*Logica Trianguli*, 5, 2001, 19-41

# INTERNAL AND EXTERNAL CONSISTENCY OF ARITHMETIC

Yvon GAUTHIER

**Abstract**

What Gödel referred to as "outer" consistency is contrasted with the "inner" consistency of arithmetic from a constructivist point of view. In the set-theoretic setting of Peano arithmetic, the diagonal procedure leads out of the realm of natural numbers. It is shown that Hilbert's programme of arithmetization points rather to an "internalisation" of consistency. The programme was continued by Herbrand, Gödel and Tarski. Tarski's method of quantifier elimination and Gödel's *Dialectica* interpretation are part and parcel of Hilbert's finitist ideal which is achieved by going back to Kronecker's programme of a general arithmetic of forms or homogeneous polynomials. The paper can be seen as a historical complement to our result on "The Internal Consistency of Arithmetic with Infinite Descent" (*Modern Logic*, vol. 8, n° 1-2, 2000, pp. 47-86). An internal consistency proof for arithmetic means that transfinite induction is not needed and that arithmetic can be shown to be consistent within the bounds of arithmetic, that is with the help of Fermat's infinite descent and Kronecker's general or polynomial arithmetic, thus returning into arithmetic without the detour of Cantor's transfinite arithmetic of ideal elements (the tranfinite ordinals).

## 0. Introduction

In his original paper [6], Gödel proves an incompleteness theorem for Peano arithmetic and acknowledges that his second incompleteness result (on consistency proofs) does not contradict Hilbert's formalist standpoint, since it is possible that some finitist proofs could not be represented in the formal system of Peano arithmetic and more comprehensive systems, i.e. set theory and classical analysis (see [6], p. 197). Gödel's proof uses ω-consistency and in a 1966 note of the English translation of his paper [7], Gödel speaks of ω-consistency in terms of "outer" consistency. Although Rosser [16] has reduced ω-consistency to "inner" simple consistency by incorporating recursive enumerability to an extension $S_k$ of S (the formal system containing

Peano arithmetic), it is not an internalization of consistency and I want to show in the following that an internal (as opposed to external) consistency proof for arithmetic is possible in the sense intended by Hilbert, a possibility which remains apparently an open question for Gödel. Gödel's own *Dialectica* interpretation can be seen as an attempt to provide such a finitist consistency proof in terms of functionals of finite type over the integers.

**1. Arithmetic within and without**

We can express ω-consistency in the following manner: for any first-order theory T for Peano arithmetic

$$n \vdash_T A^{-},n \rightarrow \nvdash_T \ x \neg Ax$$

for the numeral $^{-},n$ and all formulas Ax. The first part of the expression is "external" in the sense that it draws from the outer world of arithmetic to establish the consistency of the formal system S of arithmetic (the second part of the expression) which could be read

$$n \vdash_S A^{-},n \rightarrow \neg\vdash_S \ x \ Ax$$

to make the passage from external to internal consistency of S. In Gödel's words — in the 1930 abstract — ω-consistency is defined for properties F(x) of natural numbers. B. Rosser (after Kleene) introduced general recursive functions and the concept of recursive enumerability of formulas within S to reduce ω-consistency to simple consistency and thus generalize Gödel's result together with Church's result on recursive undecidability [2]. The fact that in set-theoretic arithmetic there is a recursively enumerable set which is not recursive is basic (see Kleene [13], theorem XII). As Kleene puts it:

> "The class $\ x \ y \ T_1 (z, x, y)$ of the numbers z which define functions $\phi(x)$ recursively is not recursive".

More generally, the set of recursive functions cannot be enumerated by a recursive function; in particular, as in Church's paper [2], there is no binary recursive predicate which enumerates all unary ones. For example, let $P_k$ be a binary predicate; for each number k, define a unary predicate $P_{(k)}$

$$P_{(k)}(a) \leftrightarrow P(a, k).$$

By diagonalization, let us have a unary predicate Q defined by

$$Q(a) \leftrightarrow \neg P(a, a).$$

Q will be distinct from all the $P_{(k)}$, since by putting $Q = P_{(k)}$ we obtain the following contradiction

$$P(k, k) \leftrightarrow P_{(k)}(k) \leftrightarrow Q(k) \leftrightarrow \neg P(k, k).$$

This is an effect of the diagonal procedure borrowed from Cantor's arithmetic and transplanted into Peano's arithmetic. Although the diagonal procedure does not lead outside the class of recursive functions when applied to a particular recursive sequence of Gödel numbers for a system of equations (defining recursive functions), the notion of a general recursive function offers no constructive process for determining when a recursive function is defined, as Kleene says ([12], p. 738). The crux here is indeed when the diagonal procedure is applied to the total enumeration, that is, the class or the set of all such sequences. Gödel acknowledges ([6], p. 175) the extraneous character of the diagonal procedure when he says that it is to a certain extent a matter of chance (<*gewissermaßen zufällig*>) if a given formula obtained by diagonal substitution turns out to be an undecidable sentence that says of itself that it is not provable; self-reference is but a by-product of the diagonal procedure which generates what one can call Cantor numbers beyond Gödel numbers for formulas in PA. Here is a brief sketch of a proof using ω-consistency for Cantor numbers.

Set

$$C = c_i = g_{i1}\, g_{i2} \ldots g_{ii}$$

for C the diagonal or Cantor number of the sequence of Gödel numbers of sentences of S enumerated by

$$C_1 = g_{11}\, g_{12} \ldots g_{1n}$$
$$C_2 = g_{21}\, g_{22} \ldots g_{2n}$$
$$\vdots$$
$$C_n = g_{n1}\, g_{n2} \ldots g_{nn}.$$

$C(= c_i)$ will be different of all c's by having $c_i$ differ from all c's by at least one assignement of a Gödel number to any given symbol in a recursively enumerable sequence (of symbols). The sentence

(*) $$x_2 \neg \underline{Pr}\ (\bar{C}, x_2)$$

(where Pr is for proof and underlined terms indicate that we are inside the formal system S) is undecidable in S and we have

$$\nvdash_S \quad c\ Pr\ (\bar{C}, c);$$

for $\neg (\ )$, we have

$$\nvdash_S \quad x_2 \neg Pr\ (\bar{C}, x_2)$$

hence

$$\vdash_S \quad c\ Pr\ (\bar{C}, c).$$

But $c \neq C$ for all c's and I can't have the fixed point theorem or diagonalization

$$\vdash_S C \leftrightarrow A(\ulcorner,c)$$

for A(c), a formula obtained from a formula $A(x_1)$ with the one free variable $x_1$ by substituting the Gödel number of the sentence c to $x_i$. I conclude therefore

$$\vdash_S \quad c \; Pr \; (\bar{C},c)$$

a contradiction. Inside S, a Cantor number differs from any Gödel number

$$c \; (c \neq C)$$

and, moreover, it is undecidable whether it is denumerable or non-denumerable. The result emphasizes the incompleteness of PA, since one cannot even demonstrate that $\bar{C}$ represents a decidable sentence — if it has a Gödel number or not. We can certainly evoke Skolem's paradox for set theory in this curious situation, since inside S, $\bar{C}$ is non-denumerable (( )does not have a Gödel number), but from outside of S, it must have a Gödel number, ( )being an arithmetical sentence of S. The Cantor number being non-denumerable does not even belong to Cantor's second number class defined by

$$\lim_{n \to \omega} \left\{ \omega^{\cdot^{\cdot^{\cdot^{\omega}}}} \right\}^{n} = \varepsilon_0.$$

If it were, $\omega_0$-consistency would correspond to $\varepsilon_0$-consistency. The fact that the ordinal $\varepsilon_0$ provides a consistency proof (due to Gentzen) for Peano arithmetic means only that one must transcend $\omega_0$ into $\omega_1$ which, according to Cantor's normal form theorem, is no more representable in polynomial form: $\varepsilon_0$ is a transcendental ordinal! In order to justify the diagonal procedure, from Cantor to Gödel, one must get beyond natural numbers in the transcendental point of view of the transfinite or transarithmetical universe. As Tarski remarks in his [17], $\omega$-consistency (and $\omega$-completeness) require an "actually infinitistic" system $T_\infty$ with an infinite induction rule (called now the $\omega$-rule), while the system $T_\omega$ of primitive recursive arithmetic is only a "potentially infinitistic" system.

Of course, Gödel's use of the diagonal procedure in the arithmetization of the formal system S of arithmetic is in close analogy with Richard's paradox, as Gödel himself points out. The lexicographic order mentioned in footnote 15 of [6] clearly refers to Richard's enumeration of sentences defining a real number; Richard number is not in the enu-

meration, since it differs by at least one decimal from all other sentence numbers, nevertheless it is defined by a finite sequence (of letters in the lexicographic order). Cantor number likewise is not in the enumeration of all Gödel numbers, although it is defined by diagonalization in the infinite sequence of natural numbers. Gödel's terminology involves class signs, the (denumerable) totality N of which is arranged in some ordered sequence: the class of natural numbers denoting the negations of proofs clashes with a sequence R of class signs generated diagonally and for a certain natural number q, R(q) is neither provable, nor unprovable. The set of all finite sequences is thus the proper arena and one can apply the diagonal procedure to sequences of Gödel numbers to generate the Cantor number of a given sequence which does not belong to the enumeration of Gödel numberings. It is the programme of arithmetization of metamathematics initiated by Hilbert in 1922 (see [10]) which is at stake here. I shall concentrate on the final form ot the programme in the *Grundlagen der Mathematik* [8].

## 2. Hilbert's programme 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 Z of (primitive recursive) classical arithmetic. Hilbert devised the transfinite choice function to bridge the gap between finite arithmetic and Cantor's transfinite arithmetic (see [11]). But once the higher level of existence has been reached, one as to return or climb back to the finite basis: this is the descent method <*Methode der Zurückführung*> ([8], 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.

### *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 [11]. 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

$$\forall x Ax \rightarrow A(a)$$

and the excluded middle principle

$$\neg \forall x Ax \rightarrow \exists x \neg A(a)$$

these axioms constitute the axiomatic framework for the symbol $\varepsilon$ and its minimal character could provide a passage from arithmetic to analysis and set theory with the rules of logic being only an auxiliairy means <*Hilfsmittel*> or even a deviation <*Umweg*>.

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

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

by a method of symbolic resolution

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

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 $\varepsilon$-terms and the rank of an $\varepsilon$-expression is the maximal (finite) number of expressions in a sequence of $\varepsilon$-expressions. As for polynomials, one obtains a reduction to a disjunctive form of terms without the $\varepsilon$-symbol, that is a linear expression. The second $\varepsilon$-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

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

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

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

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" ([8], II, p. 87).

The principle is a direct consequence of the least number principle with the general recursive function μ

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

with

$$A(x) \rightarrow \quad y\,(A(y) \qquad z\,(z < y \rightarrow A(z))),$$

but the general procedure is reminiscent of polynomial decomposition in irreducible factors, i.e. the Euclidian 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.

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 mimicks 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 the second edition of Hilbert and Bernays, II, 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

$$n_0 \cdot 2^h + n_1 \cdot 2^{h-1} + \ldots + n_{h-1} \cdot 2 + n_h$$

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 $\varepsilon$-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

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

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

The second $\varepsilon$-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

$$r_1 \ldots \; r_r \; n_1 \ldots \; n_s \, A(r_1, \ldots, n_s)$$

to obtain a disjunction

$$A(t_1^{(1)}, \ldots, t_r^{(1)}, f_1(t_1^{(1)}, \ldots, t_r^{(1)}), \ldots, f_s(t_1^{(1)}, \ldots, t_r^{(1)}) \quad \ldots \quad A(t_1^{(m)}, \ldots, t_r^{(m)}, f_1(t_1^{(m)}, \ldots, t_r^{(m)}), \ldots, f_s(t_1^{(m)}, \ldots, t_r^{(m)}))$$

where the terms $t_j^{(i)}$ do not contain the $\varepsilon$-symbol and the fi'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 $\varepsilon$-symbol can be formulated and opens the way to an Herbrand-type consistency proof.

*2.2. Herbrand's theorem*

The elimination theory can be seen as a forerunner to Herbrand's consistency theorem for the predicate calculus. We give a brief treatment of Herbrand's formulation. Let A be a formula in prenex form, for instance

$$A \equiv \; x \;\; y \;\; z \;\; t \, B(x, y, z, t)$$

with B quantifier-free. Introduce two new function letters with f unary and g binary with terms $U_1 \ldots U_n$, $W_1 \ldots W_n$, then A is provable in predicate calculus in the form

$$A \equiv B(U_1, f(U_1), W_1, g(U_1, W_1,)) \quad \ldots \quad B(U_n, f(U_n), W_n, g(U_n, W_n)).$$

This disjunction, as the former one, is derivable in propositional calculus and may be used as a criterion of refutability in a *negative* interpretation (see Hilbert-Bernays, [8], II, p. 170 ff).

The negation of A is

$$\neg A \equiv \quad x \quad y \quad z \quad t \; \neg B(x, y, z, t)$$

or

$$\neg A \equiv \neg B(x, f(x), z, g(x, z))$$

and while Herbrand tought of propositional formulas as refutable in an infinite or indefinite recursive domain <*champ infini*>, Kreisel has introduced the no counterexample interpretation as a functional interpretation of higher type: the type recursive functionals are simply defined by

$$B_{x_1 \ldots x_n} [F_1(f_1, ..., f_n), ...) \; F_m(f_1, ..., f_n)]$$

with B open. For a true formula A, we have

$$B[F(f, g), f(F(f, g)), G(f, g), g(F(f, g), G(f, g))]$$

where the F's and the G's are obviously our new type recursive functionals.

This last formula A is true if there is no counterexample of the form

$$\neg B \; [x, f(x), z, g(x, z)]$$

with f and g being arguments of the higher-type recursive functionals F and G; F and G are continuous and may thus be linked with polynomials of arbitrary degree; we can define composition of F and G as

$$F \cdot G = (\sum_i F_i x^i) \, (\sum_j G_j x^j) = \sum_i \sum_j (F_i G_j x^{i+j}).$$

Since we cannot quantify over all such functionals — by diagonalisation there is a recursive functional wich is distinct from all recursive functionals — we must restrict ourselves to polynomials of finite degree and use descent on degrees and heights of polynomials to recover a finitist version.

Let us remark that primitive recursive functions can be easily translated as polynomial functions. It is obvious for initial *constant* functions; composition and recursion are treated as the convolution product of functions $G \cdot H$ for G and H such as

$$F(x)\vec{n} = G_n \, (H_1(a_n), ..., H_p(a_n))$$

with $H \cdot G = \sum_i \sum_j (G_i H_j x^{i+j})$.

The μ-operator as the equivalent of the least number principle is replaced by infinite (finite) descent on decreasing powers of a polynomial of finite degree

$$F(x) \, \vec{n} = f_0 x^n + f_1 x^{n-1} + ... + f_{n-1} x + f_n.$$

Along with Hilbert's idea of a terminating sequence of predecessors for a given n, Fermatian descent allows for a finite reduction process in the guise of a decreasing linear order of powers of a given polynomial.

*2.3. Quantifier elimination*

An other line of attack in Hilbert's metamathematical programme was pursued by Tarski and gave birth to model theory (see [11], p. 66). Elimination of quantifiers led Tarsky to the positive solution of the decision problem for elementary algebra and geometry [18]. The end result of which is a disjunctive normal form (disjunction of conjunctions of atomic formulas), a close relative to the Hilbert-Ackermann theorem for open theories, that is theories whose non-logical axioms are formulas without quantifiers. Obviously, here is a meeting ground for proof theory and model theory — which evolved quite independently afterwards under the auspices of the compactness theorem. But to arrive at the syntactic result, Tarski followed a route quite similar to Hilbert's elimination theory. The point of departure is a system of polynomials (see [18], p. 31)

$$\alpha \equiv \alpha_0 + \alpha_1\xi + \ldots + \alpha_m\xi^m$$

$$\beta \equiv \beta_0 + \beta_1\xi + \ldots + \beta_n\xi^n$$

$$\gamma_1 \equiv \gamma_{1,0} + \gamma_{1,1}\xi + \ldots + \gamma_{1,n_1}\xi^{n_1}$$

$$\vdots$$

$$\gamma_r \equiv \gamma_{r,0} + \gamma_{r,1}\xi + \ldots + \gamma_{r,n_r}\xi^{n_r}$$

over which a function T is defined for formulas $\Phi$ of the form

$$(\underset{k}{E}\,\xi)\,[a = 0]$$

where $\underset{k}{E}\,\xi$ means "there exist exactly k values of $\xi$" such that $T(\Phi)$ is an equivalent quantifier-free formula. The elimination procedure relies essentially on Sturm's theorem on the number of real roots of a polynomial between two arbitrary values $f_0(x)$ and $f_1(x)$ of the variable and reduces to an Euclidiean algorithm for finding the greatest common divisor of $f_0(x)$ and $f_1(x)$ in the counting of variations of sign in the given polynomial (equation or inequality). Although Tarski mentions Kronecker and despite van den Dries' suggestion that elimination theory has evolved in the wake of Kronecker [19], Tarski does not draw directly from Kronecker's theory of forms (polynomials). Kronecker's general arithmetic of "algebraic quantities" is a theory of content of polynomials, but Tarski will use a notion of content only in his theory

of implication and logical consequence. In that context, Sturm's theorem appears as a special case of Kronecker's divisor theory. I shall outline in the next section a treatment of polynomials in the more general setting of Kronecker together with Fermat's infinite descent, which is in fact a generalization of Euclid's algorithm. If Tarski concludes ([18], p. 53) that the decision method amounts to a proof of consistency and completeness (for real closed fields, for example), my aim is self-consistency of arithmetic and I review now Gödel's idea of an internal consistency proof as an extension of the finitist point of view.

*2.4. Gödel's construction*

Gödel [5] introduced functionals (recursive functions of higher types) over all finite types as abstract objects beyond the (concrete) natural numbers. The *Dialectica* interpretation has been extended by Spector, Howard and Kreisel and others in the intuitionistic spirit of bar-induction and bar-recursion of finite type. Although Gödel was animated by intuitionistic motives, his proof for Heyting arithmetic can be translated for Peano arithmetic where its constructive content can be carried over. I propose a different approach to the consistency problem. Arithmetic here is not Peano arithmetic, but Fermat (or Fermat-Kronecker) arithmetic with Fermat's infinite descent replacing Peano's induction and we have Kronecker's indeterminates instead of functional variables. The "general arithmetic" of polynomials (or forms, in Kronecker's terminology) is built upon "effinite" (infinitely proceeding, in Brouwerian terminology) sequences. Finite sequences are sets and the Cauchy (convolution) product for polynomials is used as a mapping from sequences to sequences in **N** while the degree of a polynomial replaces the type of a formula, the motive here being a formulas-as-polynomials interpretation.

Gödel states in a phrase reminiscent of Gentzen that the notion of accessibility <*Erreichbarkeit*> is an abstract concept which requires a kind of reflection on finite constructions. Such a notion is the notion of a computable functional of finite type over the integers, which Gödel substitutes for the abstract notions of assertion and proof in intuitionistic mathematics. Formulas like

$$F' = \quad x \quad y \; A[x, y, z]$$

and

$$G' = \quad w \quad v \; B[v, w, u]$$

will be used to obtain a consistent interpretation of Heyting's arithmetic: for example, we have

$$(F \quad G)' = \quad y, w \quad VZ\,[A(y, Z(y, w), x) \quad B(V(y), w, u)]$$

and

$$(\neg F)' = \quad y \quad \overline{\phantom{x}},Z \;\neg A(y, \overline{\phantom{x}},Z(y)\,, x)$$

where x, y, v and w are finite sequences of variables of arbitrary type, u is a sequence of number variables while Y, V, Z and $\overline{\phantom{x}},Z$ are second-order variables — A and B are quantifier-free. Those generalized formulas constitute the functional interpretation. Gödel defines the finite types inductively with the following three clauses:

1. 0 is a finite type (the type of integers);
2. if s and t are finite types, then $s \times t$ (their Cartesian product) is a finite type;
3. if s and t are finite types, then $s \rightarrow t$ is also a finite type.

*Remark*. The third clause means that there is a mapping from functionals of type s to functionals of type t.

The last transformation raises questions of interpretation and the literature on the subject is abundant, but I observe only that I translate this mapping as a convolution product for polynomials. By the Curry-Howard isomorphism we can identify types and formulas, in particular a product of types is identified to a conjunction of formulas. I extend the isomorphism by having implication identified to a power representation. Formulas can be rendered in the following manner:

$$x \; Ax \qquad y \; By = \sum_0^n (\Sigma\, {}^{-},a_0 x + \Sigma\, {}^{-},b_0 x)^n$$

and

$$x \; Ax \qquad y \; By = \prod_0^n (\Pi\, {}^{-},a_0 x + \Pi\, {}^{-},b_0 x)^n$$

where ${}^{-},a_0$ stands for $1 - a_0$ with integral coefficients a and b and indeterminate x. But here we have an isomorphism between formulas and polynomials which seems more natural in view of the fact that a constructive or intuitionistic type theory (*à la* Martin-Löf) built upon the isomorphism does entertain arbitrary objects (or sets) in a typified language whose logic is imported and not internally motivated. Combinatory logic is of no help in that context, since it fulfils only an abstract goal which seems superfluous in arithmetic.

Such a rendering of formulas is in line with Hilbert's arithmetization programme as we shall presently see.

*2.5. Arithmetization*

Hilbert had introduced the notion of a "disparate system of functions" in [8] 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

$$\phi_1, \ldots, \phi_s,$$

the disjunction $S_p^{(\phi)}$ is derivable in the propositional calculus. A disparate function system is, for example (see [8], II, p. 175)

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

where the $\psi_i$ 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 ([8], 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 diagonalisation procedure in contrast to Cauchy's diagonalisation (the convolution product) which we can apply to Fermat-Kronecker arithmetic (see [4]).

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 ([8], 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 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 [15].

**3. Self-consistency**

Robinson's theory of arithmetic Q is consistent and essentially undecidable. But E. Nelson's proof for the self-consistency of Q in [15] rests on a notion of genetic, as opposed to formal, number which allows for a computable or polynomially bounded exponentiation in the form

$$\sigma_0 (l, n) = f \text{ Exp Comp } (l, n, f)$$

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

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

$$\forall n \neg\phi (n) \quad \text{for } \phi = e^y.$$

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 [15], 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 the 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. 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. Fermat, Euler, Lagrange, Legendre and Kummer all used the method to prove important theorems in number theory. Nowadays, Mordell, Weil and others use it in arithmetic (algebraic) geometry. Legendre, for example proved that

$$ax^2 + by^2 = z^2$$

with natural numbers a, b, neither of which is the perfect exact square of another number. The descent must stop at 1 in the substitution of smaller coefficients and the equation is shown to be solvable by a process of reduction (or decomposition).

*3.1. The formalization of infinite descent*

Fermat's arithmetic is characterised by the method of infinite descent and I maintain that from the metamathematical point of view, that is from the proof-theoretic point of view, infinite descent fulfills the role of induction without requiring the notion of infinite set. It is obvious that Fermat did not have the ω-point of view in mind. Fermat says that he has invented the method of infinite or indefinite descent, but it is already <*in nuce*> in Euclid. Take, for example, proposition 31 of book VII of the *Elements* "Any composite number can be divided by a prime number". The proof uses a decomposition or reduction which cannot go on indefinitely since any descending sequence of natural numbers is finite. Fermat himself has put his method to use in his proof of the impossibility of the Diophantine equation $x^4 + y^4 = z^2$ which is reduced to $x^4 + y^4 = z^4$; this is a particular case of Fermat's last theorem

$$n > 2 \quad x \quad y \quad z\ (x^n + y^n \neq z^n).$$

The principle of infinite descent can be formulated as follows: if the existence of a property for a given n implies the existence of the same property for an arbitrary smaller number, then this property is possessed by still smaller numbers *ad infinitum*, which is impossible since any descending sequence of natural numbers is finite. In order to formalize this principle, we introduce here the quantifier ∓x, the "effinite" quantifier.

In symbols, we have for the rendering of the intuitive notion of an unbounded or unlimited sequence obtained by "positive" descent

$$\mp x\ \{([Ax \quad y\ (y < x)\ Ay] \rightarrow \quad y \quad z\ (z < y)\ Az)$$

$$\rightarrow \quad z\ (z = 0 \quad 1 \quad n)\ Az\} \rightarrow \mp x\ Ax$$

which means that the sequence is continuing on indefinitely, or rather "effinitely", starting from the least number, which may be 0, 1, or n.

This principle of descent does not need a universal quantifier, only an "effinite" quantifier for finite or rather indefinite descent; effinite means potentially infinite, indefinite sequences or Brouwer's "infinitely proceeding sequences". To such effinite sequences, one could assign an "unlimited" natural number, as in Nelson [15], while finite natural numbers are assigned to finite initial segments (sets) of those sequences.

Since infinite descent is impossible — any descending sequence of positive integers must stop at 0, the prepositional bound of the sequence of natural numbers — we have the following "negative" version

$$\exists\!\!\!-\, x \{[Ax \quad y\,(y < x)\, Ay] \rightarrow \quad y \exists\!\!\!-\, z\,(z < y)\, Az\} \rightarrow \exists\!\!\!-\, x \neg Ax$$

which means that the property (or set of properties) postulated for the infinite descent is false for all natural numbers "effinitely" — with $\exists\!\!\!-\, z\, Az$ instead of $\quad z\, Az$ in the antecedent (for a more detailed treatment, see [4] and [5]).

*3.2. The polynomial translation*

There are various ways to translate a formal system into the natural numbers, simple substitution of numerical variables as in Ackermann [1], translation of logical into arithmetical operations as in Goodstein's equational calculus [14]. In view of our use of Kronecker's results, we choose the polynomial translation.

We are going to need some facts about the ring of polynomials in one indeterminate in our consistency proof. We pass briefly over the preliminaries (the graded ring of two or more polynomials has the same convolution product, which is our main tool).

Polynomials of the form

$$f = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n$$

where the $f_i$ are the coefficients with the indeterminate x build up the subring K[x] of the ring K[[x]] of formal power series. The degree of a polynomial is the degree of the last non-zero coefficient (k = n), while the leading coefficient of a polynomial f of degree k is the constant $f_k$ and f is called monic if its leading coefficient is 1. Thus polynomials are power series having only a finite number of non-zero coefficients. The involution or Cauchy product of two polynomials will play an important role in our translation; we write it

$$f \quad g = (\Sigma_m f_m x^m)\,(\Sigma_n g_n x^n) = \Sigma_m \Sigma_n f_m g_n x^{m+n}.$$

The sum f + g of polynomials f and g is obtained by simply adding corresponding coefficients. Homogeneous polynomials have all their non-

zero terms of the same degree and they can be put in the following convenient form

$$a_0 x^m + a_1 x^{m-1} y + ... + a_m y^m.$$

We are interested in irreducible (= prime in K[x]) polynomials. Every linear polynomial is irreducible. K[x] has the property of unique factorization and this fact will be crucial in the following.

I am going to make an essential use of Kronecker's notion of the content of forms in ([14], p. 343). A form M is contained in another form M' when the coefficients of the first are convoluted (combined in a Cauchy product) in the coefficients of the second. This idea of a content <*Enthalten-Sein*> of forms can be summarized in the phrase "The content of the product is the product of the contents (of each form)" which can be extracted from Kronecker's paper [14]. This is in fact a version of Gauss' lemma, which says that for polynomials f and g with integer coefficients, the content of fg is the content of f times the content of g. Thus, for a form to be contained or included in another form is simply to be linearly combined with it (to have its powers convoluted with the powers of the second form).

We can adopt here a general principle of substitution — elimination formulated by Kronecker. We state the *Substitution Principle*:

1) *Two homogeneous forms (polynomials) F and $F^o$ are equivalent if they have the same coefficients (i.e. content);*

2) *Forms can be substituted for indeterminates (variables) provided the (linear) substitution is performed with integer coefficients*.

We have immediately the following **Proposition 1** (proposition X in Kronecker):

> *Linear homogeneous forms that are equivalent can be transformed into one another through substitution with integer coefficients.*

We have also the following **Proposition 2** (proposition $X^o$ in Kronecker):

> *Two polynomials F and $F^o$ are equivalent, if they can be transformed into one another*.

These propositions can be considered as lemmas for the unique factorization theorem for forms which Kronecker considered as one of his main results. The substitution procedure is simultaneously an elimination

procedure, since indeterminates (<*Unbestimmte*>) are replaced by integer coefficients. Thus an indefinite (or effinite) supply of variables can be made available to a formal system and then reduced by the substitution - elimination method to an infinitely descending or finite sequence of natural numbers, as will be shown in the following.

The substitution process takes place inside arithmetic, from within the Galois field F*, i.e. the minimal, natural or ground field of polynomials which is the proper arena of the translation and indeterminates — Kronecker credits Gauss for the introduction of <*indeterminatae*> — are the appropriate tools for the mapping of formulas into the natural numbers. The important idea is that indeterminates in Kronecker's sense can be freely adjoined and discharged and although Kronecker did not always suppose that his forms were homogeneous, we restrict ourselves to homogeneous polynomials.

*Definition*. The height of a polynomial is the maximum of its lengths (number of its components or terms) — the height of a polynomial is indicated by a lower index.

We state eight clauses for the polynomial translation with a *valuation map* $\hat{\phi}$.

*Clause 1*. An atomic formula A can be polynomially translated as

$$\hat{\phi}\ (A)\ [n] = (a_0\ x)$$

(where the $a_0$ part is called the determinate and the x part the indeterminate and $\hat{\phi}$ is the polynomial valuation function or map). Here the coefficient $a_0$ corresponds to a given natural number (the "valuator") and 0 indicates that it is the first member of a sequence, x being its associate indeterminate. The polynomial $(a_0x)$ is thus a combination of the two polynomials (1, 0, 0, 0...) and (0, 1, 0, 0...). We identify polynomials by their first coefficients.

*Clause 2*. The negation of an atomic formula, that is ¬A, is translated as

$$\hat{\phi}\ (\neg\ A)\ [n] = (1 - a_0x).$$

*Clause 3*. The conjunction A and B is translated as $\hat{\phi}$ (A B) [n × m] = $(a_0x)$ $(b_0x)$ for the product of monomials $(a_0x)$ and $(b_0x)$.

*Clause 4*. The disjunction A or B is rendered by $\hat{\phi}$ (A B) [n + m] = $(a_0x + b_0x)$.

*Clause 5*. Local implication A → B is rendered by $\hat{\phi}$ (A → B) [$m^n$] = $(\bar{a}_0x + b_0x)^n$ for $\bar{a}_0x = 1 - a_0x$.

*Remarks.* How is implication to be interpreted polynomially? A developed product of polynomials has the form

$$a \quad b = (\Sigma_i a_i x^i)( (\Sigma_j b_j x^j) = \Sigma_i \Sigma_j a_i b_j x^{i+j}.$$

For $a^b$ we could simply write $(a + b)^n$ for the binomial coefficients and put

$$(a_0x + b_0x)^n = a_0{}^n x + n\, a^{n-1}\, x\, bx + [n\,(n-1)/2!]\, a_2{}^{n-2}x^2\, b_2x^2 + ... + b_0{}^n x^n$$

in short

$$(a_0x + b_0x)_{i\langle n}^{\ n} = \Sigma_{i+j=n}\, a_i b_j x^n.$$

The rationale for our translation is that we want to express the notion of inclusion of a in b by intertwining or combining their coefficients in a "crossed" product, the sum of which is $2^n$, which is also the sum of combinations of n different objects taken r at a time

$$\Sigma_{r=0}^{\ n}\ C_n^r.$$

Linear combination of coefficients is of course of central importance in Kronecker's view and one of his fundamental results is stated: "Any integral function of a variable can be represented as a product of linear factors". Kronecker refers to Gauss' concept of congruence and shows that a modular system with infinite (indeterminate) elements can be reduced to a system with finite elements (for all this, see [3]). This is clearly the origin of Hilbert's basis theorem on the finite number of forms in any system of forms with

$$F = A_1 F_1 + A_2 F_2 + ... + A_m F_m$$

for definite forms $F_1$, $F_2$, ..., $F_m$ of the system and arbitrary forms $A_1$, $A_2$, ..., $A_m$ with variables (indeterminates) belonging to a given field or domain of rationality (‹*Rationalitätsbereich*›). The fact that exponentiation is not commutative is indicated by the inclusion a b. The combinatorial nature of implication is made more explicit in polynomial expansion and is strengthened by the symplectic (interlacing) features of local inclusion of content. We may also define implication, in analogy with the relative complement, as

$$(1^N - a_0x) + b_0x$$

where $1^N$ is the arithmetic universe polynomially expanded up to n.

*Clause* 6) $\hat{\phi}$ ( x Ax) [n + m + $\ell$ ...] = $\sum_{0...}$ $(a_0x + b_0x + c_0x...)i<n$ where $\sum$ is an iterated sum of numerical instances with $a_0$ as the first member of the sequence.

*Clause* 7) $\hat{\phi}$ ( x Ax ) [n × m × $\ell$ ] = $\Pi_0(a_0xb_0xc_0x)i<n$ .

*Clause* 8) $\hat{\phi}$ ($\exists$x Ax) [n × m × $\ell$ ...] = $\Pi_{0...}$ $(a_0xb_0xc_0x...)n$ .

*Remarks.* The effinite quantifier calls for some clarification. While the classical universal quantifier stands here for finite sets only, the effinite quantifier is meant to apply to infinitely proceeding sequences or effinite sequences. These are not sets and do not have a postpositional bound; we put an n to such sequences and a $2^n$ to sequences of such sequences

$$0, 1, 2, ..., n, ..., 2^n$$

with the understanding that n signifies an arbitrary bound. It should be pointed out that Boole in his *Mathematical Analysis of Logic* (1847) had also a universe (of classes) denoted by 1; negation was interpreted as 1 - x. The fact that the ring K[x] of polynomials enjoys the unique factorization property exhibited by infinite descent coupled with the proof by infinite descent of the infinity of primes makes essential use, from our point of view, of the effinite quantifier.
We then have a combinatorial formulation

$$\Pi_0^n (a_0xb_0xc_0x \quad n_nx^n)$$

for the effinite quantifier; since n! = $\Pi_{c \leq n}$ c, the combinations of n. I call this scheme the absolute or standard scale. Any other scale is an associate scale (of indeterminates) and it is reducible by substitution to the standard scale.
As a foundational precept, there is no $\omega$. Any transnatural or transarithmetic (transfinite, in Cantorian terminology) ordinal scale, e.g. up to $\varepsilon_0$, is an associate scale and is by definition reducible. It is clear, from a Kroneckerian point of view, that Cantor's transfinite arithmetic becomes a dispensable associate (with an indeterminate pay-off!). The arithmetic universe N is naturally bounded by $2^n$ and not by $2^{\aleph_0}$ for infinite power series.

## 4. Conclusion

A proof of the internal consistency of arithmetic (Fermat-Kronecker arithmetic or FKA) proceeds along the following lines: the

radical translation of logic into polynomial arithmetic, the embedding of arithmetic itself in polynomials — with indeterminates playing the rôle of variables — in which the degree (and the height) of a polynomial replace the type of a given formula (or sentence) in the arithmetic universe; infinite descent orders polynomials according to their decreasing order until one reaches linear (irreductible) polynomials. Cauchy's diagonal or the convolution product does not lead outside the domain (of rationality) of polynomials and the combinatorial nature of logic is preserved in the closure of algebraic extensions [5]. The elimination of logic in the process is inherited from Kronecker's elimination theory and stands in close analogy to the elimination of quantifiers in model theory. A model-theoretic question like the one found in Hodges ([12], p. 22) finds here an immediate answer. Hodges asks what could Kronecker mean by the arithmetical existence of algebraic numbers. It is not enough to say that we have a canonical model for Kronecker's construction, as Hodges reckons. H. Weyl in his classic *Algebraic Theory of Numbers* [20] has the right answer when he emphasizes the algorithmic character of Kronecker's divisor theory against Dedekind's non-constructive ideal theory. Unique factorization for polynomials is gained through the (constructive) descending chain condition, not with the help of abstract existence assumptions. But elimination of logic is more in accordance with the proof-theoretic (metamathematical) programme that Hilbert conceived for the consistency problem. Syntax dominates over semantics in that context. The programme could not be fufilled for set-theoretic Peano arithmetic as Gödel has shown, but the possibility of such a programme was left open by Gödel himself for an arithmetic without the induction postulate. Infinite or indefinite descent, in Fermat's words, does indeed achieve consistency for indefinite (or effinite) quantification over the unlimited sequence of natural numbers. Primitive recursive arithmetic has direct polynomialization without the disadvantage of general recursiveness — the $\mu$-operator is taken care by infinite descent or the decreasing order of polynomial exponents. Matijasevi ,c 's theorem has obviously no hold on the polynomial translation since recursive enumerability of polynomial orders stops short of infinite quantification (over the set of positive integers).

Finally, arithmetical or polynomial logic bypasses types, sets and classes in its unique recourse to the algebra (generalized arithmetic) of polynomials as generalized integers. After all, Cantor's normal form is but a polynomial expression with the ordinal polynomial

$$\zeta = \gamma_0\beta^{\alpha_n} + \gamma_1\beta^{\alpha_{n-1}} + \ldots + \gamma_{n-1}\beta^{\alpha} + \gamma_n,$$

a finite series of infinite powers. But then one needs transfinite induction for the descent in order to have an "external" consistency proof for arithmetic in the style of Gentzen and Ackermann. What I have tried to show is that such a transfinite descent can be escaped by the internal consistency proof for polynomials of finite order with finite descent. Hilbert was the first to associate finite integers and transfinite ordinals (of Cantor's second number class) in his attempt to solve the continuum hypothesis (see [II]). His idea was to have functions of natural numbers correspond to transfinite ordinals in the omega hierarchy < $\varepsilon_0$. Gödel, after Gentzen, will use the idea to prove the relative consistency of the continuum hypothesis in Z-F, but Gödel admitted that he had adopted a transcendental (external) attitude to obtain his result. It is somehow ironic that while Hilbert hoped for a finitist solution for the first two problems of his famous list, his inspiration led logicians away from his metamathematical programme of finitary (constructive) proofs. The proof in [4] is an attempt at recovering that initial spirit in terms of an internal logic of arithmetic.

Université de Montréal, gauthiyv@philo.umontreal.ca

## REFERENCES

[1] Ackermann, W., "Zur Widerspruchsfreiheit der reinen Zahlentheorie", *Math. Ann*, 117, 1940, pp. 162-194.
[2] Church, A., "An unsolvable problem of elementary number theory", *Am. J. Math.*, 58, 1936, pp. 345-363.
[3] Gauthier, Y., "Hilbert and the Internal Logic of Mathematics", *Synthese* , 101, 1994, pp. 1-14.
[4] Gauthier, Y., "The Internal Consistency of Arithmetic with Infinite Descent", *Modern Logic*, vol. 8, Nos 1-2, 2000, pp. 47-86.
[5] Gödel, K., "Über eine noch nicht benütze Erweiterung des finiten Standpunktes", *Dialectica*, 12, 1958, pp. 230-287. See also Gödel, K., *Collected Works*, vol. II, Oxford University Press, Oxford, 1990, pp. 271 ff.
[6] Gödel, K., "Über formal unentscheidbare Sätze der *Principia Mathematica* und verwandter System I", *Monatsh. für Math. v. Physik*, 38, 1931, pp. 173-198.
[7] Gödel, K., "On formally undecidable propositions of *Principia Mathematica* and related systems I", in *From Frege to Gödel*, ed.

Jean van Heijenoort, Harvard University Press, Cambridge, Mass., 1967, pp. 616-617.
[8] Hilbert, D., Bernays, P., *Grundlagen der Mathematik I et II*, 2 Aufl., Springer-Verlag, Berlin, 1968 and 1970.
[9] Hilbert, D., Ackermann, W., *Grundzüge der theoretischen Logik*, Springer-Verlag, Berlin, 1928.
[10] Hilbert, D., "Neubegründung der Mathematik" and "Die logischen Grundlagen der Mathematik", in *Gesammelte Abhandlungen*, Spinger-Verlag, Berlin, 1935, vol. 3, pp. 157-177 and pp. 178-191.
[11] Hilbert, D., "Über das Unendliche", *Math. Ann*., 95, 1926, pp. 161-190.
[12] Hodges, W., *Model Theory*, Cambridge University Press, Cambridge, 1993.
[13] Kleene, S. C., "General Recursive Functions of Natural Numbers", *Math. Ann.*, 112, 1936, pp. 727-742.
[14] Kronecker, L., "Grundzüge einer arithmetischen Theorie der algebraischen Grössen", in *Werke*, ed. by K. Hensel, 5 vols., Chelsea, New York, vol. III, pp. 245-387.
[15] Nelson, E., *Predicative Arithmetic*, Mathematical Notes 32, Princeton University Press, Princeton, N.J., 1986.
[16] Rosser, J. B., "Extensions of some theorems of Gödel and Church", *JSL*, 1, 1936, pp. 87-91.
[17] Tarski, A., "Einige Betrachtungen über die Begriffe der ω-Widerspruchsfreiheit und der ω-Vollständigkeit", *Monatsh. für Math. v. Physik*, 40, 1933, pp. 97-112.
[18] Tarski, A., *A decision method for elementary algebra and geometry*, 2nd rev. ed., University of California Press, Berkeley and Los Angeles, 1951.
[19] Van den Dries, L., "Alfred Tarski's Elimination Theory for Real Closed Fields", *JSL*, 53, 1988, pp. 7-19.
[20] Weyl, H., *Algebraic Theory of Numbers*, Princeton University Press, Princeton, N.J., 1940.