Effectiveness and Provability

by

Wilfried Sieg

July 1992

Report CMU-PHIL-31

Philosophy
Methodology
Logic

Pittsburgh, Pennsylvania 15213-3890

Effectiveness and Provability

to appear in: *Rendiconti di Seminario Matematico e Fisico di Milano*

Wilfried Sieg
Carnegie Mellon University
Pittsburgh, PA 15213, USA

The focus of this brief report is a facet of current logical investigations that exhibits the subtle irony of much foundational work: On the one hand it is directly tied to philosophical concerns in mathematics, and on the other hand it is directly relevant to practical, yet fundamental issues in other sciences. The notions of "effectiveness" and "provability" were considered as being properly understood in the late 19th century. In the meantime, they have received precise mathematical definitions — but only when attention is restricted in specific ways: As to effectiveness, we must focus on "mechanical procedures"; as to provability, we must focus on "formal theories". Gödel pointed to the connection between the broad *informal* notions when he asked, whether there are effective but non-mechanical procedures that can systematically provide us with new mathematical principles. Gödel was thinking very speculatively of a procedure that yields stronger and stronger axioms of infinity and thus extends larger and larger segments of the cumulative hierarchy of sets. But I want to turn attention to the concrete, painstaking work that has been done to clarify and to relate the notions of "effectiveness" and "provability" -- effectiveness understood in a mechanical sense, and provability restricted to second order arithmetic for the development of classical analysis.

1. From Kronecker to Hilbert (and back). The foundational concerns of mathematicians I alluded to appear most clearly during the second half of the 19th century in the opposing views on the "arithmetization of analysis" entertained by Leopold Kronecker and Richard Dedekind. The opposing views were expressed openly, but with rhetorical restraint, in Kronecker's paper "Über den Zahlbegriff" and in Dedekind's almost contemporaneous essay *Was sind und was sollen die Zahlen.* At issue were methodological restrictions on mathematical arguments and concepts. As to concepts, Kronecker insisted that mathematical notions must be *decidable* in finitely many steps; as to arguments, he considered proofs of existential statements to be complete only when they exhibit objects satisfying the claim expressed by the statement. The almost immediate

consequence of this restrictive methodology for analysis was Kronecker's rejection of the general concept of irrational number. Dedekind had given a precise extension to this concept in his earlier essay *Stetigkeit und irrationale Zahlen.* Indeed, he had given an axiomatic characterization of real numbers (as elements of a complete ordered field), had provided what we would call a set-theoretical model for the axiom system, and had established the system's categoricity.

The set-theoretic methods used so freely by Dedekind in both of his foundational essays turned out to be in need of restrictions. It was clear to Georg Cantor that the unrestrained principles employed by Dedekind in his second booklet led to contradictions. Hilbert was informed about these difficulties by Cantor as early as 1897, and he tried to secure the "classical" basis for analysis in his paper "Über den Zahlbegriff". The title, without any doubt, was chosen to allude polemically to Kronecker's earlier paper; Hilbert intended to *prove the existence* of the set of real numbers and thus to refute Kronecker — by establishing in a sort of model theoretic way the consistency of (essentially) Dedekind's axiomatization for the real numbers. I formulate matters vaguely, since Hilbert's proposal is quite tentative and vague.

The more elementary contradictions in set theory found in 1901/1902 by Russell and Zermelo made Hilbert rethink matters. Taking into account the formalizability of mathematical proofs (discovered by Frege and Peano) and the radicalization of the axiomatic method (exhibited so masterfully in his own "Grundlagen der Geometrie"), Hilbert looked in a completely new way at the consistency problem. In his address to the Second International Congress of Mathematicians in Heidelberg (1904) he proposed first to formalize logic and mathematics simultaneously and then to prove that none of the finite syntactic configurations constituting proofs has a contradiction as its conclusion! Note that this novel understanding of consistency as a *syntactic* property allowed him to

adopt a Kroneckerian point of view with respect to "meta-mathematics". Bernays described the change of perspective in this way:

> Under the influence of the discovery of the antinomies in set theory, Hilbert temporarily thought that Kronecker had probably been right there [i.e., right in insisting on restricted methods]. But soon he changed his mind. Now it became his goal, one might say, to do battle with Kronecker with his own weapons of finiteness by means of a modified conception of mathematics.

The 1904 proposal, ambitious in goals, but still vague in details, was elaborated slowly during the next decade and was pursued vigorously in the twenties with the aid of Bernays, Ackermann, von Neumann, and Herbrand. The *finitist* standpoint Hilbert took at that time was seen by Hilbert himself as essentially coinciding with Kronecker's position and, incidentally, also with Brouwer's. It remained the goal of *Hilbert's Program* to establish the consistency of classical theories $\mathbf{T}$ like Zermelo-Fränkel set theory or the system of *Principia Mathematica*. However, such a proof was no longer seen as guaranteeing the existence of a model, but rather as ensuring the instrumental usefulness of $\mathbf{T}$. After all, one can finitistically prove the equivalence of the consistency statement and the reflection principle for statements in the language of finitist mathematics $\mathbf{F}$: $\mathbf{F}$ proves $\mathrm{cons}_{\mathbf{T}}$ iff $\mathbf{F}$ proves $\mathrm{Pr}_{\mathbf{T}}(a,'\psi') \rightarrow \psi$, for any ψ in the language of $\mathbf{F}$. (Here $\mathrm{cons}_{\mathbf{T}}$ expresses the consistency of $\mathbf{T}$, and $\mathrm{Pr}_{\mathbf{T}}(a,'\psi')$ says that a is a $\mathbf{T}$-proof of the $\mathbf{T}$-formula that expresses ψ.)

Hilbert hoped that the strict formalization of mathematics would allow an algorithmic treatment of many other problems. One problem whose consideration he urged most strongly was the *Entscheidungsproblem* or decision problem for predicate logic. Its classical formulation is found in his 1928 book with Ackermann, called *Grundzüge der Logik*.

> The Entscheidungsproblem is solved, if one knows a procedure that permits the decision concerning the validity, respectively satisfiability of a given logical expression by a finite number of operations.

The decision problem was viewed as a problem of *fundamental importance* and was pursued by some, e.g., Herbrand, because its solution would also provide a solution to the consistency problem.[1]

2. Mechanical Effectiveness. As is well-known, Gödel's First Incompleteness Theorem refuted Hilbert's fundamental assumption of complete formalizability; the Second Incompleteness Theorem refuted the consistency program when allowing only finitist means. After all, the latter were supposed to be elementary mathematical means and as such should be captured by sufficiently strong theories, certainly by theories like ZF or PM. Yet such theories cannot be shown to be consistent, according to the second of Gödel's results, by arguments that are formalizable within these very theories. Gödel's paper appeared in 1931; only a few years later the unsolvability of the decision problem was established by Church and Turing.

These sweeping general claims rest on, what is usually called, *Church's Thesis*; the thesis says that the informal notion of effectiveness or calculability is captured by a precise mathematical concept, e.g., recursiveness or, equivalently, by λ-definability and Turing-computability. Only such a mathematical notion allowed the general characterization of "formal" theories and the proof of the Incompleteness Theorems for *all* formal theories satisfying some minimal representability and derivability conditions. Similarly, only with respect to a well-determined class of procedures could a negative solution of the decision problem be obtained.

Remark. The thesis of Church is fundamental also in cognitive science and artificial intelligence; one should, however, be very conscious of the fact that only mechanical procedures were analyzed, not arbitrary mental procedures. The most convincing analysis of the informal notion was given by Turing and ultimately rests on the claim that human memory is necessarily limited; see my paper "Mechanical procedures and mathematical experience".

---

[1] The possibility of finitely axiomatizing theories in predicate logic was taken for granted.

The search for a precise and adequate concept of effective calculability was sparked by Gödel's discoveries. In April 1931, Herbrand suggested in a letter to Gödel the class of primitive recursive functions be extended and that "recursive functions" be defined as solutions of simple functional equations. In contrast to Gödel, who built in his 1934 Princeton Lectures on Herbrand's suggestion, and who gave the modern definition of general recursive functions, Herbrand insisted that the termination of computing function values (in finitely many steps) should be finitistically provable. If the informal concept of finitist provability is replaced here by provability in a formal theory T, then we can establish direct connections between the class of functions whose termination (or totality) can be proved in T and a possibly natural class K of recursive functions. The first significant result along these lines was established by Kreisel in 1951: The provably total functions of Peano arithmetic are exactly the <eo-recursive functions.

Such results have been refined recently to establish proof theoretic characterizations of important complexity classes, e.g., Buss's characterization of the polynomial-time computable functions. The hope here is that relations between the formal theories might reveal relations between their associated function classes. The fact that a theory T has a particular class of provably total functions can actually be used to prove independence results for Π^0_1-statements, i.e., for statements of the form (Vx)(3y)Rxy with quantifier-free R. If one knows that any Skolem-function for such a statement must grow faster than all elements in a class C of recursive functions, then the statement cannot be proved in a theory T whose class of provably total functions coincides with C. This methodology has been used for a number of theories and a variety of combinatorial theorems; Simpson (1987) gives a very nice exposition of such results.

3. Formal Provability. But how is it possible to extract from formal derivations information concerning provably total functions,

that is, the class of Skolem-functions for Π^0_2-theorems? The fundamental tools are versions of Herbrand's Theorem, which states in its simplest form for Σ^0_1-statements: If $(\exists x)\psi x$ is provable (in logic) and ψ is quantifier-free, then there is a sequence of terms t_0, ... ,t_n and a proof of $\psi t_0 \vee \ldots \vee \psi t_n$. This theorem and its extensions are only starting-points for the detailed mathematical refinement of proofs concerned with obtaining *good* bounds for particular theorems; Luckhardt's work concerning Roth's Theorem on rational approximations of algebraic-irrational numbers exemplifies this kind of mathematical work.

But I want to pursue here the aim of characterizing the provably total functions of a theory and not the aim of determining good bounds for particular theorems. The use of *sequent calculi* to describe formal provability is technically most convenient for this purpose. The language underlying the logical calculi is that of second-order logic with variables and parameters for individuals (numbers) and for unary functions (from numbers to numbers); after all, we want to develop analysis. Sequent calculi were introduced by Gentzen and are given here in a form due to Tait: One proves finite sets of formulas $\Gamma, \Delta, \ldots$; formulas are built up from (negated) atomic formulas by $\wedge$, $\vee$, $\exists$, $\forall$; negations (of complex formulas), conditionals, and biconditionals are considered to be defined. We have logical axioms (LA), simple rules for the introduction of logically complex formulas, and the so-called cut-rule (C) that generalizes the rule of modus ponens. The rules of the calculi are (among) the following ones, where Γ,ϕ stands for the union of Γ and singleton ϕ:

LA: $\quad \Gamma, \varphi, \neg\varphi\,, \qquad \varphi$ atomic

$\wedge$: $\quad \dfrac{\Gamma,\varphi_0 \qquad \Gamma,\varphi_1}{\Gamma,\varphi_0\wedge\varphi_1}$

$\vee_i$: $\quad \dfrac{\Gamma,\varphi_i}{\Gamma,\varphi_0\vee\varphi_1}\,, \qquad i = 0,1$

$$\underline{C}: \quad \frac{\Gamma,\varphi \qquad \Gamma,\neg\varphi}{\Gamma}$$

The rules for number quantifiers are:

$$\underline{\forall}: \quad \frac{\Gamma,\varphi a}{\Gamma,(\forall x)\varphi x} \qquad a \notin P(\Gamma)$$

$$\underline{\exists}: \quad \frac{\Gamma,\varphi t}{\Gamma,(\exists x)\varphi x}$$

(The expression $a \in P(\Gamma)$ means that the parameter a occurs in one of the formulas in Γ.) The rules for function quantifiers are analogous. Derivations are built up in tree form; let me use D,E,... as syntactic variables ranging over derivations. *Gentzen's Hauptsatz*, the fundamental fact concerning these calculi, states: Every derivation of a sequent Γ can be transformed into a cut-free (or normal) derivation of Γ. By inspecting the rules one can see immediately that all formulas occurring in a normal derivation of Γ are *subformulas* of elements of Γ. Thus, whenever Γ is provable at all, it is provable by means of a derivation that contains only formulas whose complexity is bounded by the complexity of the formulas occurring in the endsequent.

These proof theoretic considerations can be extended to theories with purely universal axioms and additional rules, e.g., for identity and induction. Identity can be axiomatized by the rules:

$$\frac{\Gamma,\varphi t}{s \neq t, \Gamma, \varphi s} \qquad \frac{\Gamma,\varphi t}{t \neq s, \Gamma, \varphi s}$$

and the axiom $\Gamma, a=a$. The induction principle can be formulated as a rule for formulas in a class Θ, and this Θ-IA is given in the form:

$$\frac{\Gamma,\varphi 0 \qquad \Gamma,\neg\varphi a, \varphi a'}{\Gamma, \varphi t}$$

Here the parameter a is not in P(ru{cpt}); t is any term; qpa is in 6; and 0 is a class of formulas like QF, A_o, zj, ifi. In this broadened context one has to give up complete cut-elimination in favor of cut-reduction; that is, cuts are allowed, but the cut-formulas must be in a given class 0 of formulas. Such derivations are called *&-normal.*

0-normalization. Let T be a theory (of arithmetic) all of whose axioms are in 0 and whose induction principle is 0-IA; if there is a T-derivation of r, then there is a 0-normal T-derivation of r.

Assume now that the theory[2] provably satisfies some basic closure conditions, namely, closure under explicit definition, definition by cases, and bounded search; then one can establish the following lemma:

i-inversion. Let T be an Herbrand theory, let r contain only purely existential formulas, and let y be quantifier-free; if D is a T-derivation of r,(3x)\j/x, then there is a term t* and a (QF-normal) T-derivation D* ofr,yt*.

For the basic theory (BT), consisting of universal axioms for zero, successor, the defining equations for all primitive recursive function(al)s, QF-comprehension (^-abstraction), and QF-induction, one can use the 3-inversion lemma to prove:

Theorem. The provably total functions of (BT) are exactly the primitive recursive functions.

This is not surprising, since (BT) is a rather simple conservative extension of primitive recursive arithmetic. What *is* surprising is that (BT)f's extension (F), obtained from (BT) by adding the induction principle for Z?-formulas, the axiom of choice for the same class of formulas, and K6nigf's Lemma WKL for trees of 0-1-sequences has two features: (1) The theory is still conservative over primitive recursive arithmetic and thus has as its provably total functions

2 If induction is restricted to formulas in QF and the axioms are purely universal, I call such a theory an Herbrand theory.

exactly the primitive recursive ones; and (2) **The theory allows the** development of significant parts of analysis. **The** axiom of choice AC_0 is taken in the form:

$$(Vx)(3y)4>xy \text{ -» } 0f)(Vx)<|>xf(x)$$

König's infinity lemma for trees of 0-1-sequences is formulated in our framework by

$$(Vf)[T(f) \text{ A } (Vx)(3y)(lh(y)\text{-}x \text{ A } f(y)\text{-}1) \text{ ->}(3g)(Vx)\ f(\overline{g}(x))=1];$$

where T(f) expresses that f is (the characteristic function **of)** a **tree** of 0-1-sequences; lh is the length-function for sequences of numbers. Note that T(f) is a purely universal formula:

$$(Vx)(Vy)\ [(f(x*y)=1 \text{ -» } f(x)\text{-}1) \text{ A } (f(x*<y>)\text{-}1 \text{ ->}y\leq 1)]$$

The proof of fact (1) is sketched in Section 4; regarding fact (2) I simply mention results that were established by Friedman **and** Simpson. Their work is in a long tradition of developing analysis in second-order arithmetic reaching back to Weyl's *Das Kontinuum* (1918) and to lectures of Hilbert in the early twenties.

Theorem. Over (BT+Z?-IA+S?-ACo) one can establish the equivalence of the following statements:
(i) WKL;
(ii) the Heine-Borel Theorem (Every covering of the unit interval by **a** countable sequence of open intervals has a finite subcovering);
(iii) every continuous function on the unit interval is uniformly continuous;
(iv) every continuous function on the unit interval is bounded [has **a** supremum and attains it];
(v) the Cauchy-Peano Theorem on the existence of solutions **for** ordinary differential equations.

4. Eliminating WKL. As an indication of the metamathematical work involved in the reductive considerations, I will show (following [Sieg 1991]) how the weak version of König's Lemma can

be removed from BT-derivations of sequents A containing only Z?-formulas. In the formulation of the WKL-elimination lemma I call D a *BT-derivation of* A[--WKL], if D is a derivation of A together with negations of (instantiations of) WKL and negations of BT-axioms.

WKL-elimination lemma. If D is a QF-normal BT-derivation of AHWKL], then there is a QF-normal BT-derivation of A.

Proof (by induction on the length of D). I concentrate on the central case when the last rule in D introduces an instance of -iWKL; that is,

T(f) A (Vx)(3y)(lh(y)«x A f(y)-1) A -(3g)(Vx) f($\bar{g}$(x))-1.

(Recall that T(f) is a purely universal statement and expresses that f is the characteristic function of a tree of 0-1-sequences.) There are QF-normal BT-derivations Dj, i≤2 and all shorter than D, of

A [--WKL], T(f)
A [-.WKL], (Vx)(3y)(lh(y)-x A f(y)=1), and
AhWKL],(Vg)(3x)f($\bar{g}$(x))*1.

Using $\underline{V}$.-inversion and the induction-hypothesis we obtain Ej, i≤2, of

A, T(f)
A, (3y) (lh(y)-c A f(y)-1), and
A, (3x) f($\bar{u}$(x))*1

with new parameters c and u. The $\underline{3}$.-inversion lemma provides terms t and s and also QF-normal BT-derivations Fi and F2 of

A, lh(t[c])-c A f(t[c])=1 and A, f($\bar{u}$(s[u]))*1.

The terms s and t may contain further parameters, but u does not occur in t. Now observe: (i) t yields sequences of arbitrary length in the tree f that do not necessarily form a branch; (ii) f($\bar{u}$(s[u]))*1 expresses the well-foundedness of f. In short, we have a binary tree (according to E_o) that contains sequences of arbitrary length and is well-founded. This conflicting situation can be exploited by means of a formalized recursion theoretic observation: s can be majorized

(in the sense of [Howard]) by a numerical term s* that does not contain u, since ucan be taken to be majorized by 1. Let t[s*] be the 0-1-sequence

$$t_0, \ldots, t_{s^*-1}$$

and define with ^-abstraction the function u* by

$$u^*(n) = t_n \quad \text{if } n < s^*$$

and u*(n) equals 0 otherwise. $\overline{u^*}(s^*)$ obviously equals t[s*]; f is provably a tree according to Eo; and s* is a bound for s. Thus, we have from F_2 a derivation G2 of A,f(t[s*])*1. From *F*<\ one can obtain easily a derivation d of A,f(t[s*])=1. A cut of G1 and G_2 yields the sought for derivation E of A. **Q.E.D.**

Clearly, this elimination lemma together with analogous results for the zf-induction principle and the zf-axiom of choice does provide computational information; that is expressed in the following corollary.

Corollary. If **(BT** + zf-IA+zf-ACo+WKL) proves the restatement (Vx)(3y)vxy, then there is a primitive recursive function f and a proof of yaf(a) in (PRA).

Mathematical investigations of the sort I described do stand in a long tradition, but they have focused on weak subsystems of analysis only during the last 15 years; and yet, they have uncovered most surprising results. The systematic connection of weak arithmetic theories with complexity classes was begun to be explored only with Buss (1986); and yet, there is already an impressive body of results and a growing arsenal of techniques. There is also a reasonable expectation that we might obtain real mathematical information from a pursuit of (what I would like to call) "Kronecker's Program" and that we might gain more detailed computational information from the proof theoretic characterization of complexity classes. But what I find most remarkable, from a slightly detached perspective, is this: Broad foundational concerns

have been sharpened and de-ideologized, and they have moved us to invent tools for addressing questions of concrete and genuine interest.

BIBLIOGRAPHY

S. Buss — *Bounded Arithmetic*; Bibliopolis, 1986

R. Dedekind — *Stetigkeit und irrationale Zahlen*; Braunschweig, 1872

Was sind und was sollen die Zahlen; Braunschweig, 1888

K. Gödel — Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, Monatshefte für Mathematik und Physik 38 (1931), 173-198

On undecidable propositions of formal mathematical systems; Lecture Notes, Princeton, 1934, reprinted in: *The Undecidable* (M. Davis, ed.), New York, 1965, 39-71

D. Hilbert — Über den Zahlbegriff; Jahresberichte der Deutschen Mathematiker-Vereinigung 8 (1900), 180-194

W. Howard — Hereditarily majorizable functionals of finite type; in: Lecture Notes in Mathematics 344; Springer-Verlag, 1973, 454-461

G. Kreisel — On the interpretaion of non-finitist proofs I; J. Symbolic Logic 16 (1951), 241-267

L. Kronecker — Über den Zahlbegriff; published in 1887, reprinted in *Werke*, Vol. III, Part 1, Teubner, 1899, 251-274

H. Luckhardt — Herbrand-Analysen zweier Beweise des Satzes von Roth: polynomiale Anzahlschranken; J. Symbolic Logic 54 (1989), 234-263

W. Sieg — Herbrand analyses; Arch. Math. Logic 30 (1991), 409-441

Mechanical procedures and mathematical experience; to appear in: *Mathematics and Mind*, A. George (ed.), Oxford University Press

S.G. Simpson — Unprovable theorems and fast-growing functions; Contemporary Mathematics vol. 65, 1987, 359-394

W.W. Tait — Normal derivability in classical logic; in: *The syntax and semantics of infinitary languages*, J. Barwise (ed.), Lecture Notes in Mathematics 72, 1968, 204-236