Logique & Analyse **213** (2011), 49–68

HILBERT PROGRAMME AND APPLIED PROOF THEORY

YVON GAUTHIER

Abstract
My discussion centers around Ulrich Kohlenbach's *Applied Proof Theory: Proof Interpretations and their Use in Mathematics* [21] which appears as a major work in the "proof mining project" of recent proof theory. The emphasis is on the tradition of proof theory originating with Hilbert and his motivations. I examine also Hilbert's Kroneckerian inspiration and I maintain that Hilbert's programme is the continuation of Kronecker's programme by logical and metamathematical means. I conclude that despite Kreisel's proposal of a shift of emphasis in traditional proof theory, Hilbert's original proof-theoretical ideal is still alive and proof mining is in the purview of Hilbert programme.

1. *Introduction*

One could tentatively distinguish at least five varieties within the field of proof theory. Hilbert's original proof theory (*Beweistheorie*) which he called metamathematics (*Metamathematik*) or the internal (*inhaltliche*) theory of formal systems (proofs) was meant to deal with consistency as a philosophical question and a mathematical problem. Although the consistency of arithmetic was not the sole problem of the Hilbert Programme, I consider it as the main target of the still alive proof-theoretical mathematical goal. G. Kreisel has distinguished between General Proof Theory which treated the general notion of proof(s) and Reductive Proof Theory which was concerned with constructive (modified) reductions of Hilbert's original proof-theoretic programme after Gödel's incompleteness results. In that connection, one could also mention Friedman-Simpson programme of reverse mathematics or Feferman's of predicative mathematics — E. Nelson's predicative arithmetic is radically Hilbertian. Reductive proof theory could be seen as a programme

for unwinding or extracting constructive content from the gangue of non-constructive or classical proofs. D. Scott has coined the term "proof mining" for what was to become "applied proof theory" in the hands of Ulrich Kohlenbach and co-workers. Applied proof theory could also be contrasted with abstract proof theory which deals with extensions of Hilbert's finitary framework into the set-theoretic (transfinite) ordinal hierarchy, although applied proof theory does not repudiate entirely the transfinite realm in the deployment of intuitionistic mathematics. I want to insist in the following on the foundational and philosophical significance of applied proof theory.

Applied proof theory has the explicit aim to extract constructive (and qualitative) data together with effective bounds from non-constructive proofs of theorems, mainly in classical analysis; this aim is achieved by using constructive and at times non-constructive means, especially in fixed point theory, as Kohlenbach admits (see [21]. p. vii, and [22]), and still the procedures stemming from intuitionistic principles like bar-induction and bar-recursion allow for the "binding" of information in classical proofs. The tools in question are logical — to be distinguished from combinatorial or purely arithmetical and polynomial means. Extraction of bounds from existing "unbounded" proofs is performed using logical techniques stemming mainly from Herbrand's theorem and Gödel's functional (*Dialectica*) interpretation. Other notions like Kreisel's no-counterexample interpretation, modified realizability and Howard's majorazibilty could be seen as derived from those two primary sources. One should also mention in that connection, besides the pioneering work of F. Richman and others, the work of T. Coquand, H. Lombardi and others (see [3], [2] and [4]) using the same logical tools in a programme for the extraction of computational content in abstract algebra.

The logical profit is banked on the informational content of the extractive procedure and this is of course more apparent in fully non-constructive classical analysis than it is, for instance, in number theory. In elementary number theory — elementary because it does not use analytical means or methods —, logic is not involved in the unwinding of proofs, since number theory can do it on its own. For example, Euler's theorem on the infinity of primes (after Euclid's constructive proof) obtains with a minorization ($\log\,\log x$) on the divergent series of inverses of primes

$$\sum_{p\leq x} 1/p \geq \log\log x - \log 2 (x \geq 2).$$

Let us note here that Euler introduced analysis in his original proof, but here elementary properties of the logarithmic function are used to arithmetize the analytical statement with limits. A similar example is given by Kohlenbach (see [21] pp. 15–16) and can serve as a motto for the extractive practice:

in order to get the best computable results, define sharply the interval of values. It is not generally known (and not mentioned by Kohlenbach) that Kronecker, the pioneer of constructive mathematics, has insisted on such a procedure. In his criticism of Bolzano's theorem on intermediate values, Kronecker vilifies Bolzano for having used the crudest means (*den rohesten Mitteln*) to obtain an analytical result which cannot be applied to the roots of an entire function. In his refinement of Sturm's theorem on the change of signs in the real roots of an algebraic equation, Kronecker calls for the localization (*Isolierung*) of real roots in an algebraic equation with the help of multiple equations and inequations (see [11]). The idea of localization of roots could also be found in Selberg's elementary proof of Dirichlet's analytical proof on the distribution of primes in arithmetic progressions, where Selberg uses only elementary properties of the logarithmic function. In that context, Kohlenbach recalls some recent results by Avigad, Gerhardy and Towsner using logical analysis on the classical ergodic theorem in connection with the Green-Tao theorem on the existence of arbitrary long progressions in the distribution of primes. A more recent result by Kohlenbach (and Leustean) applies the functional interpretation to obtain more quantitative information on the mean ergodic theorem — for a further improvement, see the recent paper by Gaspar and Kohlenbach [6]. As far as number theory is concerned, Kohlenbach mentions extractive variations of van der Waerden theorem (on arithmetic progressions in sets) — in this case the variation has produced a better bound, but no new information on the combinatorial content of the proof. A more informative result using a Herbrand analysis was obtained by H. Luckhardt on Roth's theorem on the rational approximations of an algebraic irrational number [26]. This last result is certainly in line with a Kroneckerian spirit. Kohlenbach also mentions a more speculative potential mining of the Tanyama-Weil theorem in arithmetic geometry including Wiles's proof on Fermat's last theorem. Here one must add a reminder to the logician. André Weil has stressed the effectiveness of number-theoretic results by Fermat's method of infinite descent, for instance in the theory of finite fields, and Weil's own results have influenced considerably recent work in model theory — see [31] for Weil's view on infinite descent in finite fields. No mention is made of infinite descent in Kohlenbach's book and proof-theorists are reminded that Weil did not deem the diagonal method to be a valid method of proof in number theory. Of course, number theory is not the main target of applied proof theory, it is rather classical analysis and the central chapters of the book focus on Polish metric spaces, approximation theory and fixed point theory of non-expansive mappings. Those applications are rather involved technically, but they rest on logical methods that are duly reviewed in the introductory chapters — roughly half the length of the book. The book is indeed a major work in the field of applied proof theory and its impact on mathematical practice should be significant. That

was the objective of the proof theory practiced by G. Kreisel who wanted a logic relevant for mathematics — see Delzell [5] for the extensive review of Kreisel's unwinding of Artin's proof on the representation of rational functions by sums of squares. Kohlenbach's book reflects quite faithfully that objective.

2. *Hilbert's project of arithmetization*

Hilbert's intent in introducing the ε-symbol was to insure the passage from arithmetic to the ideal elements of set theory (including analysis), that is to insure consistency of infinitary mathematics with the help of finitary arithmetic, the theory of (primitive recursive) classical arithmetic. Hilbert devised the transfinite choice function to bridge the gap between finite arithmetic and Cantor's transfinite arithmetic (see [17]). But once the higher level of existence has been reached, one has to return or climb back to the finite basis: this is the descent method (*Methode der Zurückführung*) (see [19], II, p. 190) which consists of a construction (*Aufbau*) and its decomposition (*Abbau*) in arithmetical terms. The whole problem of consistency is thus a matter of recovering finite arithmetic through a process of elimination of the ε-symbol and the critical formulas attached to it. To the question often asked "Why introduce the ε-symbol if it is only to eliminate it afterwards?" the answer is simply: "To build up the ideal realm and redescend to the (arithmetical) foundations in order to secure the whole edifice of mathematics." Logic (and the axiomatic method) remains only a tool, insofar at it warrants elementary arithmetical inferences and the truth of elementary arithmetical statements (see [9]).

2.1. *The ε-symbol and its elimination*

The first axiom for the ε-symbol is

$$A(a) \rightarrow A(\varepsilon_x A(x))$$

where $\varepsilon(A)$ is a transfinite logical choice function [17]. The existential quantifier is defined by

$$\exists x Ax \equiv A(\varepsilon_x A(x))$$

and the universal quantifier by

$$\forall x Ax \equiv A(\varepsilon_x \neg A(x))$$

meaning that universal quantification can be asserted if no counterexample can be found — after a finite search, that is a finite iteration of the transfinite choice function.

Together with the Aristotelian axiom

$$\forall x Ax \to A(t)$$

and the excluded middle principle

$$\neg\forall x Ax \to \exists x \neg A(x)$$

these axioms constitute the axiomatic framework for the symbol ε and its minimal character could provide a passage from arithmetic to analysis and set theory with the rules of logic being only an auxiliary means (*Hilfsmittel*) or even a deviation (*Umweg*).

The introduction of the ε-symbol requires two theorems on critical formulas and their elimination: the first ε-theorem eliminates critical formulas attached to a term t

$$A(t) \to A(\varepsilon_r A(r))$$

by a method of symbolic resolution

$$(R) = \begin{cases} A(t_1) \to A(\varepsilon_r A(r)) \\ \vdots \\ A(t_n) \to A(\varepsilon_r A(r)) \end{cases}$$

which reproduces the decomposition of polynomials since terms and expressions are ordered according to degree and rank; the degree here is the maximal (finite) number of terms in a sequence of ε-terms and the rank of an ε-expression is the maximal (finite) number of expressions in a sequence of ε-expressions. As for polynomials, one obtains a reduction to a disjunctive form of terms without the ε-symbol, that is a linear expression. The second ε-theorem applies the same method to existential formulas and the identity axiom. It is the induction schema which creates problems here and requires a new critical formula

$$A(t) \to A(\varepsilon_r A(r)) \neq t'.$$

Substitution in this case is effected by means of number-names (*Ziffer*) or numerals for the ε-terms and the method will induce a formulation of the

principle of induction with the help of the ε-symbol. The formulas

$$A(a) \rightarrow A(\varepsilon_x A(x)) \neq a'.$$

and

$$a \neq 0 \rightarrow \delta(a)' = a$$

for the existence of successors and their recursion give way to a new induction principle which is stated:

> For every numerical predicate P which applies to at least one number, there is a number corresponding to P but for whose predecessor, if it exists at all, P is not applicable (see [19], II, p. 87).

The principle is equivalent to the least number principle with the general recursive function μ

$$A(a) \rightarrow (\mu_x A(x)),$$

with

$$A(x) \rightarrow \exists x(A(y)\ and\ \forall z(z < y \neg A(z))),$$

but the general procedure is reminiscent of polynomial decomposition in irreducible factors, *i.e.* the Euclidean algorithm of the greatest common divisor and its generalization by infinite descent for polynomials of degree n or by the chain condition for polynomial rings. S. Kripke has drawn an argument from this obvious fact to the collapse of the Hilbert programme (see note 1 and [24]). What is paradoxical in that connection is that the epsilon substitution method is used relying on ideal elements with transfinite induction to show the 1-consistency or ω-consistency of arithmetic. Of course, one needs here 2-consistency or outer consistency for Peano arithmetic, as Gödel says, but Gödel did not deny the possibility of an inner consistency proof, as I maintain later on. It remains though that the method of infinite descent is best suited for finite arithmetic and its internal logic (see [8] and [11]). Infinite descent is still an essential ingredient in an abstract or generalized form in contemporary arithmetic-algebraic geometry, for example in Galois cohomology theory.

The substitution principle takes the form of global or partial substitutions and the effective substitutions for terms will consist in finding the resolvent or the solution polynomial in reducing substitutions of term instances to substitutions in fundamental types of terms, *i.e.* terms that are not part of an other term. The process mimics Kronecker's general theory of elimination and the consistency proof will lead to the "*irreducible*" reduced formulas, as can be shown on the example of Ackermann's consistency proof

for arithmetic — reproduced in [19], Supplement V, pp. 535–555. Ackermann's proof relies essentially on the reduction number of global substitutions (*Gesamtersetzungen*) for numerals and functions using the machinery of recursive function theory: one ends up with a "normal sequence" in a polynomial expression

$$n_0 \cdot 2^k + n_1 \cdot 2^{k-1} + \ldots + n_{k-1} \cdot 2 + n_k$$

for the numbers n substituting for terms. The reduction number has the value 1 or 0, depending upon the global substitution being reduced to 0 or $j \neq 0$. The total number of global substitutions is 2^n when the number of ε-terms (of rank 1) occurring in the series of formulas is n, as is the case for the number of coefficients in the binomial, for example. For higher ranks, primitive recursive equations suffice

$$\psi(1, n) = 2^n$$

$$\psi(m + 1, n) = 2^{n\phi(m,n)} \cdot \psi(m, n).$$

The second ε-theorem has to do with the critical formulas of the second kind and the symbolic resolution of existential formulas. The main idea is to eliminate the existential quantifier from formulas like

$$\exists r_1 \ldots \exists r_r \forall n_1 \ldots \forall n_s A(r_1, \ldots, n_s)$$

to obtain a disjunction

$$\begin{array}{c} A(t_1^{(1)}, \ldots, t_r^{(1)}, f_1(t_1^{(1)}, \ldots, t_r^{(1)}), \ldots, f_s(t_1^{(1)}, \ldots, t_r^{(1)})) \vee \ldots \vee \\ A(t_1^{(m)}, \ldots, t_r^{(m)}, f_1(t_1^{(m)}, \ldots, t_r^{(m)}), \ldots, f_s(t_1^{(m)}, \ldots, t_r^{(m)})) \end{array}$$

where the terms $t_j^{(i)}$ do not contain the ε-symbol and the f_i's are function symbols with r arguments

$$f_1(c_1, \ldots, c_r), \ldots, f_s(c_1, \ldots, c_r).$$

If an equality axiom is added, a pure predicate calculus without the ε-symbol can be formulated and opens the way to a Herbrand-type consistency proof.

Hilbert had introduced the notion of a "disparate system of functions" with the explicit aim of producing a consistency proof for the pure predicate calculus (*i.e.* without identity). The functions in question are simple arithmetic functions which associate a numeral with a numerical expression in such a

manner that for a given numerical symbol (*Ziffer*) P and a disparate function system

$$\phi_1, \ldots, \phi_i,$$

the disjunction $S_p^{(\phi)}$ is derivable in the propositional calculus. A disparate function system is, for example (see [19], II, p. 175)

$$\phi_i(n_i, \ldots, n_r) = \psi_0^i \cdot \psi_1^{n_1} \ldots \psi_r^{n_r} \quad (i = 1, \ldots, s)$$

where the ψ_i's are the first $r+1$ primes. The idea is to associate, *disparately*, to each r-tuple of numerical symbols a different numerical symbol. The procedure looks like Brouwer's choice sequences, as Hilbert remarks, and can be extended to infinitely proceeding sequences. This first step in the arithmetization process must be completed by an arithmetical imitation of the grammatical structure of logical formulas (see [19], II, p. 217) through a translation with the help of recursive functions and predicates. Gödel achieved that kind of translation for the syntax of Peano arithmetic. We know that in this case the arithmetization could not be completed, mainly because the induction over an infinite set of numbers lends itself to Cantor's diagonalization procedure in contrast to Cauchy's diagonalization (the convolution product) which is applicable in Fermat-Kronecker arithmetic.

It might be worthwhile to note that the potential infinity of Brouwer's choice sequences, which Hilbert alludes to, allows for a treatment of the consistency problem compatible with Hilbert's programme. It is apparently in his attack on Cantor's continuum problem (see [19], II, p. 216) that Hilbert had the idea of arithmetization. The fact that the translation of transfinite arithmetic into finite arithmetic has not succeeded in Hilbert's hands is certainly one of the reasons for the success of the incompleteness results. Hilbert's programme however is not confined to set-theoretic arithmetic in Hilbert's own terminology and Kohlenbach's work is clearly in line with the arithmetization programme where one wants to remove the analytical clothing to uncover the arithmetical statements hidden beneath [20]. I am tempted to say that the ideal of arithmetization survives for the very reason that, as Hilbert confessed, the programme itself antedates Hilbert's efforts and can be traced back to Kronecker's idea of arithmetization of algebra. Arithmetization of logic is but a consequence of that original programme which was taken anew by E. Nelson's predicative arithmetic.

Robinson's theory of arithmetic Q is consistent and essentially undecidable. But E. Nelson's proof for the self-consistency of Q (in [28]) rests on a notion of genetic, as opposed to formal, number which allows for a computable or polynomially bounded exponentiation in the form

$$\sigma_0(\ell, n) = \exists f\ expcomp(\ell, n, f)$$

$$\sigma_n = \sigma_0(n, n).$$

where $expcomp(\ell, n, f)$ means that for all i in the domain of f, $i \leq n$ and $f(0) = \ell$; this leads for a given a to $explog(f(i), a)$ for $loglog\, a = f(i)$, a formula similar to the one I used for Euler's theorem on the infinity of primes.

The theorem on logical consistency says for a theory T:

$$T \text{ is tautologically consistent} \rightarrow T \text{ is } \sigma\text{-consistent}$$

and the inference

$$\sigma(b) \rightarrow \sigma(Sb)$$

is genetic while exponentiation $e(n)$ does not imply $\forall n\, e(n)$; exponentiation is not total.

This is reminiscent of Herbrand's arithmetic with induction on formulas without free variables (quantifier-free induction). Nelson's proof is based upon the Hilbert-Ackermann consistency proof for open theories (without quantifiers) which reduce to disjunctive propositional formulas — as in Herbrand's theorem — and they can be considered as *de facto* or intrinsic polynomials. In Nelson's genetic self-consistency proof for predicative arithmetic, the numbers denoted by terms of the arithmetized theory are bounded by the terms themselves (see [28] p. 176), while in the case of polynomialized arithmetic, the numbers (the terms) are bounded by the degree (and the height) of the translation polynomial. Bounded polynomial arithmetic would be an appropriate name for such an arithmetic. If we look at primitive recursive arithmetic and add as in Hilbert or Herbrand some restricted form of the least number principle (also found in Nelson), we are coming close to an arithmetic which I call Fermat arithmetic, where Peano's induction postulate is replaced by the method of infinite descent, which is not equivalent to (formal) infinite induction from a constructive point of view: the equivalence requires a double negation over an infinite set of natural numbers, a procedure which is obviously disallowed on constructivist (intuitionistic) grounds. Here one should point out that intuitionistic principles are not always up to the task. Poincaré — who calls infinite descent "récurrence" — and Peirce are two authors who have forcefully emphasized the distinction for different reasons. The main reason to me is that infinite descent embodies a central method of proof in number theory. The method is employed negatively as *reductio ad absurdum*, but also positively [8]. Fermat, Euler, Lagrange (who called infinite descent *réduction*), Legendre and Kummer all used the

method to prove important theorems in number theory. Nowadays, Mordell, Weil, Serre, Faltings and others use it in arithmetic (algebraic) geometry.

Hilbert acknowledges that Kronecker has succeeded in constructing a finitary theory of algebraic numbers and of the field of algebraic numbers, but he says that this theory was to be found only in Kronecker's lectures without mentioning that the major paper of 1882 *"Grundzüge einer arithmetischen Theorie der algebraischen Grössen"* [25] contains certainly the main ingredients of the theory. Nevertheless, Hilbert does not misrepresent Kronecker's achievements and one can suppose that it is the same process of association he has in mind when he wants to adjoin ideal elements to finite arithmetic, although he seems to give credit to Kummer rather than to Kronecker [17].

2.2. *Hilbert's finitist stance*

The finitist "stance" (*die finite Einstellung*) is certainly the heir of Kronecker's arithmetical constructivism, but the introduction of the ε-symbol and formal logic that one eliminates to come back to the internal (*inhaltliche*) logic of arithmetic means that finite arithmetic is self-consistent by construction: logical formulas are true by granting them numerical content through numeral substitution in the method of return and polynomial decomposition or descent reverses the process of construction into a process of reduction. If the notion of predecessor is more structural or less internal than the notion of "smaller than", as Hilbert suggests, it is to preserve the axiomatic character of the least number principle, but its true arithmetical nature is revealed in the finite process of the Fermatian method of descent.

Formal logic for Hilbert has only an ancillary role, it only guarantees the passage from arithmetic to its algebraic extensions through the adjunction of ideal elements (indeterminates). But these ideal elements are algebraic in essence and Kronecker did not need formal logic for his general arithmetic. For Kronecker, the negative transcendence of non-algebraic extensions cannot be redeemed by indeterminate quantities (see [25], p. 253). At this point, one is reminded of Steinitz who in his 1910 *Algebraische Theorie der Körper* has "completed" the Kroneckerian theory of domains of rationality integrating infinite transcendent extensions (with an infinite number of indeterminates also called "transcendents"), but only by resorting to set-theoretic notions of well-order (the axiom of choice and transfinite induction on ordinals). The continuation is no more of Kronecker's intent and Kronecker had warned (see [25], p. 156) against infinitary procedures and had emphasized the fact that infinite power series have an arithmetical construction of their coefficients and also that finite polynomial expressions dispense with any extension of the concept of finite series.

The way back from extensions in the ideal realm meant for Hilbert that consistency of analysis and set theory could be attained by finite means.

But the reduction has also another meaning for Kronecker: the theory of divisors or congruences in modular systems affords a reductive theory of algebraic extensions under the isomorphism between extensions with a finite number of indeterminates and polynomials in the field (or rather domain of rationality) of algebraic numbers. It is that lesson which Hilbert seems to have remembered, at least partially, in his ultimate finitist programme of the *Grundlagen der Mathematik*. But it is the algebraic closure of the theory of indeterminates (beneath the theory of real fields) which limits upstream Hilbert's programme while Gödel's incompleteness results are only a downstream obstacle that is not fatal to finitist foundations understood in Kroneckerian terms.

It is common knowledge that mathematics or proof theory is concerned with finitary methods as in Hilbert's conception of a theory of formal systems. I contend that the consistency question is the crux of the matter and that it requires a finistist approach in the sense of Kronecker. The rather sketchy attempt on the simultaneous foundation of logic and arithmetic in the 1904 paper *"Über die Grundlagen der Logik und der Arithmetik"* (see [18]) puts forward the concept of homogeneous equations in a manner reminiscent of Kronecker's combinatorial theory of (homogeneous) polynomial equations. Consistency, following Hilbert, boils down to the homogeneous equation $a = a$ or inequation $a \neq a$. At the time, according to the testimony of Bernays, Hilbert was tempted to lay down his arms to the finitist Kronecker, whom he accused of dogmatism; but under the threat of the paradoxes, he momentarily abandoned his foundational query, and submitted to Kronecker in perpetuating the Kroneckerian tradition among others in number theory and in algebra. It is only in 1918 that Hilbert resumed his foundational research and returned to finitism, not without polemizing with Kronecker (posthumously!), Brouwer and Weyl whom he considers as Kronecker's direct heirs. The simultaneous foundation of logic and arithmetic still dominates his preoccupations and the recourse to the notion of formal system is meant as a mechanism (a finite algorithm) for the introduction of ideal elements. My hypothesis is that this process mimics Kronecker's association of forms in his general arithmetic and the consistency which is required for the association of ideal elements can only be achieved by a formalism which is the exact counterpart of an arithmetic (polynomial) algorithm, *e.g.* the method of descent as a generalized Euclidean algorithm.

The propositions of general arithmetic that are found in Kronecker's *"Grundzüge einer arithmetischen Theorie der algebraischen Grössen"* [25] can be considered as so many axioms from which Kronecker derived his results with arithmetical means alone. In his 1918 *"Axiomatisches Denken"* (see [18], pp. 146–156), Hilbert pinpoints the properties of independence and consistency as the main features of the axiomatic method. Relative consistency of geometry and other scientific disciplines, Hilbert suggests, is based

on the consistency of arithmetic, but there is no further foundation for arithmetic and, Hilbert adds, set theory. Logic is the ultimate foundation and it must also be axiomatized and in the final analysis there only remains for the axiomatic method the question of decidability which must be settled "in a finite number of operations" (see [18], p. 154). Here Hilbert gives the example of the theory of algebraic invariants for which he had provided a finiteness proof inspired by the very method he had used in his major result: Hilbert's finite basis theorem depends heavily on Kronecker's own methods in general arithmetic and becomes the paradigm case for the decidability property of a logical system! But there is no logic involved in Hilbert's result and his paradigmatic case is drawn from polynomial arithmetic (Kronecker's general arithmetic of forms). Decidability implies, of course, that we have an algorithm or a finite procedure to decide of a given question in a "finite number of steps". We then come back to our point of departure and it is not surprising to see that most decidable theories are elementary (first-order) algebraic theories and have ended as the subject-matter of model theory, not proof theory. The method of quantifier elimination, for instance, is a test for decidability and has been employed by Tarski in his well-known model-theoretic results; van den Dries has stressed the influence of Kronecker's methods in that context [30]. But then what is the logical point of the decision method? A decidable theory if consistent is finitely so. In the specific case of the elementary theories, logic does not play any special role since the equational calculus of polynomials does not need other operations than the purely arithmetical (combinatorial) laws.

The case for logic rests solely on the alleged conservative extensions of arithmetic into the transfinite domain of ideal elements. It remains though that even if Hilbert had hoped for a logical introduction of ideal elements, he has constantly stressed that a finite process (or procedure) is the inference engine of internal (*innere*) consistency [9], [11].

Internal consistency is obtained by internal means in the case of general arithmetic as in the case mentioned above of the theory of algebraic invariants. Hilbert was not mistaken there and he saw consistency as internal to the polynomial equation calculus when he defined consistency as the equation $a = a$ and inconsistency as $a \neq a$. One of the essential tools of internal consistency is the convolution product which generates linear polynomial expressions from linear polynomial expressions as in Kronecker's result, Dedekind's Prague theorem or Hilbert's work in invariant theory. The convolution or Cauchy product can be called Cauchy diagonal. A serious blow to Hilbert's programme was given from the outside, the "external" Cantor diagonal in Gödel's results. The set-theoretic diagonalization does not belong to number theory or algebra, but to set-theoretic arithmetic, as Hilbert himself has named it, but it is also set theory that he wanted to secure in his proof theory. It is another paradoxical situation for the logician Hilbert to

see his full-blown programme for consistency of set theory and analysis put in jeopardy by a set-theoretic device!

A more balanced view would call for a reconciliation of Kronecker's and Hilbert's programmes. New foundations for Hilbert's programme invite to dig deeper in Hilbert's programme and to lay bare the roots of Hilbert's metamathematical idea. Consistency and decidability constitute the main avenues we have followed — independence being a minor logical track for our purpose — and they appear already in Kronecker's work in another disguise.

3. *The continuation of Hilbert's programme*

Herbrand's theorem and Gödel's functional interpretation were devised as a response to Hilbert's programme. Herbrand wanted a finitist consistency proof for arithmetic and his theorem for predicate logic is in the line of the Hilbert-Ackermann consistency theorem which says:

> An open theory T is inconsistent iff there is a quasi-tautology which is a disjunction of negations of nonlogical axioms of T.

An open theory T has its nonlogical axioms quantifier-free and a quasi-tautology is a tautological consequence of instances of equality axioms. Herbrand's theorem holds for quasi-tautologies in classical first-order predicate calculus with equality and it is in this form that it is employed in applied proof theory. Gödel proposed his quantifier-free *Dialectica* interpretation to overcome the finitist framework by introducing functionals as abstract types beyond the natural numbers or the concrete objects of a Hilbertian formal system. The shift of emphasis initiated by Kreisel and the course taken by Kohlenbach consist in focusing on the existential quantifier in formulas in order to "scoop in" the parameters of a given proof in functional terms. There seems to be a task more modest than Hilbert's grand design of the consistency problem couched in the universal quantifier — the existential quantifier can be more easily eliminated! Here again a reminder: Hilbert had conceived a polynomial calculus (the epsilon calculus) subjected to infinite descent in order to reduce ε-formulas — infinite descent is called *"die Methode der Zurückführung"* in Hilbert and Bernays (see [19], p. 190), as I have shown above, and it is natural to think that both Herbrand and Gödel had such a calculus in mind and hoped to further it by other means, that is a theory of ascending types versus the number-theoretic method of infinite descent — this could be the main cleavage between number theory and logic (and the cumulative hierarchy of set theory by the same token) but infinite descent is

still at work in ZF with von Neumann's axiom of foundation inspired by Mirimanoff's idea of finite descent for ordinals (*ensembles ordinaires*) (see [10] p. 38 and [11] p. 83), that is transitive sets. With von Neumann ordinals arose the identification (confusion) of transfinite induction with infinite descent in axiomatic set theory, beyond Mirimanoff's finitist stance [27]. At any rate, Herbrand's and Gödel's efforts have resulted in a proof theory searching for polynomial bounds, but it should be noted that this proof theory is not interested in the computational complexity of proofs for logical calculi (the work of Cook, Urquhart, Krajicek, Pudlák and others) but in extracting bounds for proofs in classical analysis. If the business of proof mining is not devoid of tricks, as Kreisel has admitted [23], the main objective is the transformation of non-effective proofs into effective ones. Effective may mean computable, but sometimes effective proofs are hard to compute or hardly computable and the constructive content is far from being apparent; nonetheless, the objective is most of the time to retrieve more information from a non-constructive proof.

The paradigm theory is here again number theory and polynomial arithmetic. What Kronecker called general arithmetic (*allgemeine Arithmetik*) for his theory of forms or homogeneous polynomials is in more ways than one the mother theory of contemporary arithmetic-algebraic geometry where a given result of finiteness does not yield an explicit calculation for solutions (or the number of points). Among the logical methods used by applied proof theory, it is the functional interpretation which is privileged and it comes equipped with a logical (hereditarily inductive) relation of majorazibility $\geq$ (due to W.A. Howard) which is in a sense the logical counterpart of number-theoretic minorization. The relation

$$x^* \text{ majorizes } x\ (x^* \geq_0 x)$$

is defined for closed terms by induction on functionals of finite types; as Kohlenbach points out it is a structural property of the closed terms which eschews normalization (see [21], p. 60). As is well known, the logical background of the functional interpretation was intuitionistic, since constructions over and above formal objects (concrete representations of natural numbers) were allowed in. E. Bishop wanted to reduce those constructions to their numerical content, but the logical formalisms that have evolved from intuitionistic motivations pervade the techniques of applied proof theory. For instance, the fan rule that is mentioned and used by Kohlenbach (see [21] p. 111) is a descendant of Brouwer's fan theorem which is a finiteness law for spreads (*spreiding*) in an arborescent structure whose branches are assigned natural numbers; this is the equivalent of the axiom of choice and it is linked with the (weak) König's lemma on a finitely-branched infinite tree.

Brouwer derived from the fan principle his famous theorem stating that "Every total function in the real interval $[0, 1]$ is uniformly continuous". Kleene's realizability interpretation for intuitionistic logic with numerical realizers or witnesses for functions, Kreisel's modified realizability, Gödel's negative translation from intuitionistic logic to classical logic, Markov's principle of double negation elimination for the existential quantifier, bar-recursion associated with the fan rule, all those notions are called to duty in the prospection procedures. Modified realizability was put forward to escape Markov's principle

$$\neg\neg\exists x A(x, y) \rightarrow \exists x A(x, y)$$

independent from intuitionistic principles and not realizable in the typed lambda-calculus of modified realizability. But the full functional calculus on all finite types, that is the full-blown system HA^{ω} of Heyting arithmetic can accommodate Markov's principle; Kohlenbach even shows (chapter 7) that an extensional Heyting arithmetic can be made semi-intuitionistic by adopting highly non-constructive principles. Meanwhile, the functional interpretation assigns to each formula $A(a)$ of HA^{ω} a formula

$$B \equiv \exists x \forall y A(x, y, a)$$

where A is quantifier-free and x, y are variables of finite type. The idea is to extract a computational witness (a realizer) as a closed term by more or less constructive means. This is a task Kohlenbach accomplishes with a vast array of technical means and an extensive logico-mathematical machinery — for instance, chapter 11 treats "The functional interpretation of full classical analysis" via a variety of comprehension and choice principles. A nice application is on Polish (complete and separable) metric spaces where a function (type-1 object) represents a unique element X for a computable enumerative procedure that picks a closed term as a bound. Other examples in function approximation theory abound.

Whatever the benefits of the functional interpretation in the process of proof transformations, one should not forget that Gödel had in mind what I call the "internal consistency" of arithmetic in contrast with the external or outer consistency, the so-called ω-consistency or 1-consistency. Gödel was apparently not satisfied with Gentzen's recourse to transfinite induction and had not rejected an inner treatment of the consistency problem. In a 1972 note (see [15]), Gödel draws the attention to a remark he had made in 1966 (see [14] on "outer" or ω-consistency saying that "perhaps it has not received sufficient notice". Gödel's insistence on outer consistency refers to Hilbert's own characterization of a formal system as *"äusseres Handeln"* or external treatment of internal or contentual inference *"inhaltliches Schliessen"*. The very idea of outer consistency means that internal consistency of various

systems of arithmetic cannot be proven within the concrete finite ressources afforded by the external treatment of a formal system. Consistency or ω-consistency must be assumed from without in order to justify the transfinite axioms, as Gödel says. That does not mean however that Hilbert's consistency programme is doomed to failure, only that it must be pursued by more internal — or more abstract — means. Gödel's *Dialectica* interpretation is an attempt in that direction — see my Abstract in the *Bulletin of Symbolic Logic* [12].

4. *Concluding remarks*

We know that Herbrand defended a finitist point of view in the lineage of Hilbert. In a recent article in *Philosophia Mathematica* [1], Jeremy Avigad credits Harvey Friedman with the following *Grand Conjecture*:

> Every theorem published in the *Annals of Mathematics* whose statement involves only finitary mathematical objects (*i.e.,* what logicians call an arithmetical statement) can be proved in elementary arithmetic.

But Herbrand had already what I call Herbrand's conjecture:

> Transcendental methods cannot prove theorems of arithmetic that cannot be proven within arithmetic itself.
> *Écrits logiques* (see [16], p. 152. My translation. See my Abstract in *JSL* [7])

What Herbrand obviously meant is that theorems in arithmetic must always be provable with aritmetical means alone. Herbrand stated his conjecture for a suitable formal system which he does not describe — not a subsystem of Peano arithmetic that Avigad has obviously in mind. Herbrand was also a practitioner of (algebraic) number theory and he expressed himself in Kroneckerian terms when he used what he called "intuitionistic" arguments where one supposes that an object (logical or mathematical) does not exist without the means to construct it. In the same line of thought, he defends the potential infinite for his notion of infinite domain (*champ infini*) by saying that it is built iteratively *"pas à pas"* or *"Schritt zu Schritt"* in Kroneckerian terms.

Hilbert introduced ideal elements (*ideale Elemente*) in order to have a clear-cut divide between the finite and the non-finite, a divide that Aristotelian logic did overlook, because it could not survey — *"Unübersichtlichkeit"* in Hilbert's text [17] — the extent of its applications. The idea of the epsilon-calculus for the ε-symbol was to enable the extension of the simple laws of Aristotelian logic, excluded middle and universal instantiation with existential import, to the transfinite universe of ideal statements: once this is achieved, one could redescend in the finite by elimination of the ideal elements or the epsilon formulas by a finite process in polynomial arithmetic, that is the use of infinite descent (*die Methode der Zurückführung*), as I have shown in my book *Internal Logic* (see [11], pp. 68 and ss.) — of course, the second incompleteness result on external consistency could only be obtained from a transcendent point of view, the ω-view, outside that framework (*idem*, pp. 46, 80, 192).[1]

Intuitionistic logic, after the work of Brouwer, Kolmogorov, Heyting and Gödel, fares better in discriminating between the finite and the infinite, simply by rejecting the extension of classical logical laws beyond the finite domain and by digging the principles that govern the potential infinite. This explains why it is the starting point of the functional interpretation privileged by applied proof-theorists; in their hands, intuitionistic logic is extended by various non-constructive principles or one-way translations from intuitionistic logic to classical logic. There is the foundational shift from Hilbert's programme and it has proven successful in recent proof-theoretic research. Still the shift does not mean that applied proof theory has gone adrift from Hilbertian proof theory and the abundance of applications should not distract the outsider from the fact that all the results, particularly in fixed-point theory, rely on logical metatheorems stemming from general proof-theoretic methods and ideas (from Herbrand and Gödel) that are an integral part of the Hilbertian heritage. Kohlenbach's work must be seen in that perspective. Of course, the constructivist motto has to be substantiated by further foundational research into the historical, logico-mathematical and philosophical motives of proof theory. Hilbert was certainly the first mathematician to think of mathematical proofs in terms of a systematic study of the internal logic of deductive reasoning (*das inhaltliche logische Schliessen*) in line with

[1] Apparently, in recent lectures on "The Collapse of the Hilbert Programme", Saul Kripke has rediscovered and reproduced the very same argument (see [24]). Although Kripke does not mention infinite descent as in previous lectures, he refers to a minimilization argument which amounts to the same for Mirimanoff's *ensembles ordinaires* obtained by descent or transitive sets in ZF also obtained from descent via the axiom of foundation or regularity. Compare my own abstract [12] and paper [8]. See also my 1997 French book [10], pp. 38–39 and pp. 208–212.

Kronecker's constructive stance in his general arithmetic (*allgemeine Arithmetik*) for which he claimed "*innere Wahrheit und Folgerechtigkeit*", that is internal truth and consistency; these objectives could very well be shared by applied proof theory in the search for the effectivity of proofs in classical analysis. E. Bishop in his pioneering work on constructive analysis was looking for the numerical content of classical mathematics and had admitted that he had been inspired by Kronecker rather than by Brouwer. This is not the road taken by logicians in proof theory. Proof theory puts the emphasis on proofs with the aim of making manifest their constructive hidden content and that is a major endeavour in foundational research.

If applied proof theory and the proof mining enterprise represents a shift of emphasis in original (pure!) proof theory as Kohlenbach repeats after Kreisel, it remains that the idea of extracting more constructive information from a given classical proof concurs with the idea of security or certainty that Hilbert defined as the ideal goal of his proof theory and the motto of applied proof theory could very well be "More information, more certainty". Detracting from that ideal, which is not epistemic but foundational, would mean fruitless prospection for proof-theorists, either in the abstract realm of constructivist principles or in the mining field of promising applications.[2]

Département de Philosophie
Université de Montréal
C.P. 6128, succursale Centre-ville
Montréal, Québec
H3C 3J7 Canada
E-mail: yvon.gauthier@umontreal.ca

REFERENCES

[1] J. Avigad. Number Theory and Elementary Arithmetic. *Philosophia Mathematica*, XI:257–284, 2003.

[2] T. Coquand. Herbrand et le programme de Hilbert. *Gazette des Mathématiciens*, 118:17–28, 2008.

[3] T. Coquand, H. Lombardi, and C. Quitte. Generating non-Noetherian Modules Constructively. *Manuscripta Mathematica*, 115:513–520, 2004.

[4] M. Coste, H. Lombardi, and M.F. Roy. Dynamical Methods in Algebra: Effective *Nullstellensätze*. *Ann. Pure Appl. Logic*, 111:203–256, 2001.

[2] I thank Professor Kohlenbach for additional information and comments on this paper. I also thank an anonymous referee for numerous helpful remarks.

[5] C.N. Delzell. Kreisel's Unwinding of Artin's Proof, Part 1. In P. Odifreddi, editor, *Kreiseliania*, pages 113–246. A.K. Peters, 1996.
[6] J. Gaspar and U. Kohlenbach. On Tao's "Finitary" Infinite Pigeonhole Principle. *Journal of Symbolic Logic*, 75(1):355–371, 2010.
[7] Y. Gauthier. Le constructivisme de Herbrand. *The Journal of Symbolic Logic*, 48(4):1230, 1983.
[8] Y. Gauthier. Finite Arithmetic with Infinite Descent. *Dialectica*, 43(4):329–337, 1989.
[9] Y. Gauthier. Hilbert and the Internal Logic of Mathematics. *Synthese*, 101:1–14, 1994.
[10] Y. Gauthier. *Logique interne. Modèles et applications.* Diderot, Paris, 1997.
[11] Y. Gauthier. *Internal Logic. Foundations of Mathematics from Kronecker to Hilbert.* Kluwer, Synthese Library, Dordrecht / Boston / London, 2002.
[12] Y. Gauthier. The notion of outer consistency from Hilbert to Gödel. *The Bulletin of Symbolic Logic*, 13(1):136–137, 2007.
[13] K. Gödel. Über eine noch nicht benüzte Erweiterung des finiten Standpunktes. *Dialectica*, 12:230–237, 1958.
[14] K. Gödel. On formally undecidable propositions. In Jean van Heijenoort, editor, *From Frege to Gödel: a source book in mathematical logic 1879–1931*, pages 616–617. Harvard University Press, 1967.
[15] K. Gödel. In S. Feferman, editor, *Collected Works*, volume II, page 305. Oxford University Press, New York / Oxford, 1990.
[16] J. Herbrand. *Écrits logiques.* J. van Heijenoort, ed. PUF, Paris, 1968.
[17] D. Hilbert. Über das Unendliche. *Mathematische Annalen*, 95:161–190, 1926.
[18] D. Hilbert. *Gesammelte Abhandlungen III.* Chelsea, New York, 1932.
[19] D. Hilbert and P. Bernays. *Grundlagen der Mathematik I et II.* Springer-Verlag, Berlin, 2. edition, 1968–1970.
[20] U. Kohlenbach. Arithmetising Proofs in Analysis. In Lascar, D., Larrazabal, J.M. and G. Mints, editors, *Logic Colloquium '96*, volume 12 of *Springer Lecture Notes in Logic*, pages 115–158. 1998.
[21] U. Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics.* Springer-Verlag, Berlin / Heidelberg, 2008.
[22] U. Kohlenbach. Functional Interpretation and its Use in Current Mathematics. *Dialectica*, 62:223–267, 2008.
[23] G. Kreisel. Extraction of bounds: interpreting some tricks of the trade. In P. Suppes, editor, *University-level computer-assisted instruction at Stanford: 1968–1980*, pages 153–164. Stanford University Institute for Mathematical Studies in the Social Sciences, 1981.

[24] S. Kripke. The Collapse of the Hilbert Program: Why a System Cannot Prove its Own 1-consistency. *The Bulletin of Symbolic Logic*, 15(2):229–230, 2009.
[25] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. In K. Hensel, editor, *Werke*, volume III, pages 245–387. Teubner, Leipzig, 1968.
[26] H. Luckhardt. Herbrand-Analysen zweier Beweise des Satzes von Roth: Polynomiale Anzahlschranken. *Journal of Symbolic Logic*, 54:234–263, 1989.
[27] D. Mirimanoff. Les antinomies de Russell et Burali-Forti et le problème fondamental de la théorie des ensembles. *L'enseignement mathématique*, 19:17–52, 1917.
[28] E. Nelson. *Predicative Arithmetic.* Number 32 of Mathematical Notes. Princeton University Press, Princeton, N.J., 1987.
[29] J.R. Shoenfield. *Mathematical Logic.* Addison-Wesley, Reading, Mass, 1967.
[30] L. van den Dries. Alfred Tarski's Elimination Theory for Real Closed Fields. *Journal of Symbolic Logic*, 53:7–19, 1988.
[31] A. Weil. *Number Theory: An Approach Through History, From Hammourabi to Legendre.* Birkhäuser, 1984.