Suppose now that $\psi(\alpha)$ is not a theorem of $\overline{\mathfrak{S}}_\lambda$. Let H be the Heyting algebra of all open elements of $\bar{L}_\lambda$, $H=\boldsymbol{H}(\bar{L}_\lambda)$. Then by the same argumentation as above

$$(H)\Phi_\alpha(\{\mathbf{I}|a_i|\})=(\bar{L}_\lambda)\Phi_{\psi(\alpha)}(\{|a_i|\})=|\alpha|\neq e,$$

which proves that α is not a theorem of $\overline{\mathfrak{S}}_\chi$ (see 2.2).

References

[1] J. Łukasiewicz, *Elementy logiki matematycznej*, Warszawa 1929.

[2] — und A. Tarski, *Untersuchungen über den Aussagenkalkül*, Comptes Rendus de la Société des Sciences et des Lettres de Varsovie, Classe III, 23 (1930).

[3] J. C. C. McKinsey and A. Tarski, *On closed elements in closure algebras*, Annals of Math. 47 (1946), p. 130.

[4] — *Some theorems about the sentential calculi of Lewis and Heyting*, Journal of Symbolic Logic 13 (1948), p. 1-15.

[5] H. Rasiowa and R. Sikorski, *A proof of the completeness theorem of Gödel*, Fundamenta Mathematicae 37 (1950), p. 193-200.

[6] — *Algebraic treatment of the notion of satisfiability*, Fundamenta Mathematicae 40 (1953), p. 62-95.

[7] — *On existential theorems in non-classical functional calculi*, Fundamenta Mathematicae 41 (1954), p. 21-28.

INSTYTUT MATEMATYCZNY POLSKIEJ AKADEMII NAUK
MATHEMATICAL INSTITUTE OF THE POLISH ACADEMY OF SCIENCES

Reçu par la Rédaction le 10. 5. 1954

Some applications of formalized consistency proofs

by

G. Kreisel (Reading) and Hao Wang (Philadelphia, Pa.)

Introduction

A well-known result due to Gödel [5] states: If (F) is one of the usual systems of arithmetic (for sufficient conditions on (F) see [9], p. 285) the formula which is ordinarily taken as the arithmetization of the *consistency* of (F) cannot be proved in (F) itself. Thus the consistency proof for Z_μ^1 ([9], p. 293) due to Ackermann [2] uses the principle of ordinal induction up to the first ε-number, which cannot be formalized in Z_μ, and the consistency proof by means of a truth definition ([9], p. 339) uses a predicate which cannot be formalized in Z_μ either. It is now natural to ask whether the "ideas" of these consistency proofs may be formalized in Z_μ: the result of such a step would then be a consistency proof for a subsystem (F) of Z_μ; (F) would be demonstrably weaker than Z_μ since a formula of Z_μ which expresses the consistency of (F) would be provable in Z_μ but not in (F). We shall denote such a formula by $\mathrm{Con}(F)$; it is to be understood that the formula chosen for expressing the consistency of (F) satisfies conditions sufficient to ensure the application of Gödel's second undecidability theorem.

In this way we are led to systems which are obtained from Z_μ by suppressing all those proofs of Z_μ which are too "complex"; several definitions of complexity will be used, the principal ones being the maximum number of bound variables occurring in any formula of the proof, and the number of distinct critical ε-matrices (Grundtypen, [9], p. 93), if the Hilbert ε-symbol is used instead of quantifiers. These measures of complexity are suggested by the two consistency proofs mentioned above. We may note in passing that, for our present purpose, the consistency proof by means of a truth definition is more appropriate because it can be immediately applied to any extension of Z_μ by means of transfinite induction, and other principles of proof which satisfy the rule of infinite induction ([11], p. 124).

Our first application of these results concerns the elimination of the induction scheme of Z_μ by means of a finite set of axioms (which are themselves formulae of Z_μ). It was established in [13] and [16] that there is no finite set of theorems of Z_μ from which all theorems of Z_μ may be deduced by means of the predicate calculus of first order. We now show that there is no finite set of formulae of Z_μ, consistent over the predicate calculus, from which all theorems of Z_μ may be deduced by means of the predicate calculus. This is a foil to the result of [10]: there is a finite set of formulae such that a formula A of Z_μ may be deduced from them if and only if A is a theorem of Z_μ; but these formulae contain (auxiliary) predicate symbols which do not belong to Z_μ. Much of what we do is implicit in [13], but it seems convenient to set out the results anew.

Our second application concerns Gödel's result on the length of proofs, stated in his short note [4]. Using two (different) definitions of length — or, perhaps, better: complexity — of proofs we find: suppose two systems of arithmetic (F), (F') are such that any proof of (F) is also a proof of (F') and $\mathrm{Con}(F)$ is a theorem of (F'); then, for any function Φ, not necessarily computable, there are infinitely many formulae A_n of (F) whose shortest proof in (F) has length l_n, and whose shortest proof in (F') has length $l_{n'}$, and $l_n > \Phi(l_{n'})$. Mostowski's variant of Gödel's result, given in [14], is restricted to computable functions Φ, because of his (different) definition of „length of proof"; we may note that on his definition there are less than n proofs of length $\leqslant n$ while on both our definitions there are infinitely many proofs of length $\leqslant n$.

In the third application we return to the well-worn topic of axiom systems (F) of the predicate calculus with a finite number of axioms. It is known (Skolem-Gödel-Bernays) that if $\mathrm{Con}(F)$ is a theorem of Z_μ then a model for the axioms of (F) may be established in Z_μ: in other words, there are predicates and functions of Z_μ such that the axioms of (F) turn into theorems of Z_μ if these predicates and functions are substituted for the non-logical constants of (F) (cf. Theorem 6 of [6]). We now obtain a converse to it: if a model for (F) can be established in Z_μ then $\mathrm{Con}(F)$ is a theorem of Z_μ. This extends the known result (see [6], Theorem 1) that if (F) has a model in Z_μ then $\mathrm{Con}(Z_\mu) \to \mathrm{Con}(F)$ is a theorem of Z_μ, *i. e.*, given a model of (F) in Z_μ one can establish in Z_μ the consistency of (F) relative to Z_μ. We use our result to show that the version of set theory without an axiom of infinity (S), for which Bernays obtained a finite axiomatization [3], does not have a model in Z_μ. — We permit ourselves the digression of showing that $\mathrm{Con}(Z_\mu) \leftrightarrow \mathrm{Con}(S)$ in Z_μ, thereby answering a question raised by McNaughton ([15], p. 141).

To fix ideas, we base our proofs on the system Z_μ as a typical system of arithmetic. Naturally, most results apply to other systems of arithmetic, too; in particular to extensions of Z_μ. We mention such extensions if and only if we have some non-trivial comment on them.

I. The consistency proofs

Definition. *The system* $Z_\mu^{(n)}$. A proof of Z_μ which contains $\leqslant n$ distinct critical ε-matrices, is a proof of $Z_\mu^{(n)}$.

Observe that no restriction is here imposed on the rank of these ε-matrices; however on inspection of the rules of proof of Z_μ, there is a relation between the highest rank and the number of critical ε-matrices: *e. g.*, if a quantifier-free formula of Z_μ cannot be proved by means of formulae of rank $\leqslant n$, it cannot be proved with $<\lambda(n)$ critical matrices, and $\lambda(n)$ is unbounded. Note further that, for sufficiently large n, $Z_\mu^{(n)}$ satisfies the conditions under which Gödel's second undecidability theorem has been established.

LEMMA A. *For each integer* n, $\mathrm{Con}(Z_\mu^{(n)})$ *can be proved in* Z_μ.

This is, in effect, established in [2]: there, an (informal) consistency proof is given which establishes $\mathrm{Con}(Z_\mu^{(n)})$ by means of ordinal induction up to ω_n $(\omega_1 = \omega, \omega_{n+1} = \omega^{\omega_n})$. By [9], p. 366, for each n, ordinal induction up to ω_{n+1} can be formalized in Z_μ.

(This lemma was mentioned on p. 123 of [11] for a subsystem of Z_μ analogous to $Z_\mu^{(n)}$).

Definition. *The system* $Z^{(n)}$. A proof of Z ([9], p. 49) whose formulae contain $\leqslant n$ bound variables, is a proof of $Z^{(n)}$.

Observe that here no restriction is imposed on the number of distinct ε-matrices.

LEMMA B. *For each integer* n, $\mathrm{Con}(Z^{(n)})$ *can be proved in* Z.

This can be proved by modifying the truth definition of [9], p. 330-338.

It is assumed that "natural" definitions of the following syntactical terms and predicates have been chosen.

$\eta_1^{(m)}(n), \ldots, \eta_m^{(m)}(n)$ as in [9], p. 235.

$\varrho(m, a, n)$ is the number of the formula got from A (with number a) by replacing the variable v_i, $i \leqslant m$, in A by $\eta_i^{(m)}(0^{(n)})$ and v_j, $j > m$, by 0. It is not assumed that all v_i, $i \leqslant m$, occur in A. All the variables we use in the proofs will be v_1, v_2, v_3, etc. Trivially, if A is a closed formula, $\varrho(m, a, n) = \varrho(0, a, 0)$ (v_i are free variables.)

$P(a, b)$ if and only if a is a numerical proof of the formula b (*i. e.*, a proof in the elementary calculus, no variables). We recall that the consistency of numerical arithmetic can be proved in Z.

If a and b are numbers of A and B, then $t(a, b)$ is the number of $A|B$.

$U(a)$ if and only if a is the number of a formula of the form $(x)B(x)$, and then $s[u(a), y]$ is the number of $B(0^{(y)})$.

Similarly, $Q(a)$ if and only if a is the number of a formula of the form $(Ex)B(x)$, and then $s[q(a), y]$ is the number of $B(0^{(y)})$.

For each k, a truth definition $T_k(b)$ can be given by means of a formula of Z, satisfying the following conditions (compare [9], p. 334):

$$T_0[\varrho(m,a,n)] \text{ if and only if } (Ey)P[y,\varrho(m,a,n)]$$

$$\text{or}\quad (Ex)(Ey)\{x<\varrho(m,a,n) \,\&\, y<\varrho(m,a,n) \,\&\, \\ \&\, \varrho(m,a,n)=t(x,y) \,\&\, [T_0(x)|T_0(y)]\};$$

$$T_{k+1}[\varrho(m,a,n)] \text{ if and only if } T_k[\varrho(m,a,n)]$$

$$\text{or}\quad \Big\{U[\varrho(m,a,n)] \,\&\, (y)\,T_k\Big[\varrho\Big(m,s\big(u(a),y\big),n\Big)\Big]\Big\}$$

$$\text{or}\quad \Big\{Q[\varrho(m,a,n)] \,\&\, (Ey)\,T_k\Big[\varrho\Big(m,s\big(q(a),y\big),n\Big)\Big]\Big\}$$

$$\text{or}\quad (Ex)(Ey)\{x<\varrho(m,a,n) \,\&\, y<\varrho(m,a,n) \,\&\, \\ \&\, \varrho(m,a,n)=t(x,y) \,\&\, [T_{k+1}(x)|T_{k+1}(y)]\}.$$

It can be verified in the usual manner that $T_k(b)$ is a normal truth definition in the sense of [7], and hence $\mathrm{Con}(Z^{(k)})$ may be proved in Z. Note that $T_n(b)$ is a truth definition for the system $Z^{(n)}$ only, and not for Z; in particular, n is not a free variable.

Observe that the consistency proof of Lemma B is capable of various extensions: *e. g.*, if $\mathfrak{Z}$ is an extension of Z by some principle of transfinite induction, we get a consistency proof of $\mathfrak{Z}^{(n)}$ in $\mathfrak{Z}$.

II. Systems of arithmetic based on the predicate calculus

$P_{\mathfrak{A}}$ denotes the system consisting of the predicate calculus of first order with the closed formula $\mathfrak{A}$ of Z as its only axiom. $\mathrm{Prov}_{\mathfrak{A}}(n,m)$ is a primitive recursive formula of Z such that for numerals $O^{(n)}$, $O^{(m)}$, $\mathrm{Prov}_{\mathfrak{A}}(O^{(n)}, O^{(m)})$ can be proved in Z if and only if n is the number of a proof in $P_{\mathfrak{A}}$ of the formula with the number m; $e(O^{(n)})$ is the number of the negation of the formula with number n.

We use $\vdash_{\mathfrak{A}} A$, $\vdash_z A$ to mean: A can be proved in $P_{\mathfrak{A}}$, Z.

THEOREM 1. *If $P_{\mathfrak{A}}$ is consistent, there is a theorem of Z which cannot be proved in $P_{\mathfrak{A}}$.*

By means of the Gödel substitution function we obtain a term $\mathfrak{q}$ of Z whose value is the number of the following formula (which we call $\mathfrak{Q}$), namely

$$(x)(Ey)\{\mathrm{Prov}_{\mathfrak{A}}(x,\mathfrak{q})\rightarrow\cdot\, y<x \,\&\, \mathrm{Prov}_{\mathfrak{A}}[y,e(\mathfrak{q})]\}.$$

$\mathfrak{Q}$ denotes $(Ey)\{y<O^{(n)} \,\&\, \mathrm{Prov}_{\mathfrak{A}}[y,e(\mathfrak{q})]\}$, and $\mathfrak{Q}^{(n)}$ denotes the disjunction

$$\mathrm{Prov}_{\mathfrak{A}}[O,e(\mathfrak{q})] \vee \mathrm{Prov}_{\mathfrak{A}}[O',e(\mathfrak{q})] \vee \ldots \vee \mathrm{Prov}_{\mathfrak{A}}[O^{(n-1)},e(\mathfrak{q})].$$

LEMMA 1. *The following argument is easily formalized in Z: if $\mathfrak{Q}$ can be proved in $P_{\mathfrak{A}}$, i. e., $\mathfrak{A}\rightarrow\mathfrak{Q}$ can be proved in the predicate calculus, then, by Herbrand's theorem, there is a proof of $\mathfrak{A}\rightarrow\mathfrak{Q}$ in the predicate calculus, in which no formula contains more quantifiers than the formula $\mathfrak{A}\rightarrow\mathfrak{Q}$ itself, say k. This proof is also a proof in $Z^{(k)}$.*

By lemma B,

$$\vdash_Z[(Ex)\mathrm{Prov}_{\mathfrak{A}}(x,\mathfrak{q})\rightarrow\cdot\, T_k(\mathfrak{a})\rightarrow T_k(\mathfrak{q})].$$

Also

$$\vdash_Z[\neg\mathfrak{Q}\rightarrow(Ex)\mathrm{Prov}_{\mathfrak{A}}(x,\mathfrak{q})].$$

But, since $T_k(a)$ is normal:

$$\vdash_Z[T_k(\mathfrak{a})\leftrightarrow\mathfrak{A}],\quad \vdash_Z[T_k(\mathfrak{q})\leftrightarrow\mathfrak{Q}].$$

Hence

$$\vdash_Z[\neg\mathfrak{Q}\rightarrow\cdot\,\mathfrak{A}\rightarrow\mathfrak{Q}],\quad \textit{i. e.}\quad \vdash_Z(\mathfrak{A}\rightarrow\mathfrak{Q}).$$

LEMMA 2. *Either there is a theorem of Z which cannot be proved in $P_{\mathfrak{A}}$, or there is a numeral $O^{(n)}$ such that $\vdash_{\mathfrak{A}}\mathfrak{Q}^{(n)}$.*

(1) $\vdash_{\mathfrak{A}}(\mathfrak{A}\rightarrow\mathfrak{Q})$, *i. e.* $\vdash_{\mathfrak{A}}\mathfrak{Q}$, is false, and then, by lemma 1, we have a theorem of Z which is not a theorem of $P_{\mathfrak{A}}$, or

(2) $\mathfrak{Q}$ can be proved in $P_{\mathfrak{A}}$ by a proof with number $\mathfrak{n}$, say.

In case (2) $\vdash_Z\mathrm{Prov}_{\mathfrak{A}}(O^{(\mathfrak{n})},\mathfrak{q})$, and thus:

either

(2.1) $\vdash_{\mathfrak{A}}\mathrm{Prov}(O^{(\mathfrak{n})},\mathfrak{q})$ is false though $\vdash_Z\mathrm{Prov}_{\mathfrak{A}}(O^{(\mathfrak{n})},\mathfrak{q})$,

or

(2.2) $\vdash_{\mathfrak{A}}\mathrm{Prov}_{\mathfrak{A}}(O^{(\mathfrak{n})},\mathfrak{q})$ and, since $\vdash_{\mathfrak{A}}\mathfrak{Q}$, also $\vdash_{\mathfrak{A}}\mathfrak{Q}_{\mathfrak{n}}$.

In case (2.2), since $\vdash_Z[\mathfrak{Q}_n\rightarrow\mathfrak{Q}^{(n)}]$,

either

(2.21) $\vdash_{\mathfrak{A}}(\mathfrak{Q}_{\mathfrak{n}}\rightarrow\mathfrak{Q}^{(\mathfrak{n})})$ is false though $\vdash_Z(\mathfrak{Q}_{\mathfrak{n}}\rightarrow\mathfrak{Q}^{(\mathfrak{n})})$

or

(2.22) $\vdash_{\mathfrak{A}}\mathfrak{Q}^{(\mathfrak{n})}$.

Since in each case whose number contains a digit 1, we have a theorem of Z which cannot be proved in $P_{\mathfrak{A}}$, the lemma follows.

LEMMA 3. *If $\vdash_{\mathfrak{A}}\mathfrak{Q}^{(n)}$ then either $P_{\mathfrak{A}}$ is inconsistent or there is a theorem of Z which cannot be proved in $P_{\mathfrak{A}}$.*

Since $\mathfrak{Q}^{(n)}$ is a numerical formula, either $\vdash_Z\mathfrak{Q}^{(n)}$ or $\vdash_Z\neg\mathfrak{Q}^{(n)}$. In the former case, $\vdash_{\mathfrak{A}}(\neg\mathfrak{Q})$, and either $\vdash_{\mathfrak{A}}\mathfrak{Q}$ (when $P_{\mathfrak{A}}$ is inconsistent) or $\mathfrak{A}\rightarrow\mathfrak{Q}$ is not a theorem of $P_{\mathfrak{A}}$, though, by lemma 1, it is a theorem of Z. In the latter case, either $\neg\mathfrak{Q}^{(n)}$ cannot be proved in $P_{\mathfrak{A}}$ though $\vdash_Z\neg\mathfrak{Q}^{(n)}$, or both $\vdash_{\mathfrak{A}}\mathfrak{Q}^{(n)}$ and $\vdash_{\mathfrak{A}}\neg\mathfrak{Q}^{(n)}$ when $P_{\mathfrak{A}}$ is inconsistent.

The theorem follows from the last two lemmata.

Remark 1. A shorter but less informative proof of Theorem 1 is the following. Let k be the number of quantifiers of (a prenex normal form of) Con$(P_{\mathfrak{A}})$. If $\neg$Con$(P_{\mathfrak{A}})$, there is a proof in the predicate calculus of $\neg\mathfrak{A}$. By Herbrand's theorem, which can be established in Z, if $\neg\mathfrak{A}$ can be proved in the predicate calculus, it can be proved by a proof each formula of which contains $\leqslant k$ quantifiers. Thus $\neg\mathfrak{A}$ can be proved in $Z^{(k)}$. Hence, by the normal truth definition of $Z^{(k)}$, $\vdash_Z \neg \text{Con}(P_{\mathfrak{A}}) \to \neg\mathfrak{A}$. Therefore, the following formula is a theorem of Z:

(i) $$\mathfrak{A} \to \text{Con}(P_{\mathfrak{A}}).$$

Now, if $P_{\mathfrak{A}}$ contained all theorems of Z, *i. e.*, if $P_{\mathfrak{A}}$ were an extension of Z, the deducibility conditions of [9], p. 286 which ensure the application of Gödel's second undecidability theorem, would apply to $P_{\mathfrak{A}}$ (since we are using the "natural" proof predicate for $P_{\mathfrak{A}}$); further, the formula (i) and hence Con$(P_{\mathfrak{A}})$ would be theorems of $P_{\mathfrak{A}}$, and hence $P_{\mathfrak{A}}$ would be inconsistent.

(By analysing the proofs in Z of the formulae 1, 2, 3 on *p.* 285, 286 of [9], one could exhibit, as in our proof of Theorem 1, for any given consistent $P_{\mathfrak{A}}$ a theorem of Z which cannot be proved in $P_{\mathfrak{A}}$.)

Remark 2. A proof of Theorem 1 can also be obtained by using Skolem's models for arithmetic as in [16]. Thus, given $\mathfrak{A}$ and $P_{\mathfrak{A}}$, either some theorems of Z are not derivable in $P_{\mathfrak{A}}$, then nothing is left to prove. Or all theorems of Z are provable in $P_{\mathfrak{A}}$. Then we can carry out for $P_{\mathfrak{A}}$ Ryll-Nardzewski's construction in [16] and get a case of the induction schema which is derivable in Z but not derivable in $P_{\mathfrak{A}}$ if $P_{\mathfrak{A}}$ is consistent. Hence, if all theorems of Z are provable in $P_{\mathfrak{A}}$, $P_{\mathfrak{A}}$ must be inconsistent. The proof of Theorem 1 is complete.

Remark 3. The theorem shows once again — if such a lesson were needed — the inadequacy of the "intuitive" (uncritical) approach to truth definitions: $\mathfrak{A}$ may well be an "intuitively false" formula, and, therefore, "intuitively", any formula should be provable from $\mathfrak{A}$ via a truth definition, yet not even all theorems of Z can be proved from $\mathfrak{A}$ (by means of the predicate calculus). (We find it difficult to work up a paradox since the flaw is too obvious.)

III. Length of proof

The obvious idea underlying the present section is this: suppose a definition of *length of proof* of a system (F) is given such that, for each n, Con$(F^{(n)})$ can be proved in (F) where $(F^{(n)})$ is the system obtained from F by retaining only those proofs of (F) whose length does not exceed n; suppose further that Gödel's second undecidability theorem applies to $(F^{(n)})$; then the length of the proof of Con$(F^{(n)})$ in (F) exceeds n. If (F') is a system in which Con(F) itself can be proved, and if Con$(F^{(n)})$ can be proved from Con(F) by proofs of bounded length (for all n) we have the following result:

Given any function Φ, there are infinitely many formulae A_n of (F) which can be proved in (F) with shortest proof of length $l(n)$, and can be proved in (F') by a proof of length $l'(n)$ and $l(n) > \Phi[l'(n)]$.

To see this, let a proof of Con(F) in (F') have length c; the proofs of Con$(F) \to$ Con$(F^{(n)})$ have length $\leqslant d$; then we may take for A_n the formula Con$(F^{(n+n_0)})$ where $n_0 \geqslant \max[\Phi(i)]$, $i \leqslant c+d$.

Note that the introduction of Φ here is unnatural; it is done only to permit easier comparison with the results of [4] and [14] where such a function Φ is used. In fact the natural formulation is this: the shortest proofs of A_n in (F') are of bounded length, while the length of the shortest proof of A_n in (F) exceeds n.

We shall now show that the definitions of length given in the first section apply here.

THEOREM 2. *Suppose the length of a proof of Z_μ is measured by the number of distinct ε-matrices which it contains, and suppose (F') is an extension of Z_μ in which* Con(Z_μ) *can be proved. Then, for each n,* Con$(Z_\mu^{(n)})$ *can be proved in (F') by proofs of bounded length, but its shortest proof in Z_μ is longer than n.*

For, Con(Z_μ) means that there is no proof of Z_μ, which leads to $0=1$, and Con$(Z_\mu^{(n)})$ means that there is no such proof of length $\leqslant n$. Hence, Con$(Z_\mu) \to$ Con$(Z_\mu^{(n)})$ is proved in Z_μ by the use of a single critical ε-matrix. Since (F') is an extension of Z_μ, the length of the shortest proof in (F') of Con$(Z_\mu^{(n)})$ does not exceed the length of the shortest proof of Con(Z_μ) by more than 1. Hence the shortest proofs in (F') of Con$(Z_\mu^{(n)})$ are of bounded length. By lemma A, Con$(Z_\mu^{(n)})$ can be proved in Z_μ, but only by proofs of length exceeding n.

THEOREM 3. *Suppose the length of a proof of Z is measured by the maximum number of bound variables that occur in any one of its formulae, and suppose (F') is an extension of Z in which* Con(Z) *can be proved. Then for each n,* Con$(Z^{(n)})$ *can be proved in (F') by proofs of bounded length, but its shortest proof in Z is longer than n.*

Proof as of Theorem 2, by using lemma B in place of lemma A.

Remark 1. We observe in passing that there is a crucial difference between our definitions of "length of proof" and the one used in Mostowski's book [14], where the *number* of a proof in a Gödel-numbering of proofs is taken as its length. On this definition there are only a finite number of proofs of length $\leqslant n$, and, for each n, their consistency is expressed by a numerical formula (without variables), while both $Z_\mu^{(n)}$ and $Z^{(n)}$ contain infinitely many proofs (for each n). It may be observed that, if Mostowski's definition is used, Φ may not be arbitrary, *e. g.* not

$\Phi(n)=0$ if the formula proved in (F') by the proof with number n cannot be proved in (F).

$\Phi(n)$ = length of its shortest proof in (F) if the formula which is proved in (F') by the proof with number n can be proved in (F).

Obviously, we were led to the systems $Z_\mu^{(n)}$, $Z^{(n)}$ since it so happens that their consistency is easily proved in Z. We do not wish to suggest that the definitions of length of proof which are used in the present section, are particularly natural. Perhaps a more natural one measures the length by the *number of lines* used in a proof: this is covered by Theorem 2 since a proof with n lines has $\leqslant n$ critical matrices.

Remark 2. If $L(n)$ is the length of the proof with number n, as measured by the number of distinct ε-matrices, and the proof of $\mathrm{Con}(Z_\mu)$ in (F') is of length n_0, then we can also prove Theorem 2 if we replace the formulae $\mathrm{Con}(Z_\mu^{(n)})$ by the formulae

$$(n)[L(n)\leqslant\Phi(n_0)+i\rightarrow\neg\mathrm{Prov}_Z(n,\mathfrak{q}_i)],$$

which have the Gödel numbers $\mathfrak{q}_i$ $(i=1,2,\ldots)$.

An alternative proof of Theorem 3 can be obtained similarly.

IV. Finite axiom systems of the predicate calculus

THEOREM 4. *If a finite axiom system F has a model in Z then* $\mathrm{Con}(F)$ *can be proved in Z.*

Let the model of F be the theorem F^* of Z which, by definition of a "model", is obtained by substituting non-logical constants of Z for the non-logical constants of F.

If $\neg\mathrm{Con}(F)$ there would be a proof of $\neg F$ in the predicate calculus, hence a proof of $\neg F^*$ in $Z^{(\mathfrak{m})}$ where $\mathfrak{m}$ is the number of quantifiers of F. Hence, we have in Z,

$$\neg\mathrm{Con}(F)\rightarrow\neg T_{\mathfrak{m}}(f^*)$$

(where f^* is the number of F^*).

Since $T_{\mathfrak{m}}(a)$ is a normal truth definition,

$$\neg T_{\mathfrak{m}}(f^*)\rightarrow\neg F^*.$$

Thus, in Z,

$$F^*\rightarrow\mathrm{Con}(F).$$

Remark to Theorem 4. It is clear that instead of Z we could have used the extensions of arithmetic mentioned after lemma B since

the whole proof merely depends on the use of a normal truth definition. However, it is not clear that the result applies if instead of Z we use a system of analysis, *e. g.* H of Supplement IV to [9].

Application of Theorem 4. There can be no model in Z_μ for the system (S) of [12], based on Bernays' construction of a set theory with a finite number of axioms. (This result is in sharp contrast to the primitive recursive model in [1] of general set theory with an axiom schema, where, it can be shown, each axiom has a model in Z_μ.) First, $\mathrm{Con}(S)\rightarrow\mathrm{Con}(Z_\mu)$ can be proved in Z_μ simply by following out the usual development of arithmetic in set theory. Next, if we had a model of $(S$ in Z_μ we should have a proof of $\mathrm{Con}(S)$ in Z_μ, by Theorem 4, and hence a proof of $\mathrm{Con}(Z_\mu)$, which is excluded by [9]. Thus we have decided a question raised in [8], p. 400.

Digression. By following out the steps of [12], § 11, we obtain a proof of $\mathrm{Con}(Z_\mu)\rightarrow\mathrm{Con}(S)$ in Z_μ so that $\mathrm{Con}(Z_\mu)\leftrightarrow\mathrm{Con}(S)$ in Z_μ.

THEOREM 5. $\vdash_{Z_\mu}\mathrm{Con}(Z_\mu)\rightarrow\mathrm{Con}(S)$.

By slightly reformulating (S), we can eliminate all exitential quantifiers from axioms of (S) (see [12], p. 48). Let $\mathfrak{A}$ or $B(x_1,\ldots,x_m)$ be the conjunction of the axioms of (S). If $\neg\mathrm{Con}(S)$, then the negation of $\mathfrak{A}$, which is equivalent to a formula

$$(Ex_1)\ldots(Ex_m)\neg B(x_1,\ldots,x_m),$$

is provable in the predicate calculus. By the extended first ε-theorem ([9], p. 32), we can also prove in the predicate calculus, for some constant n_0, a disjunction of the formulae:

$$\neg B(t_1^{(i)},\ldots,t_m^{(i)}),\qquad 1\leqslant i\leqslant n_0.$$

But, by [12], the formulae $B(t_1^{(i)},\ldots,t_m^{(i)})$ all have provable models in Z_μ. Hence, we may derive $\neg\mathrm{Con}(Z_\mu)$ from $\neg\mathrm{Con}(S)$ in Z_μ.

Application of Theorem 5. Let ZF and NB be respectively the set theories of Zermelo-Fraenkel and von Neumann-Bernays (see, *e. g.*, [7], p. 271). It is known that if $\mathrm{Con}(ZF)$ is added to Z_μ, there is a model of ZF in Z_μ. Combining these models of axioms of ZF with models of additional axioms of NB which are similar to those of axioms of (S), we may prove in Z_μ, similarly as with Z_μ and (S), the theorem: $\mathrm{Con}(ZF)\rightarrow\mathrm{Con}(NB)$.

References

[1] W. Ackermann, *Die Widerspruchsfreiheit der allgemeinen Mengenlehre*, Mathematische Annalen 114 (1937), p. 305-315.

[2] — *Zur Widerspruchsfreiheit der reinen Zahlentheorie*, Mathematische Annalen 117 (1940), p. 161-194.

[3] P. Bernays, *A system of axiomatic set theory*, part II, Journal of Symbolic Logic 6 (1941), p. 1-17.

[4] K. Gödel, *Über die Länge der Beweise*, Ergebnisse eines mathematischen Kolloquiums 7 (1931), p. 23-24.

[5] — *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*. Monatshefte für Mathematik und Physik 38 (1931), p. 173-198.

[6] Hao Wang, *Arithmetic translations of axiom systems*, Transactions of the American Mathematical Society 71 (1951), p. 283-293.

[7] — *Truth definitions and consistency proofs*, Transactions of the American Mathematical Society 73 (1952), p. 243-275.

[8] — *Between number theory and set theory*, Mathematische Annalen 126 (1953), p. 385-409.

[9] D. Hilbert und P. Bernays, *Grundlagen der Mathematik*, vol. II, Berlin 1939.

[10] S. C. Kleene, *Finite axiomatizability of theories in the predicate calculus using additional predicate symbols. Two papers on the predicate calculus*, Memoirs of the American Mathematical Society 10 (1952), p. 27-68.

[11] G. Kreisel, *A variant to Hilbert's theory of the foundations of arithmetic*, The British Journal for the Philosophy of Science IV, 14 (1953), p. 107-129.

[12] — *Note on arithmetic models for consistent formulae of the predicate calculus, II*, Proceedings of the XIth International Congress of Philosophy XIV (1953), p. 39-49.

[13] A. Mostowski, *On models of axiomatic systems*, Fundamenta Mathematicae 39 (1952), p. 133-158.

[14] — *Sentences undecidable in formalized arithmetic — An exposition of the theory of Kurt Gödel*, Amsterdam 1952.

[15] R. McNaughton, *Some formal relative consistency proofs*, Journal of Symbolic Logic 18 (1953), p. 136-144.

[16] C. Ryll-Nardzewski, *The role of the axiom of induction in elementary arithmetic*, Fundamenta Mathematicae 39 (1952), p. 239-263.

Reçu par la Rédaction le 19. 5. 1954

On manifolds and r-spaces *

by

A. Kosiński (Warszawa)

We shall say that a point p belonging to a space K is an *r-point* of K if each neighbourhood of p contains a neighbourhood U of p such that, for each $q \epsilon U$, $\mathrm{Fr}(U)$ is a deformation retract of $U-(q)$. (See [4]; $\mathrm{Fr}(U)$ denotes the boundary of U, *i. e.* the set $\overline{U}\cdot(\overline{K-U})$.) The neighbourhood with the property just mentioned will be called a *canonical neighbourhood*. (It is worth noting that a canonical neighbourhood U of a point p is also a canonical neighbourhood for each point $q \epsilon U$).

The space K is said to be an *r-space* if it is compact, metric, separable, finite dimensional, and if each point of K is its r-point.

It turns out that r-spaces have a very similar structure to that of topological manifolds. In particular, many of the classical theorems about the manifolds (such as for instance theorems on the invariance of domain, internal characterization of separating sets and so on) hold also in r-spaces. Moreover, among the spaces of dimension $\leqslant 2$ and among the polytopes of dimension $\leqslant 3$ connected r-spaces are identical with the manifolds. The notion of r-space gives therefore a new topological characterization of 2-manifolds. The basic problem whether there exists an r-space not homeomorphic to a manifold remains open.

This paper should be considered as a continuation of the researches of K. Borsuk on the "spheroidal spaces" ([5], [3]). In particular, the proofs of some lemmas in § 1 are suitably adapted proofs of the corresponding lemmas in [5] and [3]. These proofs are based on some auxiliary lemmas, which are modified lemmas from the papers mentioned. For the convenience of the reader all these auxiliary lemmas are gathered in the supplement at the end of the paper. (S. I, S. II etc. denote the lemmas from the supplement).

Terminology and notation. All set-theoretical topological notions used here are defined in [9]. Manifolds, pseudomanifolds, polytopes are meant in the sense defined in [2]. The homology theory here used

* Presented to the Polish Mathematical Society (Warsaw Section) at the meeting of March 12, 1954.