continuous data, and then supplies the computer with discrete formal data.

[2] An 'essential element' and not necessarily the sum total; for example, if we are interested in a conjecture A, *one* type of use of a computer is to present not a formal proof of A, but of $P_A \rightarrow A$ with an invitation to the user to consider if P_A is valid.

Reminders. To avoid a general air of unreality, it is as well to recall at this point a few simple facts. (a) Naturally, even if the programme of unwinding works out, it cannot be expected to be of comparable importance to, say, high speed computation. This is a particular case of the truism that the use of computers *within* mathematics is a very minor part of the total picture. (b) Conversely, inasmuch as the programme is useful, it cannot be expected that *clever* mathematics will often play an essential role. This is a particular case of the fact of experience, say in operational research, that one rarely gets a startling gain in efficiency by some new mathematical device for solving a (decision) problem. Far more often does one get an improvement by spotting constraints on the problem (as originally stated): one finds that in practice only few of the assertions occur which were thought to be relevant at first blush. Actually, this point applies to some extent within mathematics too when there are high, say exponential bounds for deciding all formulae of the class C; the practical conclusion is that one had better look for a more amenable class, say a subclass of C. (c) But also one should remember that there are *occasional* exceptions to the general features of present day high-brow mathematics emphasized above. The proof of the four-colour-conjectuie by Haken and Appel (explained in [1] with the benefit of advice from professional scientific journalists) was certainly *discovered* by a high-brow use of computers. At our present stage of experience it is as reasonable to look for a *check* without the use of computers as it would have been a hundred years ago to look for a finitist proof of a theorem discovered non-constructively.

2. *The passage from informal to formal proofs: the alleged spanner in the works.* When one speaks of (mechanically) unwinding or, generally, transforming proofs, one has to have a proof to start with! So naively, it seems we need machinery to pass from some given informal proof π to corresponding formal data π' and perhaps (b) that, for a *mechanical* transformation, π' has to be built up by *formal* rules. Both these ideas are quite naive. The first neglects general experience in the application of theories, the second specific experience in proof theory.

(a) What is needed is a formal representation of those features of π which are *relevant* to the transformation. Sure, one *can* ask: How do you know what is relevant, (as a child asks: Why?) But, before one imposes unrealistic demands on uses of proof theory, it is much more profitable to remember how mathematical theories are applied elsewhere. If physical theory is to be applied to some phenomenon, say the motion of the planets, it is left to the physicist to discover the physically significant features of the phenomenon. There is no 'machinery' for deciding whether chemical composition or cosmic radiation is significant — and if there were, the application of the machinery might take so long that the more significant features (position and velocity) are already out of date. The physicist uses a certain familiarity with the phenomena to spot the significant features.

And physical theory *is* of use whenever the effort involved in the passage from the raw phenomenon to the choice of data is not out of all proportion to the effort of applying the theory to those data.

(b) For the kind of unwinding mentioned in § 1, most details of a proof are *not* relevant; for example, none of the details involved in proving so-called identities, that is, $\prod_1^0$-axioms, and if the latter are true then the transformed proof will again use only true ($\prod_1^0$) axioms.

As a corollary, when we have the job of unwinding a proof π, we shall look for chunks of the proof that are used only for proving $\prod_1^0$-theorems, and suppress them altogether from the representation π' to which the proof theoretical transformation is applied; cf.: a physicist who is given data including the spectral lines of the light coming from a planet, will ignore this optical information if his job is to determine the motion of the planet.

The fact that proof theoretic methods are occasionally of use, is not in doubt. As documented in [5], pp. 113—116, even without a computer they have been applied to unwind proofs, and to extract information which the discoverers of those proofs wanted to know and did not find by themselves. Spotting relevant features of those proofs was not a major obstacle.

NB. Of course there is intrinsic logical and above all aesthetic interest in giving a closer analysis of the passage from informal proofs to (relevant) formal representations. But under ordinary circumstances the use of such a scheme is more likely to hamper than to help the effective application of computers in the unwinding of proofs. — The reader should compare here cases of mechanizing the choice of relevant features in natural science. This was necessary, for example, when sending a *robot* to Mars to look for life, since only a limited number of types of measurement (of supposedly relevant data) could be incorporated. The robot was surely much better than a scientifically untrained or thoughtless observer. But perceptive scientists on the spot would surely have done better than the robot by *not* restricting themselves to a prescribed repertoire.

3. *New examples of candidates for mechanical unwinding.* The 'new' examples are here regarded as a continuation of those discussed in [5], pp. 113—116 (where also some loose ends are pointed out which can probably be tied up by use of a computer). The 'old' examples concerned questions raised by distinguished mathematicians about their own proofs, and so it was reasonable to take the interest of the questions for granted. The interest of the new questions will be discussed briefly at the end of (a), respectively (b) below; 'briefly' because, as always, only the general interest of an open problem can be decided, the exact interest depending on the specific solution.

Warning. To fix ideas the unwinding considered below is done by normalization or cut elimination (so that one ends up with a cut free proof). This is fine for realizations of existential theorems. It is not good for finding, say, a first order proof which corresponds to a higher order proof (of say, a logical theorem). Giving a better unwinding, which in general associates a (first order) proof *with* cut to higher order proofs, is certainly a *principal open problem.*

(a) Milnor [6] showed by use of topological arguments that the only (possibly non-associative) division algebras over a real closed field have dimenmensions 1, 2, 4, 8. So, for each integer $n \neq 1, 2, 4, 8$ there is a purely logical proof of the non-existence of a division algebra of dimension n from the axioms of real closed fields, since the property of being the multiplication table for such an algebra is expressed by a first order formula.

Problem. What do the (purely) logical first order proofs look like, which are obtained by unwinding Milnor's proof (say, for $n=16, 64, 256$)?

Reminder (from §2). Naturally, one will not formalize many details of Milnor's proof, but only those steps which are relevant to the unwinding procedure.

It is known that Milnor's result does not extend to all (ordered) fields. A standard counter example is the following commutative and associative division algebra of dimension 3 over the rationals:

The elements are of the form

$$a+b\sqrt[3]{2}+c\sqrt[3]{4},$$

where a, b, c are rational.

Sums and products are defined as usual, that is, for the field of rationals extended by $\sqrt[3]{2}$.

The irrationals $\sqrt[3]{2}$ and $\sqrt[3]{4}$ satisfy cubic equations. This is optimal since inspection of standard methods yields the following:

Corollary: For all odd n Milnor's result holds for ground fields in which every polynomial of degree n has a zero (The fields need not be real closed).

Discussion. Mathematically speaking, the problem of unwinding presents a *risk*; specifically, when more is lost than gained. (A — conscious or unconscious — attraction of finitist foundations consisted in apparently removing this risk by the claim that the unwinding was needed for *justifying* Milnor's proof). The corollary above indicates *one* kind of possible gain, incidentally in terms of conventional concepts. The unwound proof will exhibit the particular (finite subset of) axioms for real closed fields that are needed for the conclusion, and may thus suggest a neat *generalization* of Milnor's result (to a larger class of fields). — On the other hand, foundationally or pedagogically speaking there is no risk. There are sufficiently many people with foundational *convictions* that unwinding is either always or never informative, that somebody is bound to learn something from the unwinding.

(b) When — in contrast to (a) above — both mathematical and logical proofs of some (logical) formula are actually available, unwinding is used to *compare* the proofs. For example, suppose DO are (first order) axioms for dense orderings without first or last element, and that F is a formula in the language of DO with the single free variable x. Then $\mathrm{DO} \rightarrow \forall x \forall x' (F \Leftrightarrow F')$ where F' is $F[x/x']$. For each such F, the implication can be proved by elimination of quantifiers, but also (mathematically) by use of the categoricity of DO for countable models and their automorphisms. The mathematical proof can be formalized in type theory, and unwound by normalization: but we really have no idea what the resulting (logical) proof looks like.

Discussion. One, very familiar way of *expressing* the malaise produced by the existence of such spectacularly different proofs is to doubt the validity of the set-theoretic notions used in the mathematical proof. But note that there are also non-ideological doubts about — the concepts needed to state — structural relations between those proofs.

Appendix : a case study

The purpose of this appendix is to expand the general discussion in Section I by reference to a specific case. Plenty of familiar material could be used for this purpose, for example, the discovery and recognition of any of the basic current axiom systems. But I (and the readers likely to profit from this article) find hackneyed examples distasteful, and so a very interesting recent discovery by Paris, already mentioned in the text, will be used instead. Besides, there is no analysis in print which puts this discovery into a broad context.

Paris discovered a striking variant RT_A('A' for arithmetical) of Ramsey's own finite version RT_F of his theorem RT on partitions of the set of pairs of a countable infinite set; for exact statements, see [7]. According to the title of [7], the most remarkable property of RT_A is that it is a 'mathematical' theorem which can be stated but not proved in first order arithmetic. As already indicated at the end of Part I, this alone is not particularly convincing since ε_0-induction (for, say, the complete $\prod_1^0$ predicate) is hardly any more meta-mathematical than RT_A, and has been known for more than 40 years to have the same remarkable property. This is made precise at the end of (b) below.

(a) As for background, it has been known since the work of Jockusch [2] that RT itself cannot be proved in most 'usual' conservative extensions of first order arithmetic with full induction; more specifically, any finite subset of axioms of those extensions is satisfied by some (finite) segment of the arithmetic hierarchy, and RT is not. On the other hand, RT_F itself can be comfortably proved in first order arithmetic, in fact, bounds for the corresponding Ramsey functions lie in E_4—E_3 of Grzegorczyk's hierarchy of the primitive recursive functions; cf. [8] p.140, Lemma 6.

(b) *Validity of* RT_A. Far and away the simplest proof of RT_A uses a deduction (by compactness) from RT itself. The same applies to RT_F.

Corollary. Taken in their literal sense, as $\prod_2^0$ theorems, a separation between RT_A and RT_F (so to speak, on the ground of a different 'kind' of validity) is suspect. — More precisely, as cannot be repeated too often, it is an *assumption* that the classification of theorems according to formal derivability in any particular (incomplete) system is significant. The discovery that RT_F and RT_A are separated by this classification, using first order arithmetic, casts doubt on the assumption

The situation changes if interest shifts from the literal sense to *bounds* for Ramsey functions, specifically *upper* bounds. NB. It is a striking discovery that, in contrast to the bulk of elementary mathematics, this shift is significant here: usually bounds are read off quite directly from a proof of a $\prod_2^0$ theorem.

Proofs via RT supply α-recursive bounds for some $\alpha<\varepsilon_{\varepsilon_0}$, by [3] inasmuch as the most obvious formalization of the proof of RT uses $\prod_1^0$—analysis (which is formally identical to the theory of the first level of ramified analysis [9]). As always this can be improved by bounding the complexity of the induction schema used in the proof of RT. — Evidently, these bounds are far beyond E_4 which, by above, bounds the original Ramsey functions (of RT_F).

The proof of RT_A in [7], via the so called $\sum_1^0$-reflection (or soundness) principle for first order arithmetic, supplies an ε_0-recursive bound. This follows from — one direction of — the well-known equivalence, for example, in 1. 7—8 on p 121 of [5], between ε_0-induction and the reflection principle. For reference below: the bound in question is *primitive recursive* in f_{ε_0}, the particular ε_0-recursive function of Wainer's hierarchy (used in [10]).

Discussion. Realistically speaking, this proof, though very agreeable to a logician, is unsatisfactory for those who really want to know bounds for Ramsey functions. (After all, for a logician, consistency is a much more interesting assertion than RT_A!) The proof requires the verification that a number of arguments *can* be formalized in first order arithmetic; evidently, a delicate matter (for a novice) in a context where there are also arguments which cannot be so formalized, specifically, proofs of RT_A!

The best upper bound for RT_A so far obtained is $f_{\varepsilon_0}(n+4)$, in [10]. The proof uses a careful proof-theoretic analysis of subsystems of first-order arithmetic in terms of Wainer's hierarchy.

It seems plausible that the machinery of [10] can be developed to give this bound by means familiar to the *principal consumer*, the combinatorial mathematician interested in RT_A. Specifically, one would use an ordering (of type ε_0) of finite partitions, called 'algebras of sets' in [10], and one would apply induction on that ordering to a combinatorial property of such partitions. In contrast, the unwinding of the proof of RT_A in [7] together with the deduction of $(\sum_1^0-)$ reflection from $(\sum_1^0-)$ ε_0-induction uses orderings of infinite cut-free proof trees and unfamiliar (derivability) properties of formulae at the nodes of those trees.

(c) *Formal underivability of RT_A : lower bounds.* Once again, a number of proofs are available. First of all, there are more or less familiar constructions of models, originally by Paris, later by Kochen-Kripke (unpublished), in which RT_A fails. By itself, this does not establish any lower bounds at all because, after all, even a (numerically) true $\prod_1^0$ statement can be formally underivable. The device used here is to have models in which all true $\prod_1^0$-statements hold, and appeal to the fact that, for $\alpha<\varepsilon_0$, all α-recursive functions are provably recursive. If a $\prod_2^0$-statement $\forall x \exists y A(x, y)$ has an α-recursive bound, defined by a Gödel-number e_α, then the $\prod_1^0$-statement

$$(*) \qquad \forall x \forall z \{T(e_\alpha, x, z) \rightarrow \exists y [y < \mathrm{U}(z) \wedge A(x, y)]\}$$

is true, $\forall x \exists z\, T(e_\alpha, x, z)$ provable, and so $\forall x \exists y\, A(x, y)$ is derivable from (*).

Corollary (for people interested in the formal independence of $\sum_1^0-\varepsilon_0$-induction). Once one has (i) a model in which all theorems and all true $\prod_1^0$-sentences of arithmetic do, but RT_A does not hold, and (ii) any ε_0-recursive *upper* bound for RT_A (as in (b) above), it is immediate that f_{ε_0} is not provably recursive.

Secondly, there is the proof in [7] which derives the $\sum_1^0$-reflection principle (in primitive recursive arithmetic) from RT_A. Appealing again to the proof theoretic equivalence mentioned in (b), we find that any Ramsey function *enumerates* all α-recursive functions for $\alpha<\varepsilon_0$, and so cannot be equal to any such function. Trivially, as in (*) above, no Ramsey function could be dominated by any such function either. In terms of Wainer's hierarchy (in [10]) : f_{ε_0} is *primitive recursive* in any bound for RT_A. This is done by unwinding the proofs of (i) $(\sum_1^0 -)$ reflection from RT_A in [7] and (ii) of $(\sum_1^0 -)$ ε_0-induction from $(\sum_1^0 -)$ reflection.

Again, neither of the proofs mentioned can be satisfactory to the principal consumer because it involves the passage from provably recursive to $<\varepsilon_0$-recursive functions. Only the latter are so defined that the property in question, rapid growth, is evident.

The third proof, by Solovay [10], shows, in terms familiar to the combinatorial mathematician, except for the notion

$$\alpha\text{ - recursive function: } \alpha<\varepsilon_0,$$

that all such functions are almost everywhere *lower bounds* for Ramsey functions of RT_A. In fact, by [10], $f_{\varepsilon_0}(n-4)$ is a lower bound.

Discussion. There is, I believe, a useful parallel between Solovay's proof and Higman's well-known characterization of subgroups of finitely presented groups (ignoring for the moment the relative interest of this part of group theory and of the partition calculus resp.). Higman discovered that a few *notions* of recursion theory combined with a good deal of group theory permit a satisfactory answer to the question:

Which finitely generated groups can be embedded in finitely presented groups?

Solovay succeeds in using a notion first thrown up in proof theory to answer the question:

How fast do Ramsey functions of RT_A grow?

Certainly, no bounds anywhere in combinatorial (or other ordinary) mathematics, have ever come near the (lower) bounds for RT_A. A critical view of traditional proof theory, specifically of the consistency programme was of some help (as claimed at the end of Part I) because — on the traditional view — the emphasis on extensional properties of provably recursive functions is quite trivial compared to the metamathematical methods used in the consistency proof.

Remark. Just as the discovery (in [8], 16. 4, based on section 14 about infinite cardinals) of the original lower bounds for RT_F, Solovay's argument obviously involves the fruits of experience with infinitary partition calculus. This is a counterpart to Jensen's successful use in (infinitary) set theory of some developments in proof theory of Bachmann's ideas for defining fundamental sequences. Certainly, not everything is the same as everything else (unless viewed very superficially). But the *particular* traditional distinctions between 'the' finite and 'the' infinite are not all that important as far as proofs are concerned; certainly less than appears to the inexperienced.

Bibliography

[1] K. APPEL and W. HAKEN, *The solution of the four-color-map problem*, Scientific American (Oct. 1977) 108—121

[2] C.G. JOCKUSCH, *Ramsey's theorem and recursion theory*, J. Symb. Logic 37 (1972) 268—280.

[3] G. KREISEL, *Ordinals of ramified analysis*, (abstract) J. Symb. Logic 25 (1960) 290—391

[4] G. KREISEL, *What have we learnt from Hilbert's second problem?* Proc. Symp. Pure Math. 28 (1976) 93—130

[5] G. KREISEL, *On the kind of data needed for a theory of proof.* Pp. 111—128 in: Logic Colloquium 76, ed. Gandy and Hyland, North Holland 1977

[6] J. MILNOR, *Some consequences of a theorem of Bott*, Annals of Math 68 (1958) 444—449

[7] J. PARIS and L. HARRINGTON, *A mathematical incompleteness in Peano arithmetic.* Pp. 1133—1142 in Handbook of Mathematical Logic, ed. J. Barwise, North Holland 1977.

[8] P. ERDÖS, A. HAJNAL and R. RADO, *Partition relations for cardinal numbers.* Acta Math. Hung. 16 (1965) 93—196

[9] K. SCHÜTTE, *Proof Theory*, Springer Verlag 1977.

[10] R. M. SOLOVAY, *Rapidly growing Ramsey functions* (to appear)

Stanford University
Dept. of Philosophy
Stanford California 94305
U.S.A.

PS (added March 1978). Since this paper was written, Part (b) of the Appendix has been improved. (i) On the formal side several of us noticed that ε_0-induction (applied to arithmetic predicates) axiomatizes the arithmetic theorems, and hence

$$\sum_1^0 -\alpha-\text{induction: } \alpha<\varepsilon_1$$

the $\prod_2^0$—theorems which follow from RT in Δ_1^0—analysis with induction restricted to arithmetic predicates (with parameters). (ii) More interestingly, J. KETONEN established the conjecture at the end of (b), proving RT_A by induction on (a predicate involving) the membership relation in H^α, for $\alpha\leq\varepsilon_0$, where H^α is his hierarchy of so called α-large, finite sets of natural numbers. (The relation is coded arithmetically). His proof uses a general scheme for weakening *suitable* definitions D of familiar closure conditions on ordinals $\varkappa$ (Mahlo, weakly compact, n-subtle); roughly speaking, by rewriting (set-theoretic) D in combinatorial language D_c where the variables for ordinals used as indices are separated from those used as elements of sets. As a result it makes sense to let the set quantifiers in D_c range over $\varkappa$-large sets of natural numbers in place of arbitrary subsets of ordinals $<\varkappa$. Ketonen's proof of RT_A shows that ε_0 is the least ordinal which satisfies (the latter, arithmetic interpretation of) $\omega—S_c$ where ω-S is the appropriate definition of *n-subtle for all n* as a partition property. -Ketonen's scheme gives further substance to the *Remark* on p. 121 at the end of this paper.

Incidentally, the formal work in (i) is sometimes useful for (ii), for example, to check bounds for (the least ordinal satisfying) D_c.