Polynomizing: Logic Inference in Polynomial Format and the Legacy of Boole

Walter Carnielli
Centre for Logic, Epistemology and the History of Science
and Department of Philosophy- UNICAMP, Campinas, BR
and Center for Logic and Computation–IST, Lisbon, PT
P.O. Box 6133, 13081-970, Campinas, SP, Brazil
carniell@cle.unicamp.br

27th June 2006

Abstract

Polynomizing is a term that intends to describe the uses of polynomial-like representations as a reasoning strategy and as a tool for scientific heuristics. I show how proof-theory and semantics for classical and several non-classical logics can be approached from this perspective, and discuss the assessment of this prospect, in particular to recover certain ideas of George Boole in unifying logic, algebra and the differential calculus.

1 From finite and hard to infinite and smooth

One of the most fascinating episodes of the history of Mathematics, which is nowadays almost considered to be a triviality, is the discovery of the polynomial representation (by infinite series) of numerical functions.

One can situate this historical point in the western historiography, although variants of his methods were already known before in Europe and in China and India as well, around the English mathematician Brook Taylor (1685 - 1731) and his book *Methodus incrementorum directa et inversa*, of 1715, which led to the development of the Taylor's and MacLaurin's expansions. Surprisingly, however, the importance of Taylor's discovery remained unrecognized until 1772, when J. L. Lagrange realized its relevance and proclaimed it to be "the principal foundation of differential calculus".

Any infinitely differentiable function $f(x)$, under certain circumstances, can be rewritten as an infinite polynomial series in the neighborhood of a base point x_0:

$$f(x) = \alpha_0(x_0) + \alpha_1(x_0) \cdot (x - x_0) + \alpha_2(x_0) \cdot (x - x_0)^2 + \dots \alpha_n(x_0) \cdot (x - x_0)^n + \dots$$

for certain coefficients $\alpha_k(x_0)$. What inspires amazement is that such coefficients are the derivatives of $f(x)$ itself calculated in the base point x_0, and the idea of a *local* representation for the function (depending on the point x_0) emerges. Much deep mathematics originated from the questions on how to restore the global behavior of a function from its local behavior (as singularity theory), and how far we have to go in the series to gain substantially all information contained in the function (as Morse theory).

This amounts to transcendental functions being represented by algebraic, polynomial functions –at the cost, however, of accepting infinite expansions. Although the Greeks used the notion of infinite in geometry and arithmetic, as in the famous arguments of Euclid's proof of the infinity of primes, one cannot lose sight, however, of the problems that surrounded the concept of infinity since the hellenistic times.

Also, the notions of finite and infinite were not coincident in ancient Greek and Chinese thought for example (see [23]), which indicates that the notion of infinity was not (and perhaps is not) absolute; this may be seen as a measure of the boldness of users of the infinite much before George Cantor attacked the problem of conferring meaning to the "unthinkable". Hermann Weyl in [33] claims that "mathematics is the science of the infinite", and compares mathematics with religion: "...the religious intuition of the infinite, the $\alpha\pi\varepsilon\iota\rho o\nu$ takes hold of the Greek soul ...". I want to argue that what lies within this idea of expanding simple constructions to the infinite, if not religion, is a powerful method, still to be completely clarified, which I venture to call *polynomizing*: the idea that "finite´´ complexity[1] can be reduced by considering (possibly infinite) polynomial-like representations. I will consider several instances of this idea, particularly in the rise of modern logic by the hands of Boole.

The discovery of power series is, in a sense, a generalization of polynomials taking into account the possibility of extending the sum to the infinite. Polynomials were basically the only functions which could be manipulated by hand to approximate trigonometric functions, for instance, which were almost beyond the capacity of 17th century calculation.

Prior to the full development of integral calculus, the discovery of the formula $\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \ldots$, independently obtained by Gottfried Willhem Leibniz (1646-1716) and by mathematicians in South India in the fifteenth century, attributed to Nilakantha (in Sanskrit verses, cf. [27]) is a good example of the difference between just thinking in terms of infinite objects and thinking in polynomial terms with regard to infinite expansions. John Wallis in 1650 found the expression $\frac{\pi}{2} = \frac{2 \cdot 2 \cdot 4 \cdot 4 \cdot 6 \cdot 6 \ldots}{1 \cdot 1 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \ldots}$ which converges slowly and is hard to generalize. On the other hand, the former expression is a particular case of the expansion $\arctan(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} \ldots$ (for $-1 \leq x \leq 1$) discovered by James Gregory (1638-1675), even if Gregory himself (cf. [18], chapter 4), failed to see that for $x = 1$ it gives the expression for $\frac{\pi}{4}$.

Apparently, Nilakantha was aware of the impossibility of representing π by

[1] Of course, I do not mean here complexity of computation, in the sense of mere efficiency: complexity is here meant in a wider sense, though not divorced from that restricted meaning.

means of a finite series of rational numbers, so the idea of infinite was probably seen as a key to solve the problem of representing π.

However, it is illuminating to see cases where infinite sums and infinite products work together to produce new mathematical knowledge. An example of such cases was a a remarkable result proved by Leonhard Euler (1707-1783) in [19] about equating an infinite sum with an infinite product, which gives an alternative proof of the infinity of prime numbers:

$$\frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ldots}{1 \cdot 2 \cdot 4 \cdot 10 \ldots} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} \ldots$$

which, in contemporary notation, can be written as:

$$\prod_{p} \frac{1}{1 - \frac{1}{p}} = \sum_{n} \frac{1}{n}$$

for all primes p and natural numbers $n \geq 1$.

This formula, which coincides with a particular case of the celebrated Riemann Zeta function at the value $s = 1$, gives an alternative proof of the fact (already known by Euclides) that there exist an infinite number of primes, by taking into account that the left-hand harmonic series is divergent.

Though I am more interested here in "infinite" methods emerging from algebra, there is of course a geometric side in the advent of the infinite expedient to produce finite calculations: as a precursor to integral calculus, Bonaventura Cavalieri (1598-1647) had completely developed a method of indivisibles, as a means of determining the size of geometric figures similar to the methods of integral calculus in his *Geometria Indivisibilibus Continuorum Nova Quadam Ratione Promota* ("A Certain Method for the Development of a New Geometry of Continuous Indivisibles"), published in Bologna in 1635.

According to [26], a method similar to Cavalieri's had already been used in China around the third century to find the volume of a sphere.

Intuition in this direction not only impacted algebra and geometry, but certainly influenced (directly of indirectly) Boole and other logicians. I want to suggest that it is possible to identify an ancient tradition of what I called "polynomizing", which has also deeply influenced logic, but this approach, although present in many aspects in Boole's work was for some reason relegated. However, as I plan to show, it can be regained inside the methods of logic–and in several aspects, from propositional to many valued, from paraconsistent to modal and even to first-order logics, and it may be used as a reasoning model, helping understand certain aspects of Boole's methods.

George Boole is reputed one of the greatest logicians or philosophers of logic of all times: John Corcoran in [16] considers the *Prior Analytics* by Aristotle and the attempts by George Boole (1815–1864) to codify the laws of thought ([6]) as the two most important logical works from before the advent of modern logic.

However, Boole is often accused of fallacies and incoherences, and his logic calculations are sometimes considered close to ridiculous: as in [17] puts it, "Readers of Boole's logical writings will be unpleasantly surprised to discover... how ill-constructed his theory actually was and how confused his explanations of it", and even Corcoran, on p.285 of [16] dares say that "Aristotle seems superior to Boole and closer to contemporary thinking. My guess would be that Aristotle would have less trouble understanding Gödel's results than Boole."

Indeed, some of calculations Boole proposed may seem awkward and inept, but the critiques would lose impetus if one regards Boole's dream of algebrizing logic and his search for missing links between ordinary algebra and Aristotelian Logic from the point of view of attempts to polynomize: Boole was more interested in the algebraic aspects of logic, by means of solving equations expressed in polynomial form, than he was in the logic aspects of algebra.

The intentions of this paper are twofold: firstly, to raise some ideas on recovering the algebraic setting of logic in a broad sense, showing how this can be applied to the clarification of some criticisms in Boole's work; a second intention is to propose a wider algebraic stand to the contemporary view of classical and non-classical logics.

2 Algebraic proof systems

Boole, in [6], attached great importance to the "index law" $x^2 = x$, placing it in such a central position that, for him, "...a fundamental law of Metaphysics is but the consequence of a law of thought".

From the purely mathematical side, this has connections to another important work of Boole: the invention of the calculus of finite differences of 1860 ([7]), preceded by his better known treatise on differential equations.

Boole was one the first to perceive clearly that the symbols in operations could be treated directly as objects of calculation, separated from the idea of quantity. However, Leibniz already admitted equations with no explicit arithmetical content such as $x + x = x$, and even talked about "blind thinking" to refer to pure reasoning reduced to arithmetical calculation (cf. [28]). It is interesting to know how Leibniz, in his *Elementa Calculi* of 1679, assigned numbers to concepts in such a way as to obtain a complete representation for Aristotelian syllogistic and complete version of algebraic logic in Boolean terms, although apparently Boole did not know his work (see [10] for proofs of correctness and completeness of the two mentioned systems).

Besides the "index law" $x^2 = x$, Boole assumed, differently from Leibniz, that $x+x = 0$ implies $x = 0$. He did not assume multiplicative inverse, but just additive inverse; from contemporary viewpoint, many problems behind Boole's methods are explained by the fact that he was not working within a *field*: he accepted the generalization of the index law $x^n = x$ in [4], but this will be rejected in [6]; indeed, for him $x^3 = x$ would lead to $x^3 - x$ to have as factors $x + 1$ and $x - 1$. The first could not be accepted, as $1 + x$ would correspond to adding x to the universe 1, and -1 is equally non interpretable, since it does not satisfy the index law $(-1)^2 = (-1)$. However, analogous difficulties will arise in the same index law $x^2 = x$, since it is equivalent to $x^2 - x = 0$, which has $x + 1$

and $x - 1$ as factors as well (for details see [22]).

Of course Boole was opening a path to future developments that would only come after his achievements, such as working with rings of characteristic 2 with unity. This would make simple to accept for instance $1 = -1$ and solve many of his difficulties– in particular, for his case, a Boolean ring with unity would suffice (a concept that possibly would never have been invented if it were not for his difficulties!).

Departing from the idea that if the intuition behind the index law had some importance for classical logic (even if exaggerated by Boole), it seemed obvious that this law could be easily generalized to the 'higher-order laws" of the form $x^n = x$ (that Boole had to reject) by employing polynomials over Galois fields: intending to explore such laws for non-classical, [11] studied the question for some finite-valued logics. I later learned that some methods for Boolean reasoning were developed by the Russian logician Platon Sergeevich Poretski in the 19th century (cf. [31], and that [34] in 1927 proposed a translation of propositions into polynomials in the realm of classical logics (with the initial intention to give a method of proof for the propositions of *Principia Mathematica*). More recently, analogous ideas have been considered by [32] (with the purposes of automatic proof theory by means of rewriting systems) and by [15] and [3] (by computing Gröbner bases with the purpose of investigating proof complexity).

However, (as far as I know) polynomial rings over Galois fields were not extensively used, nor the method extended to all finite-valued logics, to non-finite valued logics or to first-order logic.

In particular, by means of Boolean rings over finite fields (using formal series with sums and products over convenient variables) one can obtain a sound and complete method where any finite-valued derivations and classical propositional derivations reduce to solving equations in polynomial form; what is more surprising, the method cab be applied to non-finite-valued propositional logics (as far as they can be represented by means of the dyadic semantics studied in [9]) by means of introducing multivariable polynomials in appropriate rings (cf. [13]). In particular, the same method permits to represent and compute the so-called "non-deterministic" logics of A. Avron, as in [14].

The polynomial ring calculus can be successfully extended at least to the monadic fragment of first-order logic that expresses traditional syllogisms, giving a new approach to Boole's representation. So Boole's intent to unify the two sides of logic, the propositional and the quantificational, could also be seen as related to the idea of polynomizing. I wish to discuss the role of this approach as a reasoning model and suggest its role in scientific discovery.

3 The strange methods of George Boole

The idea that Boolean algebra can be regarded as abstract rings is a consequence of the sophisticated result of M. H. Stone of 1936 (cf. [30]), and the fact that any Boolean algebra can be represented by algebras of classes is seen by Stone as a precise analogue of the fact that any abstract group is represented by an isomorphic group of permutations.

Based on ideas introduced in [13], I briefly review here the intuitions of using polynomials instead of formulas for finite many-valued logics. Given a propositional logic $\mathbf{L}$, a *polynomial interpretation* for $\mathbf{L}$ is a translation $\Omega : \mathbf{L} \mapsto \mathbf{F}[X]$ of the wffs of $\mathbf{L}$ into a convenient polynomial ring $\mathbf{F}[X]$. Then a wff $\alpha \in \mathbf{L}$ is *satisfiable* if its polynomial traduct $\alpha^* \in \mathbf{F}[X]$ is closed within a certain set $D \subseteq \mathbf{F}$ of distinguished truth-values when evaluated in the field $\mathbf{F}$.

It is convenient to show first that any finite function can be expressed by means of polynomials over finite fields using a particular case of the well-known Lagrange interpolation[2] (a simple but important fact that almost certainly belongs to the mathematical folklore of combinatorics and coding theory).

Theorem 3.1. *(Representation of finite functions in $GF(p^n)$) Let A be any finite set with cardinality $\mid A \mid= k$ and $f : A^m \mapsto A$ be any function with m variables on A. Let $GF(p^n)$ be a Galois field with $p^n \geq k$ elements. Then f can be represented as a polynomial function in $GF(p^n)[x_1, \ldots, x_m]$.*

Proof. The proof is just sketched for the case of binary functions. Suppose, without loss of generality, that the elements of A are $\{0, 1, \ldots, m-1\} \subset GF(p^n)$.

Define the functions $\delta_{\langle m,n\rangle}(x, y)$ as:

$$\delta_{\langle m,n\rangle}(x, y) = \prod_{i\neq n, j\neq m} (x - i) \cdot (y - j) \cdot \prod_{i\neq n, j\neq m} (n - i)^{-1} \cdot (m - j)^{-1}$$

Clearly, $\delta_{\langle m,n\rangle}(x, y) = 1$ if $\langle x, y\rangle = \langle m, n\rangle$, and 0 otherwise.

Now, if $f : A^2 \mapsto A$ has values $f(i, j) \in GF(p^n)$, then:

$$p(x, y) = f(0, 0)\cdot\delta_{\langle 0,0\rangle}(x, y)+f(0, 1)\cdot\delta_{\langle 0,1\rangle}(x, y) \ldots f(m-1, m-1)\delta_{\langle m-1,m-1\rangle}(x, y)$$

is a polynomial in $GF(p^n)[x_1, x_2]$ which represents $f(x, y)$. Of course, a similar construction can be obtained for the general case. □

It should be remarked that it is essential to work within a Galois field $GF(p^n)$: for example the binary function $f(x, y) = max\{x, y\}$ and the unary function $g(x) = 0$ if $x \neq 2$, and $g(2) = 3$, though representable in $GF(2^2)[x, y]$, cannot be represented in $Z_4[x, y]$.

The method above gives a particularly expeditious method to compute polynomials over Z_3, since in this case the denominator $\prod_{i\neq n, j\neq m}(n - i) \cdot (m - j)$ of the functions $\delta_{\langle m,n\rangle}(x, y)$ can be easily seen to be the unity: indeed, $\prod_{i\neq n}(n-i)$ and $\prod_{j\neq m}(m-j)$ are products of distinct non zero factors, and can only be $1\cdot 2$ or $2 \cdot 1$ in Z_3; hence the product $\prod_{i\neq n, j\neq m}(n - i) \cdot (m - j)$ is 1.

This is interesting since the vast majority of examples and usage of many-valued logics falls into the three-valued case. Thus, for the specific case of converting three-valued logics into polynomial form, the functions $\delta_{\langle m,n\rangle}(x, y)$ are:

$\delta_{\langle 0,0\rangle}(x, y) = (x - 1) \cdot (x - 2) \cdot (y - 1) \cdot (y - 2)$

[2] I am indebted to Odilon Otávio Luciano from IME- USP for this remark.

$\delta_{\langle 0,1\rangle}(x,y) = (x-1)\cdot(x-2)\cdot y\cdot(y-2)$
$\delta_{\langle 0,2\rangle}(x,y) = (x-1)\cdot(x-2)\cdot y\cdot(y-1)$
$\delta_{\langle 1,0\rangle}(x,y) = x\cdot(x-2)\cdot(y-1)\cdot(y-2)$
$\delta_{\langle 1,1\rangle}(x,y) = x\cdot(x-2)\cdot y\cdot(y-2)$
$\delta_{\langle 1,2\rangle}(x,y) = x\cdot(x-2)\cdot y\cdot(y-2)$
$\delta_{\langle 2,0\rangle}(x,y) = x\cdot(x-1)\cdot(y-1)\cdot(y-2)$
$\delta_{\langle 2,1\rangle}(x,y) = x\cdot(x-1)\cdot y\cdot(y-2)$
$\delta_{\langle 2,2\rangle}(x,y) = x\cdot(x-1)\cdot y\cdot(y-1)$

We suppose, then, that all calculations are done within a convenient field $GF(p^n)$; there are two basic sets of rules to manipulate polynomials:

a) Index rules

1. $p\cdot x \vdash_{\approx} 0$, where $p\cdot x$ means $x+x+\ldots+x$ p times
2. $x^i\cdot x^j \vdash_{\approx} x^k(mod\ q(x))$ where $q(x)$ is a convenient primitive polynomial that defines $GF(p^n)$, and $k = i+j(mod\ p^n-1)$

b) Ring rules

1. $f+(g+h)\vdash_{\approx}(f+g)+h$
2. $(f+g)\vdash_{\approx}(g+f)$
3. $f+0\vdash_{\approx} f$
4. $f+(-f)\vdash_{\approx} 0$
5. $f\cdot(g\cdot h)\vdash_{\approx}(f\cdot g)\cdot h$
6. $f\cdot(g+h)\vdash_{\approx}(f\cdot g)+(f\cdot h)$

We also need some explicit metarules : For $f,g,h\in\mathbf{F}[X]$:

1. Uniform Substitution: $\frac{f\vdash_{\approx} g}{f[x:h]\vdash_{\approx} g[x:h]}$
2. Leibnitz Rule: $\frac{f\vdash_{\approx} g}{h[x:f]\vdash_{\approx} h[x:g]}$

The index rules are justified taking into account that the Galois field $GF(p^n)$ has characteristic p as a ring with multiplicative identity element, and that the multiplicative group of every finite field $GF(p^n)$ is cyclic. The ring rules come form the fact that $GF(p^n)[X]$ (on appropriate variables in X) is a polynomial ring. Uniform Substitution and Leibnitz Rule can be easily justified by induction on polynomial functions.

Now, for the definitions of deduction and proof in the polynomial ring calculus for the logic $\mathbf{L}$, let $\Gamma\cup\{\alpha\}$ be wffs in $\mathbf{L}$ and Γ^*,α^* be their translations in polynomial form: the following general completeness of the method can be proven for any finite-valued logic: $\Gamma\vdash_{\mathbf{L}}\alpha$ iff $\Gamma^*\vdash_{\approx}\alpha^*$ where $\vdash_{\approx}$ denotes the derivation of $\alpha^*\in D$ (in the equational logic defined by the above rules) from the hypothesis $\Gamma^*\in D$ (see [13] for details).

Of course, when the the set D of distinguished values is a singleton, say $D = \{1\}$, then derivations $\Gamma^* \vdash_{\approx} \alpha^*$ reduce to proving $\alpha^* \approx 1$ from the hypothesis $\Gamma^* \approx 1$, and (when $\Gamma = \emptyset$) proofs reduce to showing directly that $\alpha^* \approx 1$ by high-school manipulation of polynomials.

Just for illustration, consider the case of classical logic **PC**. Define in this case the translation $\Omega : \mathbf{PC} \mapsto Z_2[X]$ of **PC** into the Boolean ring $Z_2[X]$ as:

- $\Omega(p_i) = x_i$ for each atomic variable p_i
- $\Omega(\neg\alpha) = 1 + \Omega(\alpha)$
- $\Omega(\alpha \wedge \beta) = \Omega(\alpha) \cdot \Omega(\beta)$
- $\Omega(\alpha \vee \beta) = \Omega(\alpha) \cdot \Omega(\beta) + \Omega(\alpha) + \Omega(\beta)$
- $\Omega(\alpha \to \beta) = \Omega(\alpha) \cdot \Omega(\beta) + \Omega(\alpha) + 1$

Thus, for instance, having translated atomic variables p_i as fresh variables x_i, we have:

- $x^2 \approx x$
- $x + x \approx 0$
- $\neg\alpha \approx 1 + x$
- $\alpha \wedge \beta \approx x \cdot y$
- $\alpha \vee \beta \approx x \cdot y + x + y$
- $\alpha \to \beta \approx x \cdot y + x + 1$

Proving *reductio ad absurdum*, for example, amounts to:

- $\alpha \to \beta, \alpha \to \neg\beta \vdash_{PC} \neg\alpha$. Translating into polynomial form, we have to check that: $(x \cdot y + x + 1) \cdot (x \cdot (y + 1) + x + 1) \cdot x \vdash_{\approx} 0$
- But easily: $(x \cdot y + x + 1) \cdot (x \cdot (y + 1) + x + 1) \cdot x \approx (x \cdot y + x + 1) \cdot (x \cdot y + 1) \cdot x \approx (x^2\dot{y}^2 + x \cdot y + x^2 \cdot y + x + x \cdot y + 1) \cdot x \approx (\overbrace{x \cdot y} + \overbrace{x \cdot y} + \overbrace{x \cdot y} + x + \overbrace{x \cdot y} + 1) \cdot x \approx (x + 1) \cdot x \approx x^2 + x \approx 0$ taking into account (as indicated) that here $x^2 \approx x$ and $x + x \approx 0$.

Now, for classical logic **PC** this seems to be an obvious usage of Boolean algebras and Boolean rings, but the same can be done for all finite-valued logics[3]; of special interest are the cases of the well-known (see e.g. [21]) three-valued logics of Lukasiewicz, Gödel, Kleene, Sette, and the four-valued logic of Belnap (see [13] for concrete examples of polynomial proofs in three-valued logics).

However, some authors (as for instance [16]) see solving equations as opposed to performing deductions. In that paper J. Corcoran points to two fallacies of

[3]In a certain sense, this is the algebraic analogue of the universal method for provability in many valued logics shown in [11]

Boole: a first fallacy (p. 280 and 281) is that Boole overlooks indirect reasoning, or *reductio ad absurdum*, an important and productive form of inference: "This... is very likely part of why he missed indirect deduction (or *reductio* reasoning). There is no such thing as indirect equation-solving, of course."

This criticism cannot be taken literally, as we just have seen (as an example) an equational proof of *reductio ad absurdum*. The second fallacy, according to Corcoran, is the *Solutions Fallacy*, which involves confusing solutions to an equation with its consequences. For example, the equation $x = (x \cdot y)$ (in a Boolean algebra– an unavoidable anachronism!) does not imply the solutions $x = 0$ or $y = 0$ (since x and y may be both 1). However, $x = 0$ does imply $x = (x \cdot y)$. In defense of Boole it could be added, as S. Burris suggests in [8], that there exists a kind of "universal error" of Boole's interpreters: Boole used existential import in his Aristotelian arguments but this is usually not taken into account: for example, Boole used Aristotelian semantics, accepting arguments (as *Conversion by Limitation*) which only make sense if all classes are non-empty:'All A is B', therefore 'Some B is A'.

As an interesting example, let us recall an example by Boole from his paper of 1848 ([5], pp. 7-8), proving contraposition. The sentence "All Ys are Xs´´ is formalized in his algebra as $y = v \cdot x$ (meaning: Y is the intersection of X with some non-empty V) and he seeks the value of $1 - x$ (i.e., the class not-X).

Boole uses $x \cdot y$ to denote intersection, $x + y$ to denote union (provided $x \cdot y = 0$) and $x - y$ to denote class difference (provided $y \subsetneqq x$); thus $1 - x$ denotes the complement of x; 0 denotes the empty class, and 1 is the universe of discourse.

A point which caused some confusion in Boole's intuition is that $x \cdot y$ can be interpreted as intersection or conjunction, but + cannot be interpreted as union or disjunction: indeed, while $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ holds in propositional logic, $x + (y \cdot z) = (x + y) \cdot (x + z)$ does not hold universally in what is today called a Boolean ring; it can be easily checked that:

$x + (y \cdot z) = (x + y) \cdot (x + z)$ iff $x \cdot (y + z) = 0$.

This is, of course, due to the fact that + should be seen as "exclusive or", not usual disjunction.

First, Boole solves the equation $y = v \cdot (1 - z)$ in the new variable z (putting $1 - x = z$): $z = v \cdot (1 - y) + \frac{1}{0}(1 - v) \cdot y + \frac{0}{0}(1 - v) \cdot (1 - y)$

He then considers $\frac{1}{0}$ as an "infinite coefficient" and thus the term $\frac{1}{0}(1 - v) \cdot y$ vanishes, but $\frac{0}{0}$ is to be replaced by "an arbitrary elective symbol w"

Thus the equation becomes: $z = v \cdot (1 - y) + +w \cdot (1 - v) \cdot (1 - y)$ or $1 - x = (v + w \cdot (1 - v)) \cdot (1 - y)$

He then argues that $(v + w \cdot (1 - v))$ represents a class, since it satisfies the "index law"$(v + w \cdot (1 - v))^n = (v + w \cdot (1 - v))$, and therefore can be replaced by an "elective symbol" u: therefore $1 - x = u \cdot (1 - y)$, i.e., "All not-Xs are not-Ys".

This "elective symbol" was a source of problems and misunderstanding, and has been widely criticized since the beginning (see [28]). But the point is that Boole is actually trying to reason at the same time with algebra and with classes, so in a certain way anticipating the results that would only be clarified by M.

Stone more than 80 years later. I think that Boole was much more innovative than logicians would suppose: he even mixed ideas of differential calculus to logic, algebra and probability, a blend that we are far from understanding in the general case of non-classical logics.

4 Infinite polynomials and Aristotelian logic

In [29], Ernst Schröder, in his reformulation of Boole's logic, already considered addition and multiplication as logical operations and stressed their dual character. He introduced the symbols $\prod$ and $\sum$ as arithmetic analogues of conjunction and disjunction; quantification could thus be seen as "indefinite" operations (indefinite logical addition for existential quantification, and indefinite logical multiplication for existential quantification).

However, the approach I am considering here is significantly distinct: Schröder was probably influenced by the ideas of Charles S. Peirce, and the way he chose to see logic as a model of absolute algebra does not seem to be generalizable to logics other than classical; what I suggest, instead, is a way to employ algebra to represent and calculate logical inference[4].

Departing from such motivations, I now examine some preliminary ideas on expressing first-order logic (**FOL**)in polynomial form, but treating the monadic case only.

The translation rules for interpreting propositional logic in terms of polynomials over Z_2 can be extended to first-order logic by adding clauses defining a translation $\Omega : \mathbf{FOL} \mapsto Z_2[X]$:

1. For each constant c_i (in a denumerable universe), $\Omega(A(c_i)) = x_i^A$ (i.e., a new variable in $Z_2[X]$)
2. $\Omega(\forall z A(z)) = \prod_{i=1}^{\infty} x_i^A$. This results in:
3. $\Omega(\exists z A(z)) = \Omega(\neg\forall z \neg A(z)) = 1 + \prod_{1=1}^{\infty}(1 + x_i^A)$

It is to be noted that now polynomials are infinite (i.e, are formal series in $Z_2[X]$). To simplify notation, let $\Omega(\forall z A(z)) = \prod x_i$ and $\Omega(\exists z A(z))$= $1+\prod(1+x_i)$.

It is instructive to see some examples of proofs in **FOL**.

- $\forall z A(z) \to \exists z A(z)$:
  $(\prod x_i)\cdot(1+\prod(1+x_i))+\prod x_i+1 \approx (\prod x_i)\cdot(\prod(1+x_i))+\prod x_i+\prod x_i+1 \approx (\prod x_i\cdot(1+x_i))+\prod x_i+\prod x_i+1 \approx 1$ since $\prod x_i+\prod x_i \approx 0$ and $x_i\cdot(1+x_i) \approx 0$ for each x_i

As another example, consider:

- $(\forall z A(z) \to \forall z B(z)) \to \forall z(A(z) \to B(z)])$:

[4] Perhaps, if this contributes to a better understanding of the approach, one might call it *algebra ratiocinator*.

1. Let $\alpha := (\forall z A(z) \to \forall z B(z))$: $\prod x \cdot \prod y + \prod x + 1 \approx \prod x \cdot y + \prod x + 1$
2. Let $\beta := \forall z(A(z) \to B(z))$: $\prod(x \cdot y + x + 1)$
3. $\alpha \to \beta$: $(\prod x \cdot y + \prod x + 1) \cdot \prod(x \cdot y + x + 1) + (\prod x \cdot y + \prod x + 1) + 1 \approx$
4. $\prod(x{\cdot}y{+}x{\cdot}y{+}x{\cdot}y){+}\prod(x{\cdot}y{+}x{+}x){+}\prod(x{\cdot}y{+}x{+}1){+}(\prod x{\cdot}y{+}\prod x{+}1){+}1 \approx$
5. $\prod(x \cdot y) + \prod(x \cdot y) + \prod(x \cdot y + x + 1) + (\prod x \cdot y + \prod x) \approx$
6. $\prod(x \cdot y + x + 1) + \prod x \cdot y + \prod x \not\approx 1$

The method (as much as other proof procedures as tableaux, for instance) can also be used to find counter-models: Why is $\prod(x{\cdot}y{+}x{+}1){+}\prod x{\cdot}y{+}\prod x \not\approx 1$? Well, if there are x and x' such that $x = 0$ and $x' = 1$, and some y such that $y = 0$, then: $\prod(x' \cdot y + x' + 1) + \prod x \cdot y + \prod x = \prod(0 + 1 + 1) + \prod 0 + \prod 0 = 0$ which is precisely a usual (and intuitive) counter-model: $x = 0$ corresponds to a false instance $A(a)$, and $x' = 1$ corresponds to a true instance $A(b)$, and $y = 0$ corresponds to a false instance $B(c)$.

Boole's analysis of Syllogistic Logic can now be recovered in polynomial form. Recall the four Aristotelian categorical forms:

A – All A is B: $\forall z(A(z) \to B(z))$

I – Some A is B: $\exists z(A(z) \wedge B(z))$

E – No A is B: $\forall z(A(z) \to \neg B(z))$

O – Some A is not B: $\exists z(A(z) \wedge \neg B(z))$

where **A** and **I** are affirmative (respectively, universal and existential), **E** and **O** are negative (respectively, universal and existential), **A** = ¬**O** and **I** = ¬**E**.

Recalling our simplified notation, the categorial propositions are expressed in polynomial form as follows:

1. $\Omega(\forall z A(z)) = \prod x_i$
2. $\Omega(\exists z A(z)) = 1 + \prod(1 + x_i)$
3. $\Omega(\neg\alpha) = 1 + x$
4. $\Omega(\alpha \wedge \beta) = x \cdot y$
5. $\Omega(\alpha \to \beta) = x \cdot y + x + 1$

Mnemonically:

- **A** (All A is B): $\prod(a \cdot b + a + 1)$
- **I** (Some A is B): $1 + \prod(1 + a \cdot b)$

It is now possible to recover Boole's interpretation: for the form **A**,

- **A** holds iff $\prod(a \cdot b + a + 1) = 1$ iff $a \cdot b + a + 1 = 1$ for every a, b iff $a \cdot b + a = 0$ for every a, b iff $a \cdot b = a$ for every a, b

which coincides with Boole's formalization of **A** as "$AB = A$" in his book [4] of 1847.

It is important to remark here that $a \cdot b = a$ implies $a = 0$ if $b = 0$, and that $a \cdot b = a$ holds "vacuously" if $a = 0$.

Similarly, for the form **I**:

- **I** holds iff $1 + \prod(1 + a \cdot b) = 1$ iff $\prod(1 + a \cdot b) = 0$ iff $1 + a_0 \cdot b_0 = 0$ for some a_0, b_0 iff $a_0 \cdot b_0 = 1$ for some a_0, b_0

which by its turn coincides with Boole's formalization of **I** as "$AB = V$" in his article [5] of 1848.

5 Proving syllogisms in polynomial form

As an example let us show how to use this technique to prove the syllogism *Barbara* (mode **AAA** of the First Figure):

From		
A	All A is B	$a \cdot b = a$ for every a, b
A	All B is C	$b \cdot c = b$ for every b, c
conclude		
A	All A is C	$a \cdot a = b$ for every a, b

The proof runs as follows (recalling the mnemonic abbreviation above):

1. $a \cdot b = a$ hypothesis 1
2. $b \cdot c = b$ hypothesis 2
3. $a \cdot b \cdot c = a \cdot b$ from (2), multiplying by a
4. $a \cdot c = a$ from (3) and using (1), replacing $a \cdot b$ by a

As another example, it is instructive to prove the syllogism *Darii* (mode **AII** of the First Figure):

From		
A	All B is C	$b \cdot c = b$ for every b, c
I	Some A is B	$a_0 \cdot b_0 = 1$ for some a_0,b_0
conclude		
I	Some A is C	$a_0 \cdot c_0 = 1$ for some a_0,c_0

The proof is as follows:

1. $a_0 \cdot b_0 = 1$ hypothesis 2
2. $b_0 = b_0 \cdot c_0$ instance of hypothesis 1

3. $a_0 \cdot b_0 = a_0 \cdot b_0 \cdot c_0$ from (2)

4. $a_0 \cdot b_0 \cdot c_0 = c_0$ from (1)

5. $a_0 \cdot b_0 = c_0$ from (3) and (4)

6. $a_0 \cdot a_0 \cdot b_0 = a_0 \cdot c_0$ from (5),

7. $a_0 \cdot b_0 = a_0 \cdot c_0$ from (6), since $a_0 \cdot a_0 = a_0$

8. hence $1 = a_0 \cdot c_0$ from (1) and (7)

It is well known that from *Barbara* and *Darii* all the 19 valid syllogistic forms can be deduced, by means of the following rules:

- Conversion: Some A is B/ Some B is A (in our notation: $a_0 \cdot b_0 = 1/b_0 \cdot a_0 = 1$);
- Conversion by limitation: All A is B/ Some A is B (in our notation: $a \cdot b = a/a_0 \cdot b_0 = 1$).

Conversion is an obviously valid rule in our setting. Conversion by limitation is more complicated, since our method takes into account the "contemporary" semantics, where classes can be empty, as remarked before. In order to adapt it to "Aristotelian" semantics that assumes existential import, we have to suppose that there exists a_0 such that $a_0 = 1$. Thus, since supposing "All A is B" implies $a \cdot b = a$ holds for all a, there must be b_0 such that $a_0 \cdot b_0 = 1$. If not, then $a_0 \cdot b = 0$ for any b, which implies $a_0 = 0$, contradiction.

6 Conclusions

The methods described in this paper have a promising potentiality to any truth-functional multiple-valued logic; there is an exciting area of research in designing new proof theory techniques for such logics, and simplifying applications to multiple-valued logics in decision tables and discovering patterns, as in several other fields (it is well-known that multiple-valued logics find applications in artificial intelligence, database theory and data mining, modeling reasoning and model checking, for instance). It is important to emphasize that the method is also plainly applicable to non-finite valued logics, and also to represent binary semantics for many-valued logics[5] (cf. [13]) and even to quantum circuits and quantum gates (cf. [1]). The arguments advanced here try to conceptualize this approach, in particular when extended to quantification and non-finite valued logics, as inheritance of an admirable legacy in the mathematical thinking, which may have been disregarded by logicians. We should keep in mind that Boole's ideas included to relate logic to probability theory and to the fascinating method

[5] In such cases, the binary semantics for a finite-valued logic may be simpler and more philosophically palatable than the multiple valued one, and even permits a completely different approach to the logic, but at the cost of losing truth-functionality; see [9].

of finite differences. By exploring it conveniently we would gain new tools in logic and in our patterns of reasoning, and assess Boole's work from a new perspective.

As B. Mates points out in [25], Boolean insights rehabilitated Stoic logic, rather than Stoicism supported Boole. Starting from a historical background leading up to a modern perspective on algebraic logic, the excellent survey [2] accurately concludes (p. 511) that the ideas of Boole have not borne their full fruit yet.

We are suggesting here that Boolean insights also rehabilitated a method of looking at logic which boldly mixes logic with the roots of differential calculus. How possible would be to try to re-analyze some deep Boolean intuitions and return to a closer algebraic approach to logic, good for several logics, and to methods of differential calculus in logic, taking profit of the idea of polynomizing? As It does not seem to be easy to extend this type of calculus to full **FOL** and to higher-order logic or even to modal logics– an specially interesting application would be to extend it to the finite variables fragment of **FOL**– but this seems to be a very rewarding challenge.

References

[1] Agudelo, J. C., Carnielli, W. A. Quantum algorithms, paraconsistent computation and Deutsch's problem. Proceedings of the 2nd Indian International Conference on Artificial Intelligence, Pune, India, December 20-22, 2005.(Ed. Bhanu Prasad *et allia*). IICAI 2005, pp. 1609-1628. Pre-print available from *CLE e-Prints* vol. 5(10), 2005. URL = ftp://logica.cle.unicamp.br/pub/e-prints/MTPs-CompQuant%28Ing%29.pdf

[2] Ahmed, T. S., Algebraic logic, where does it stand today? *Bull. Symbolic Logic* 11, iss. 4 (2005), 465–516.

[3] Beame, P., Impagliazzo, R., Krajicek, J., T. Pitassi, T. and Pudlak, P. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society* 73:1–26, 1996.

[4] Boole, G., The Mathematical Analysis of Logic, Being an Essay Towards a Calculus of Deductive Reasoning. London: Macmillan, Barclay and Macmillan, 1847. (Reprinted by Basil Blackwell, Oxford, 1965).

[5] Boole, G., The calculus of logic. *Cambridge and Dublin Math. Journal* 3, 183–198,1848.

[6] Boole, G., An Investigation of the Laws of Thought, on Which are Founded the Mathematical Theories of Logic and Probabilities. Walton and Maberley, London, 1854. (Reprinted by Dover Books, New York, 1954).

[7] Boole,G., Calculus of Finite Differences (originally published in 1860) 5th Edition, Chelsea Publishing, 1970.

[8] Burris, S., The laws of Boole's thought. Unpublished, 2002. Preprint at URL http://www.thoralf.uwaterloo.ca/htdocs/MYWORKS/PREPRINTS/aboole.pdf.

[9] Caleiro, C., Carnielli, W. A., Coniglio, M. E, and Marcos, J., Two's company: "The humbug of many logical values". In *Logica Universalis*, 169–189, editor Béziau J.-Y., Birkhäuser Verlag, Basel,Switzerland, 2005. Preprint available at: URL= http://wslc.math.ist.utl.pt/ftp/pub/CaleiroC/05-CCCM-dyadic.pdf.

[10] Caicedo, X., Martín, A., Completud de dos cálculos lógicos de Leibniz. *Theoria* 16(3), 539–558, 2001.

[11] Carnielli, W. A., Systematization of the finite many-valued logics through the method of tableaux. *The Journal of Symbolic Logic*52(2), 473-493, 1987.

[12] Carnielli, W. A., A polynomial proof system for Lukasiewicz logics. Second Principia International Symposium. August 6-10, 2001, Florianópolis, SC, Brazil.

[13] Carnielli, W. A., Polynomial ring calculus for many-valued logics. Proceedings of the 35th International Symposium on Multiple-Valued Logic. IEEE Computer Society. Calgary, Canadá. IEEE Computer Society, pp. 20-25, 2005. Available from *CLE e-Prints* vol. 5(3), 2005 at: URL= http://www.cle.unicamp.br/e-prints/vol_5,n_3,2005.html.

[14] Carnielli, W. A., Coniglio, M. E., Polynomial formulations of non-deterministic semantics for logics of formal inconsistency. Manuscript.

[15] Clegg,M., Edmonds,J., Impagliazzo, R., Using the Gröbner bases algorithm to find proofs of unsatisfiability. Proceedings of the 28th Annual ACM Symposium on Theory of Computing Philadelphia, Pennsylvania, USA, 1996, pp. 174–183.

[16] Corcoran, J., Aristotle's Prior Analytics and Boole's Laws of Thought, *Hist. and Ph. of Logic* 24:261–288, 2003.

[17] Dummett, M., Review of "Studies in Logic and Probability by George Boole". Rhees, R., Open Court, 1952, *J. of Symb. Log.* 24, 203–209, 1959.

[18] Eves, H., An Introduction to the History of Mathematics, (6th ed.) New York: Saunders, 1990.

[19] Euler, L. , Variae observations circa series infinitas, *Commentarii academiae scientiarum Petropolitanae* 9 (1737), 1744, p. 160-188. Reprinted in *Opera Omnia*, Series I volume 14, Birkhäuser, p. 216-244. Available on line at www.EulerArchive.org.

[20] Giusti, E. B., Cavalieri and the Theory of Indivisibles. Cremonese, Roma, 1980.

[21] Gottwald, S., A Treatise on Many-Valued Logics, Studies in Logic and Computation, Research Studies Press Ltd. Hertfordshire, England, 2001.

[22] Hailperin, T., Boole's Logic and Probability: A Critical Exposititon from the Standpoint of Contemporary Algebra, Logic, and Probability Theory. North-Holland Studies In Logic and the Foundations Of Mathematics, 1986.

[23] Lloyd, G., Finite and infinite in Greece and China. *Chinese Science* 13, pp. 11–34, 1996.

[24] MacHale, D., George Boole: His Life and Work. Boole Press, 1985.

[25] Mates, B., Stoic Logic. University of California Press, Berkeley, CA, 1953.

[26] Martzloff, J.-C., A History of Chinese Mathematics, Springer-Verlag, Berlin, 1997.

[27] Roy, R., The discovery of the series formula for π by Leibniz, Gregory and Nilakantha. *Mathematics Magazine* 63(5):291–306, 1990.

[28] Schroeder, M., A brief history of the notation of Boole's algebra. *Nordic Journal of Philosophical Logic* 2(1):41–62, 1997.

[29] Schröder, E., Vorlesungen über die Algebra der Logik (exakte Logik).vol. 2, pt1., B. G. Teubner, Leipzig, 1891 (reprinted by Chelsea, New York, 1966).

[30] Stone, M. H., The theory of representations for boolean algebras. *Trans. of the Amer.Math. Soc.*, 40, 37–111, 1936.

[31] Styazhkin, M., I. History of Mathematical Logic from Leibniz to Peano, Cambridge: The M.I.T. Press, 1969.

[32] Wu,J.-Z., Tan, H.-Y., Li, Y., An algebraic method to decide the deduction problem in many-valued logics. *Journal of Applied Non-Classical Logics* 8(4) 1998, pp. 353–60.

[33] Weyl, H., God and the Universe:The Open World, Yale University Press, 1932. Reprinted as "The Open World" by Ox Bow Press, 1989.

[34] Zhegalkin, I. I., O tekhnyke vychyslenyi predlozhenyi v symbolytscheskoi logykye (On a technique of evaluation of propositions in symbolic logic). *Matematicheskii Sbornik* 34(1):9–28, 1927 (in Russian).