South American Journal of Logic
Vol. 5, n. 1, pp. 1–19, 2019
ISSN: 2446-6719

Numerical Existence Property and Numerical Content: Intuitionistic Logic versus Arithmetical Logic

Yvon Gauthier

Abstract

I examine claims of numerical existence for the intuitionistic disjunction and existential quantifier. I argue that those claims do not secure numerical content and that a polynomial translation of logical constants comes closer to a numerical language for mathematics in the framework of a "contentual" or internal logic of arithmetic.

Keywords: Intuitionistic disjunction and existential quantifier, numerical existence, numerical content, Kronecker's general arithmetic, modular polynomial logic.

Introduction

Intuitionistic logic and intuitionistic number theory have the disjunction property and the numerical existence property. The question is to what extent these properties imply a notion of numerical content. The objective of this paper is to evaluate the claims about the realizability conditions of numerical existence and offer an alternative to intuitionistic logic and number theory in terms of a modular polynomial logic exhibiting a direct translation of logical formulas into an arithmetical logic internal to classical arithmetic. The term classical arithmetic is meant here to be contrasted to the set-theoretical Dedekind-Peano arithmetic formalized as Peano Arithmetic (PA). Classical arithmetic is designated as Fermat-Kronecker (F-K) arithmetic for classical number theory from Fermat to Gauss, and Kummer and Kronecker and beyond (see Gauthier [5]).

1 The disjunction and numerical existence properties.

The disjunction and numerical existence properties are easy to formulate. For a disjunction $A \vee B$ intuitionistic logic requires that one of the disjuncts be true or provable and for an existential quantifier $\exists x Ax$, it requires to exhibit a term t free for x in $A[x/t]$ denoting an instantiating element or object not otherwise specified in the BHK (Brouwer-Heyting-Kolmogorov) interpretation of intuitionistic logic. S.C. Kleene ([11], [12]) had the idea of calling such an object a *realizer*, an arbitrary witness or numerical instance in a given coding system. Kleene's realizability interpretation of intuitionistic logic adjoins a number n to a *realizer* such that the disjunction $A \vee B$ needs a pair (n, m) with values in $0, 1$ (for $0 = F$ and $1 = T$) with the proviso that if $n = 0$, then m realizes A and if $n = 1$, then m realizes B); for the existential quantifier, $\exists x Ax$ is realized by a pair (n, m), iff m is a *realizer* for $A(n)$.

The general setting of Kleene's realizability is the theory of partial recursive functions with recursive enumerability for which a partial recursive function is recursively realizable , iff some natural number n realizes it. This amounts to recursive enumerability for realized formulas in intuitionistic logic. For example, $\exists x Ax$ is proven, iff there is proof of Ax for some numeral x as in Gödel numbering. G. Kreisel has introduced a modified realizability interpretation, a typed variant with continuous functionals with the specific aim of reintroducing the notion of proof for a realized formula. H. Friedman ([3]) has shown in line with Kleene's work that realizability conditions allow to derive the numerical existence property in the set of axioms of a recursively enumerable extension T of Peano arithmetic where for the intuitionistic disjunction $A \vee B$, either A is a consequence of T or B is a consequence of T; for the existential quantifier, the numerical existence property stipulates that for each closed consequence $\exists x(Con(x))$ of T where x is a numerical variable, there is natural number n such that $Con(\tilde{n})$ is a consequence of T. All this is done within Peano arithmetic (extensions and fragments or substructures included) with the usual resources of recursive enumerability and set-theoretic machinery. However the realizability notion is not expressible in intuitionistic arithmetic HA^{ω} since it involves all recursive (partial) functions or functionals (of finite type). The situation is similar to the first number class in Cantorian set-theory for the sequence of natural numbers where the final segment $(0, \omega)$ is not expressible as an isomorphism type for its order type is incomparable or irreducible to any n in the ordinal polynomial of Cantor's normal form (see Gauthier [7]). All this means that the numerical existence property is not enough to produce numerical content, simply because logic is not arithmetic and that general computable functions do not generate feasible arithmetic or polynomial arithmetic

the results of which can be computed in polynomial time. Here one should add that numerical witnesses are not arbitrary in a polynomial modular setting, since they are enumerated by a finite segment of an unlimited sequence of natural numbers in **N**, of integers in **Z** or in finite fields **Q** as André Weil has taught us. As it is the case for modular arithmetic, Euclid's algorithm can act on modular logic for the elimination of logical constants and Fermat's infinite descent can be used to eliminate quantifiers in the translation of logic into arithmetic – e.g. by a calculus on binomial coefficients corresponding to a logical formula in propositional logic and decidable first-order monadic logic – . See Gauthier (5) and (6).

2 The notion of numerical content.

E. Bishop ([1]) has advocated the idea of mathematics as a numerical language. Here the author of the classic *Foundations of Constructive Analysis* deplores the fact that intuitionistic logic and mathematics are not constructive enough and a strict numerical interpretation of implication is needed simply because the usual

$$A \to B$$

amounts simply to the data of a proof of $A \to B$ effected by a construction which outputs a proof of A into a proof of B plus a proof of the said transformation wanting of any constructive information. It seems that Bishop was aiming at an existential instantiation for implication, but has been unable to provide with the right formulation and resorted finally to an appeal to Kronecker whom he considered closer to his foundational standpoint than was Brouwer. The proof-theorist U. Kohlenbach ([13]) claims that Gödel's functional interpretation of intuitionistic logic in Gödel ([8]) comes close to numerical content by the employment of primitive recursive functionals of finite type. Kohlenbach acknowledges though that the notion was already present in Hilbert's paper (Hilbert [10]), but he doesn't go back to Kronecker. I have shown that Hilbert was certainly inspired by Kronecker's own construction in (Kronecker [14]) and I have given the details of such a construction in (Gauthier [5], chap. 4).

3 Local negation.

Negation is interpreted "negatively" in intuitionistic logic as Bishop would say:

$$\neg A \equiv A \to 0 = 1(\text{absurdity})$$

and here he would lament the lack of numerical content. Gödel's interpretation in (Gödel [8]) comes to the same when he writes

$$\neg\, p \equiv\ p \supset 0 \cdot 1.$$

The *Dialectica* interpretation can have a direct polynomial interpretation (see Gauthier [5], chap. 7.9) and negation could be defined as 1- a on the pattern of relative complementation

$$a \to b = In\ ((X - a) \cup b)$$

for a topological space X, its Interior of open sets and b. Now, one can translate this in a combinatorial formula

$$a \to b = C\ ((2^n - a) + b)$$

where C stands for combinations of integer coefficients a, b of the polynomial $(a_0x + b_0x)^n$ with a_0x standing for $2^n - a$ (2^n is here the finite arithmetical universe as the power set of n integers). See below section 5 for more details on this construction.

The minus sign also appears in Y. Gurevich's treatment (Gurevich [9]) of Nelson's constructible falsity (Nelson [15]) which is expressed in terms of Kleene's realizability notion

$$\neg A \supset 1 = 0.$$

For Gurevich's minus sign, one has

$$— (A \supset B) \equiv A \wedge -B$$

$$— \neg(A) \equiv A$$

$$— A \supset \neg A$$

and a deduction theorem stating

$$— A \supset A \supset B.$$

Local negation in (Gauthier [4]) could be seen as a still stronger notion, the minus sign in a congruence relation being arithmetical while Gurevich's strong negation is logical and set in a Kripke model for Nelson's notion of constructible falsity couched in Kleene's recursive realizability style. There again numerical content is only postulated under an apriori numerical existence property. I present in the following a scheme inspired by Kronecker's theory of forms, his divisor theory for homogeneous polynomials. Such a scheme is intended to procure a direct access to numerical content in an arithmetical (modular polynomial) logic as the internal logic of arithmetic.

4 Modular polynomial logic.

For the Kroneckerian background of modular polynomial, I summarize the polynomial translation of logical constants inspired by Kronecker's general arithmetic (*allgemeine Arithmetik*). See Kronecker (15) and Gauthier (6).

There are various ways to translate a formal system into the natural numbers, simple substitution of numerical variables as in Ackermann (1940), translation of logical into arithmetical operations as in Goodstein's equational calculus (1951). 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- a Grassmannian product could be used to the same effect).

Polynomials of the form

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

where the $f.$ 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

$$f \cdot g = \Big(\sum_m f_m x^m \Big) \Big(\sum_n g_n x^n \Big) = \Big(\sum_m \sum_n f_m g_n x^{m+n} \Big).$$

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

$$a_o x^m + a_1 x^{m-1} y + \ldots + a_m y.$$

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 our future developments[1].

[1]Kronecker had proven the unique factorization theorem in the following formulation: ≪ Every integral algebraic form(= polynomial) is representable as a product of irreducible (prime) forms in a unique way≫(see Kronecker 1882, p. 352). Kronecker is interested in the theory of divisibility for forms and considers primitive forms (forms with no common divisor greater than 1), rather than prime polynomials in his work. The notions of integral domain and unique factorization domain are direct descendants to that theorem.

4.1 The inner arithmetical model

When we write, for example,

$$\varphi_m(\exists x Ax)[n+m+\ell\ldots] = 1, \textit{iff} \sum A_n \in D_m$$

we can drop the right part and write

$$\varphi_m(\exists x Ax)[n+m+\ell\ldots] =< n+m+\ell\ldots >= 1$$

to mean that we have a complementary mapping (of the intuitionistic spread) $\xi : \mathbf{N} \to \mathbf{N}$, so that we really have a polynomial function which evaluates polynomials by sequences of natural numbers after having defined an evaluation map of formulas into polynomials. The whole process is made possible by substitution alone. Moreover, in category-theoretic language, the indeterminate x is a universal element for the functor $U(\varphi(x)) = n$ for an integer n. If we look at variables of logical formulas as indeterminates, then any number of variables may be reduced to one.

We are going to make an essential use of Kronecker's notion of the content of forms in (1882, 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 (1968, ll, 419-424). 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 (1882). We state the *Substitution Principle*:

> 1) Two homogeneous forms (polynomials) F and F' 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[2].

[2]This can be seen as the precursor of the problem of quantification over empty domains. We know that we have MP

$$\frac{A, A \supset B}{B}$$

in an empty domain, provided that A and B have the same free variables. But Kronecker had a more general theory of inclusion or content of forms in mind and the transformation in question is a composition of contents, an internal constitution of polynomials (forms) where indeterminates are not the usual functional variables.

We have also the following Proposition 2 (proposition X^0 in Kronecker):

> Two forms F and F' are absolutely 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 equivalence principle makes it possible to have a direct translation between forms (polynomials) and (logical) formulas.

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. Let us rewrite the eight clauses of 2 in the polynomial fashion of the *valuation map* $\hat{\varphi}$.

Clause 1) An atomic formula A can be polynomially translated as

$$\hat{\varphi}(A)[n] = (a_o x)$$

(where the a_0 part is called the determinate and the x part the indeterminate and $\hat{\varphi}$ is the polynomial valuation function or map). Here the coefficient (a_o) 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 $((a_o x))$ 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 $\neg A$, is translated as

$$\hat{\varphi}(\neg A)[n] = (1 - a_0 x)$$

Clause 3) The conjunction A and B is translated as $\hat{\varphi}(A \wedge B)(n \text{ x } m) = (a_0 x)\cdot(b_0 x)$ for the product of monomials $(a_0 x)$ and $(b_0 x)$.

Clause 4) The disjunction A or B is rendered by

$$(A \vee B)(n + m) = (a_0 x + b_0 x).$$

Clause 5) Local implication $A \to B$ is rendered by $\hat{\varphi}(A \to B)(m^n) = (\bar{a}_0 x + b_0 x)^n$ for $\bar{a}_0 x = 1 - a_0 x$.
Remarks : How is implication to be interpreted polynomially? A developed product of polynomials has the form

$$a \cdot b = \Big(\sum_i a_i x^i \Big) \Big(\sum_j b_j x^j \Big) = \Big(\sum_i \sum_j a_i b_j x^{i+j} \Big).$$

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

$$(a_0 x + b_0 x)^n = a_o^x = n a^{n+1} x b x + [n(n-1)/2!] a_2^{n-2} x^2 b_2 x^2 + \ldots + b_0^x x^n$$

in short

$$(a_0 x + b_0 x)_{i<n}^n = \sum_{i+j=n} (i+j) a^i b^j x^n.$$

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

$$\sum_{r=0}^{n} C_r^n.$$

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≫ (1968, II, 209-247). In his (1968, III, 147-208), Kronecker refers to Gauss's concept of congruence and shows that a modular system with infinite (indeterminate) elements can be reduced to a system with finite elements. This is clearly the origin of Hilbert's basis theorem (1965, III, 199-257) on the finite number of forms in any system of forms with

$$F = A_1 F_1 + A_2 F_2 + \ldots + A_m F_m$$

for definite forms $F_1, F_2, \ldots, F_m$ of the system and arbitrary forms $A_1, A_2, \ldots,$ 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 $a \subset b$. 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

$$(1^N - a_0 x) + b_0 x$$

where 1^N is the arithmetic universe polynomially expanded.
Clause 6) $\hat{\varphi}(\exists xAx)[m+n+\ell\ldots] = \sum_0(a_0x + b_0x + c_0x\ldots)_{i<n}$ where $\sum$ is an iterated sum of numerical instances with a_0 as the first member of the sequence.
Clause 7) $\hat{\varphi}(\forall xAx)[n \times m \times \ldots \times \ell] = \prod_0(a_0xb_0xc_0x)_{i<n}$.
Clause 8) $\hat{\varphi}(\exists\!\!\!-xAx)[n+m+\ell\ldots] = \prod_0(a_0x + b_0x + c_0x\ldots)_n$ for the *effinite* quantifier.
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 post-positional bound; we put an n to such sequences and a 2^n to sequences of such sequences

$$0, 1, 2, \ldots, n, \ldots, 2^n$$

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

$$\prod_0^n(a_0xb_0xc_0x\ldots n_nx^n)$$

for the *effinite* quantifier; since $n! = \prod_{c<n} c$, 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 ω. Any transnatural or transarithmetic (transfinite, in Cantorian terminology) ordinal scale, *e.g.* up to ϵ_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!

4.2 The consistency proof

Gentzen's pairing of reduction rules with transfinite inductions in the ϵ_0 segment may be looked at as an associate scale - the scale of ordinal numbers associated with every derivation (see Gentzen, 1969). The theorem of transfinite induction makes all ordinal numbers "accessible" by running through them in an increasing order; the reduction procedure then allows a descent

according to the decreasing order of the ordinal numbers. In the same spirit, Takeuti attempts in (1975) a justification of transfinite induction by invoking the principle : ≪When all numbers smaller than β are recognized as accessible, the β is itself accessible≫. But instead of strictly increasing sequences of ordinals $\beta_o < \beta_1 < \ldots < \beta_{\epsilon_0}$, Takeuti introduces directly strictly decreasing sequences $\mu > \ldots > \mu_1 > \mu_0$ for $\mu = lim(\omega^\mu n)$. As I have shown (see Gauthier, 1991), these ordinals are not uniformly recessible (over an immediate predecessor) and cannot count as ordinals in the absolute scale. On the other side, the associate scale can be reduced by a uniform procedure and can be entirely dispensed with, in accordance with Kronecker's general arithmetic.

Ackermann's consistency proof in (1940) also uses a decreasing sequence of ordinal indices in order to prove his finiteness result for global substitutions <*Gesamtersetzungen*> of fundamental types; his m-sequences are uniformly (immediately) recessible and the reduction procedure ends after a finite number of steps. However, despite the fact that his general recursion procedure is also built in the fashion of infinite descent, Ackermann must refer to the associate (indeterminate) scale of transfinite ordinals which he then reduces one-to-one to finite ordinals. But the transfinite ordinals are not immediately recessible and the upper bound estimate 2^α for indices of m-sequences (Ackermann, 1940, p. 193) has only a relative meaning, since it is not independent of some use of transfinite induction, as Ackermann admits[3]. Transfinite induction means always a detour via an infinite set.

Instead of the ordinal hierarchy of set-theoretic ascendency, I use here the arithmetic of irreducible polynomials to show the internal consistency of infinite descent in a direct way.

4.3 The elimination of logical constants

The connectives of negation, disjunction, conjunction are directly eliminable by translation into the arithmetic interpretation since they can be viewed as difference, sum and product of polynomials in a finite number of terms (constants and indeterminates or variables). We have then

Proposition 5.3.1 Connectives are eliminable through direct translation in the polynomial interpretation.

Proof. Rewrite the logical rules as follows for the sequent calculus with Γ

[3]Gödel's own consistency proof of arithmetic (The *Dialectica* interpretation) (1958) makes use of a general recursion schema (of functionals) over all finite types which is equivalent to complete induction. Herbrand's proof (1931) also requires general recursive functions. It is my contention that the concept of recursion stems from arithmetic reduction (recursion) procedures originating with Dedekind, but mainly from Kronecker's more algorithmic general arithmetic. Recursion is also "récurrence" which in France was another name for infinite descent.

the antecedent and Δ the (single) consequent, both consisting of polynomials (monomials); we write for negation

$$\frac{(\Gamma \cdot a_0 x) \cdot \Delta}{\Gamma \cdot ((1 - a_0 x) + \Delta)} \qquad \frac{\Gamma \cdot (a_0 x + \Delta)}{(\Gamma \cdot ((1 - a_0 x) \cdot \Delta}$$

with Δ empty *i.e.* "without content" in this case, or multiplication by zero and the understanding that the line has the meaning simply of an ordered sequence of sequents (consisting of sequences of formulas themselves). It should be obvious that we have replaced the sign $\vdash$ by the operation $\cdot$ in order to have polynomial uniformization which does not alter the meaning of the rules;
for disjunction :

$$\frac{\Gamma \cdot (a_0 x + \Delta)}{\Gamma \cdot ((a_0 x b_0 x) + \Delta)} \qquad \frac{\Gamma \cdot (b_0 x \cdot \Delta)}{\Gamma \cdot ((a_0 x b_0 x) + \Delta)}$$

and also

$$\frac{(\Gamma \cdot a_0 x) \cdot \Delta \quad (\Gamma \cdot b_0 x) \cdot \Delta}{(\Gamma \cdot (a_0 x + b_0 x)) \cdot \Delta}$$

for conjunction :

$$\frac{(\Gamma \cdot a_0 x) \cdot \Delta}{(\Gamma \cdot (a_0 x + b_0 x)) \cdot \Delta} \qquad \frac{(\Gamma \cdot b_0 x) \cdot \Delta}{(\Gamma \cdot (a_0 x + b_0 x)) \cdot \Delta}$$

and also

$$\frac{\Gamma \cdot (a_0 x + \Delta) \quad \Gamma \cdot (b_0 x + \Delta)}{\Gamma \cdot ((a_0 x + b_0 x) + \Delta)}$$

Remarks: We can treat implication as

$$\frac{\Gamma \cdot a_0 x + b_0 x + \Delta}{\Gamma \cdot ((a_0 x) + b_0 x) + \Delta} \qquad \frac{\Gamma \cdot (a_0 x + \Delta_1) \quad (\Gamma \cdot b_0 x) + \Delta_2}{\Gamma \cdot ((a_0 x) \cdot b_0 x) \cdot \Delta_1 + \Delta_2}$$

where Δ_1, and Δ_2 are two different sequences. There is some artificiality in the symmetrical treatment of intelim rules - the sagittal correspondence - in natural deduction systems (or in the sequent calculus). The symmetry induced by the inversion principle is not derived from the content (of symmetric polynomials), but from a formal duality which is not intrinsic or internal. Negation is generally not involutive- except in finite dual (Boolean) situations- and we could also introduce non-commuting variables in polynomials or in power series, while it is precluded by the double (dual) negation. In intuitionistic logic, this global symmetry is absent and the more complex situations that are reflected in the logic are an indication of more genetic, less structural features. Internal logic is an analysis of content. Here logical content = polynomial

content. Finally, the detachment or elimination rule is equivalent to *Modus Ponens* and the polynomial translation should make manifest the content of the sequential character of inference. Gentzen's linear logic –Gentzen used the phrase "*lineares Räsonieren*"- is by itself a surface phenomenon of the polynomial content. The existential quantifier and the universal quantifier over finite sets interpreted as iterated (finite) sum and iterated (finite) product are also directly eliminable. We have

Proposition 5.3.2 The existential and universal quantifiers are eliminable through direct translation in the polynomial interpretation.

Proof. The universal quantifier can be rendered by

$$\frac{\Gamma \cdot (a_0 x + \Delta)}{\Gamma \cdot (\prod_i (a_i x^i) + \Delta)}(*) \qquad \frac{(\Gamma \cdot ax) \cdot \Delta}{(\Gamma \cdot (\prod_n (a_n x^n)) \cdot \Delta)}(**)$$

where (*) means that x is an indeterminate not appearing in Γ and (* *) means that x is an arbitrary term in the polynomial. The existential quantifier is translated as

$$\frac{\Gamma \cdot (ax + \Delta)}{\Gamma \cdot (\sum_n (a_n x^n) + \Delta)}(**) \qquad \frac{(\Gamma \cdot ax) \cdot \Delta}{(\Gamma \cdot (\sum_i (a_i x^i)) \cdot \Delta}(*)$$

Remarks: The terms $a_i x^i$ are arbitrary. Since we deal with polynomials (with integer coefficients), the existence property for the existential quantifier is immediately garanteed and since the (classical) universal quantifier is limited to finite domains, its scope is always well-defined.

4.4 The elimination of implication

We want to arithmetize (local) implication. We put $1-a = \bar{a}$ for local negation. We have $(\bar{a}_o x + b_o x)^n)$ and we want to exhaust the content of implication — in Gentzenian terms, this would correspond to the exhibition of subformulas (the subformula property). We just expand the binomial by decreasing powers

$$(\bar{a}_o x + b_o x)^n) = \bar{a}_0^n x + n\bar{a}^{n-1} x b_0 x + [n(n-1)/2!]\bar{a}^{n-2} x b^2 x + \ldots + b_0^n x$$

where the companion indeterminate x shares the same power expansion. By an arithmetical calculation (on homogeneous polynomials that are symmetric *i.e.* with a symmetric function $f(x, y) = f(y, x)$ of the coefficients)

$$\begin{aligned}
(\bar{a}_o x + b_o x)^n) &= \bar{a}_0^n x + \sum_{k=1}^{n-1} (n-1/k-1)\bar{a}_0^{k-1} x + (n-1/k) a_0^k x b_0^{n-k} x + b_o^n x \\
&= \sum_{k=1}^{n} (n/k-1) a_0^k x b_0^{n-k} x + \sum_{k=0}^{n-1} (n-1/k) a_0^k x b_0^{n-k} x \\
&= \sum_{k=0}^{n-1} (n-1/k) a_0^{k+1} x b_0^{n-k} x + \sum_{k=0}^{n-1} (n-1/k) a_0^k x b_0^{n-k} x \\
&= \bar{a}_0 \sum_{k=0}^{n-1} (n-1/k)(\bar{a}_0 - 1)^k b^{n-1-k} x + \sum_{k=0}^{n-1} (n-1/k) \bar{a}_0^k x (b_0 - 1)^{n-1-k} x \\
&= (\bar{a}_1 x + b_1 x)(a_1 x + b_1 x - 1)^{n-1}
\end{aligned}$$

and continuing by descent and omitting the x's, we have

$$(\bar{a}_2 + b_2)(\bar{a}_2 + b_2 - 2)^{n-2}$$

$$\dots \quad \dots \quad \dots \quad \dots$$

$$(\bar{a}_{n-2} + b_{n-2} + \bar{a}_{n-2} + {}_{n-2} - (n-2))^{(n-(n-2))}$$

$$(\bar{a}_{n-1} + b_{n-1} + \bar{a}_{n-1} + {}_{n-1} - (n-1))^{(n-(n-1))}$$

$$(\bar{a}_n + b_n)(\bar{a}_n + b_n)^{n-n}.$$

Applying descent again on $(\bar{a}_n + b_n)$,we obtain

$$(\bar{a}_0 + b_0)$$

or, reinstating the x's

$$(\bar{a}_0 x + b_0 x).$$

Remembering that

$$(\bar{a}_x + b_x)_{k<n}^n = \sum_{k+m=n} (k + m/k) \bar{a}^k b^m x^n$$

we have

$$(\bar{a}_x + b_x)_{k<n}^{n+m=n} = \prod_{k+m=n} (k, m) = 2^n$$

or more explicitly

$$\sum_{i=0}^{m+n} c_1 x^{m+n=1} = \bar{a}_0 x \cdot b_0 x \prod_{i=1}^{m+n} (1 + c_i x) = 2^n$$

where the product is over the coefficients (with indeterminates) of convolution of the two polynomials (monomials) a_0 and b_0. We could of course calculate the generalized formula for polynomials

$$(a_0 x + b_0 x + c_0 x + \ldots + k_0 x)^n = \sum_{p,q,r \ldots s} a^p b^q c^r \ldots k^s$$

in the same manner, but we shall postpone the general case till we come to the effinite quantifier for a unified treatment.

The combinatorial content of the polynomial is expressed by the power set 2^n of the n coefficients of the binomial. I contend that this combinatorial content expresses also the meaning of local (iterated) implication. Convolution exhibits the arithmetic connectedness that serves to render the logical relation of implication. Implication is seen here as a power of polynomials, a^k and b^m with $k < m$ having their powers summed up and expanded in the binomial expansion. Some other formula may be used for the product, but it is essential to the constructive interpretation that the arithmetic universe be bounded by 2^n. One way to make things concrete is to analyse $a \to b$ in terms of

$$a \to b = C((2^n - a) + b)$$

where C can stand for combinations or coefficients. The formula is an arithmetical analogue of the topological interpretation of intuitionistic implication.
Theorem 5.4.1 Local implication $a \to b$ can be eliminated by interpreting it as $(\bar{a} + b)^n$.
Proof. By the above construction.

Here I only want to show how is produced a direct polynomial *eliminative* translation of logical constants by rewriting intelim rules of Gentzen's natural deduction system into a polynomial language. The unique identity axiom becomes the equality axiom $A = A$. There are also intelim rules and a polynomial translation for the *effinite* quantifier $\exists x Ax$ as a quantification over an unlimited sequence of natural numbers.

$$(\mathrm{I}\wedge)\quad \frac{A \quad B}{A \wedge B} \qquad ;\ a_0x, b_0x \equiv a_0x \cdot b_0x$$

$$(\mathrm{E}\wedge)\quad \frac{A \wedge B}{A} \quad \text{and} \quad \frac{A \wedge B}{B} \qquad ;\ a_0x \cdot b_0x \equiv a_0x, b_0x$$

$$(\mathrm{I}\vee)\quad \frac{A}{A \vee B} \quad \frac{B}{A \vee B} \qquad ;\ a_0x + b_0x \equiv a_0x,\ a_0x + b_0x \equiv b_0x$$

$$(\mathrm{E}\vee)\quad \dfrac{A\vee B \qquad \begin{array}{c}[A]\\ \vdots\\ C\end{array} \qquad \begin{array}{c}[B]\\ \vdots\\ C\end{array}}{C} \qquad ;\ \begin{array}{l} a_0x+b_0x\equiv c_0x\ (\mathrm{mod}\ b_0x)\\ a_0x+b_0x\equiv c_0x\ (\mathrm{mod}\ a_0x)\end{array}$$

$$(\mathrm{I}\to)\quad \dfrac{\begin{array}{c}[A]\\ \vdots\\ B\end{array}}{A\to B} \qquad ;\ a_0x\equiv b_0x(\mathrm{mod}\ a_0x+1)$$

$$(\mathrm{E}\to)\quad \dfrac{A, A\to B}{B} \qquad ;1-a_0x\equiv b_0x(\mathrm{mod}\ a_0x)$$

$$(\mathrm{I}\neg)\quad \dfrac{\begin{array}{c}A\\ \bot\end{array}}{\neg A} \qquad ;\ 1-a_0x\equiv 1(\mathrm{mod}\ a_0x)$$

$$(\mathrm{E}\neg)\quad \dfrac{A,\neg A}{\bot} \qquad ;\ 1-a_0x\equiv 0(\mathrm{mod}\ a_0x)$$

$$(\mathrm{I}\forall)\quad \dfrac{Ax}{\forall xAx} \qquad ;\ \prod_n a_0x^n\equiv a_0x(\mathrm{mod}\ n)$$

$$(\mathrm{E}\forall)\quad \dfrac{\forall xAx}{At} \qquad ;\ a_0x\equiv \prod_n a_0x^n(\mathrm{mod}\ 1)$$

$$(\mathrm{I}\exists)\quad \dfrac{At}{\exists xAx} \qquad ;\ \sum_n a_0x\equiv a_0x^n(\mathrm{mod}\ 1)$$

$$(\mathrm{E}\,\exists)\quad \frac{\exists x A \qquad \begin{array}{c}[Ax]\\ \vdots \\ B\end{array}}{B} \qquad ;\ a_0 x \equiv \sum_n b_0 x^n (\mathrm{mod}\ 1)$$

$$(\mathrm{I}\,\dot{\exists})\quad \frac{Ax_n}{\dot{\exists} x A x} \qquad ;\ \prod_{n\ldots} a_0 x \equiv a_0 x^n (\mathrm{mod}\ n \times n)$$

$$(\mathrm{E}\,\dot{\exists})\quad \frac{\dot{\exists} x A x}{A t_0} \qquad ;\ a_0 x \equiv \prod_{n\ldots} a_0 x^n (\mathrm{mod}\ 1)$$

In translating logical formulas into congruent forms, we want to represent logical constants in a polynomial language in order to integrally arithmetize (polynomialize) logic. It is manifest in that context that deduction expressed in a turnstile $A \vdash A$ or A/A is a congruence relation in a modular calculus. Implication is rewritten

$$(\bar{a}_o x + b_o x)^n$$

for $\bar{a}_o x = 1 - a_o x$, the local negation (complement) of logic; exponent n denotes the degree of the polynomial (content) of implication that we reduce in the following way by a calculus on symmetrical polynomials (forms).
Remark. In structural and substructural logics, the deduction theorem

$$A, B \vdash C, \text{ iff } A \vdash B \to C$$

is also called *residuation* in the sense that A is a residue in

$$A + B = C, \text{ iff } A = C - B.$$

In those logics, the linear combinations of the premises are subjected to various complex rules to handle the residues. But in modular polynomial logic, the residue A is associated to a positive integer multiple n (An) via a congruence relation

$$C \equiv B (\mathrm{mod}\ n)$$

meaning that $C - B$ is divisible by n, thus adding a direct numerical content to the notion of residuation. In the first three cases above (I $\wedge$), (E $\wedge$) and (I $\vee$), we could have added (mod 0) showing that the congruence relation leaves no residue or remainder, that is

$$C \equiv B \pmod 0 \text{ implies } C = B.$$

Our notion of congruence is arithmetical for modular polynomial arithmetic with integer coefficients in line with Gauss (who invented the concept) and Kronecker. The algebraic notion of congruence in structural algebraic logics does not subsume any numerical content.

5 Final remarks

As I mentioned earlier, it is the Fermat-Kronecker number theory, that is Kronecker's polynomial arithmetic with Fermat's infinite descent, which constitutes the foundational background of my work. Obviously, the foundational motive is alien to set-theoretical foundations and one could quote H.M. Edwards ([2] p. 97) on numerical extensions:

> It is usual in algebraic geometry to consider function fields over an *algebraically closed field* – the field of complex numbers or the field of algebraic numbers rather than over **Q** (the field of rational numbers). In the Kroneckerian approach, the transfinite construction of algebraically closed fields is avoided by the simple expedient of adjoining new algebraic numbers to **Q** as needed.

By transfinite construction, Edwards means clearly the use of set-theoretical devices like Zorn's lemma and model-theoretic tools like the ultrafilter lemma which are equivalent to the axiom of choice *de facto* absent of Kronecker's general arithmetic (*allgemeine Arithmetik*) of polynomials. Algebraic extensions cannot be constructively defined in general, except in finite fields with explicit numerical extensions. For example, infinite models of set theory have elementary (first-order) extensions, e.g. generic sets of Cohen's forcing relation (including its Boolean-valued models) which by the way mimicks the method of field extensions, the accessibility relation on possible worlds in a Kripke model mimicking in turn a timelike forcing relation. Such set-theoretical and logical techniques do not have any potential for concrete numerical content and could be defined as transcendental constructions over infinite sets from a Kroneckerian point of view. So-called constructive or intuitionistic type theories (as in Martin-Löf's proposals) claim to do without the excluded middle principle and the axiom of choice in the construction of types, but as soon as the finite type territory is trespassed with transfinite induction (and recursion), excluded middle is reintroduced — as noticed by Kolmogorov already in 1925 (see Gauthier [5], chap. 6.4) — together with some version of the axiom of choice (e.g. dependent choice). One could add that Peano arithmetic, Heyting arithmetic with transfinite induction and their subtheories or extensions, such as Gödel's *Dialectica* interpretation with induction on all finite types, could

not be made to have direct access to numerical content and numerical extensions in virtue of their lack in concrete constructive procedures and elementary arithmetical operations. The moral of this story may be drawn from Edward Nelson's *Predicative Arithmetic* (p. 177) in his program of arithmetization of logic. Nelson argues that impredicative arithmetic uses induction and recursion principles which need witnesses of witnesses of witnesses... for proofs of consistency, e.g. Gentzen's proof with reduction steps coupled by numerals associated with transfinite ordinals or realizability theories necessitating multiple numerical witnesses for the same logical formula. The proposal in this paper is a direct translation of logical constants into modular polynomial arithmetic with infinite descent replacing an induction postulate. Fermat's (truly finite) descent needs only finite natural numbers as direct witnesses as they are the only testifiers or verifiers of the arithmetical process. My own project for an arithmetical logic dates back to my paper in 1989 " Finite Arithmetic with Infinite Descent" *Dialectica*, 43(4): 329-337. I had sent a preprint to the great French arithmetician André Weil who had inspired my work. He responded that he approved of my use of infinite descent, but he didn't want to comment on my attempted formalization of infinite descent saying that he was not enough of a logician "trop peu logicien" (letter from André Weil, dated March 23, 1988 from Princeton Institute for Advanced Study).

Acknowledgements: I wish to thank an anonymous referee for many useful suggestions.

References

[1] E. Bishop, Mathematics as a Numerical Language, in *Intuitionism and Proof Theory*, 53–71, North-Holland, Amsterdam and New-York, 1970.

[2] H.M. Edwards, *Divisor Theory*, Birkhäuser, Basel, 1987.

[3] H. Friedman, The disjunction property implies the numerical existence property, *Proc. Nat. Acad. Sci.* USA, Vol. 72, No. 8, pp. 2877-2878, August 1975.

[4] Y. Gauthier, A theory of local negation: the model and some applications, *Archiv für mathematische Logik und Grundlagenforschung*, Vol. 25. Nos 3-4 (1985): 127- 143.

[5] Y. Gauthier, *Towards an Arithmetical Logic. The Arithmetical Foundations of Logic*, Birkhäuser/Springer, Basel, 2015.

[6] Y. Gauthier, *Internal Logic. Foundations of Mathematics from Kronecker to Hilbert*, Kluwer, Dordrecht, 2002.

[7] Y. Gauthier, Cantor's normal form theorem and algebraic number theory, *International Journal of Algebra*, Vol. 12 , no. 3 (2018): 133-140.

[8] K. Gödel, Über eine noch nicht benütze Erweiterung des finiten Standpunktes, *Dialectica*, 12 (1958): 230-237.

[9] Y. Gurevich, Intuitionistic logic with strong negation, *Studia Logica*, Vol. 36, Nos 1-2 (1977): 49-59.

[10] D. Hilbert, Über das Unendliche, *Mathematische Annalen*, 95 (1926):161-190.

[11] S. C. Kleene, On the interpretation of intuitionistic number theory, *The Journal of Symbolic Logic*, Vol. 10 (1945): 109-124.

[12] S. C. Kleene, Disjunction and existence under implication in elementary intuitionistic formalisms, *The Journal of Symbolic Logic*, Vol. 27 (1962):11-18.

[13] U. Kohlenbach, *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*, Springer, Heidelberg, 2008.

[14] L. Kronecker, Zur Theorie der Formen höherer Stufen, in *Werke* II, K. Hensel, ed., Teubner, Leipzig, 1968: 419- 424.

[15] L. Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, in Werke III, K. Hensel, ed., Teubner. Leipzig, 245- 387.

[16] D. Nelson, Constructible falsity, *The Journal of Symbolic Logic*, Vol. 14, no. 1, March 1949:16-26.

[17] E. Nelson, *Predicative Arithmetic*, Mathematical Notes 32, Princeton University Press, Princeton, New Jersey, 1986.

Yvon Gauthier
Faculty of Arts and Sciences
University of Montreal
Montreal, Canada
E-mail: yvon.gauthier@umontreal.ca