Formal polynomials, heuristics and proofs in logic

W. Carnielli

abstract. This note surveys some previous results on the role of formal polynomials as a representation method for logical derivation in classical and non-classical logics, emphasizing many-valued logics, paraconsistent logics and modal logics. It also discusses the potentialities of formal polynomials as heuristic devices in logic and for expressing certain meta-logical properties, as well as pointing to some promising generalizations towards algebraic geometry.

Keywords: formal polynomials, algebraic proof procedures, heuristics in logical proofs, many-valued logics, modal logics

1 Formal polynomials as algebraic proof procedures: a brief survey

Algebraic proof systems based on formal polynomials over algebraically closed fields (the "polynomial ring calculus") were introduced in [7] (see also [8] and [9]). However, the Russian mathematician Ivan Ivanovich Zhegalkin had already proposed in 1927 a method (cf. [26]) to translate and decide propositions from A. Whitehead and B. Russell's *Principia Mathematica* by means of polynomials with coefficients in the two-element field $\mathbf{Z}_2$; some intuitions in the same direction can be found in the work of the Russian/Ukrainian logician Platon Sergeevich Poretskij (cf. [3]).

In the development of [7], [8] and [9] sentences are identified as multivariable polynomials in the ring $GF_{p^n}[X]$ of polynomials with coefficients in the Galois field of order p^n, and propositional derivability is reduced to checking whether or not certain families of polynomials have zeros (reading truth-values as elements of the field). In this way, questions of satisfiability can be related to the Hilbert's Nullstellensatz (cf. for instance, [25])), a well-known result of algebraic geometry that asserts in general for F an algebraically

closed field and $f, g_1, \ldots, g_m$ multivariable polynomials in $F[X]$, that f has a common zero with $g_1, \ldots, g_m$ iff there is an integer k and polynomials $h_1, \ldots, h_m \in F[X]$ so that $f^k = \sum_{1 \leq i \leq n} h_i \cdot g_i$. A discussion and more details on how the uses of such fundamental results are related to obtaining proofs in many-valued logics can be found in [8] and [9].

The above mentioning of algebraic geometry is not fortuitous. Actually, commutative algebra and algebraic geometry may be the right setting to couple logic and pure mathematics. As it is well known, distinct algebraic varieties (in particular, classes of lattices) are coupled with distinct logics. Paradigmatic cases are Boolean algebras (associated to classical propositional logic) and Heyting algebras (associated to Intuitionistic Logic). Although we are using only Boolean rings (defined as polynomial rings based upon finite fields, as it will be clear in the following) where the identity $x^n = x$ is pivotal, we could naturally think about dropping this law, working with commutative rings in general.

Formal polynomials as algebraic proof procedures revamp the idea of using algebraic methods to deal with proofs, already implicit in the work of Gottfried Wilhelm von Leibniz, George Boole, Augustus De Morgan, Charles Sanders Peirce, Ernst Schröder, David Hilbert and Alfred Tarski, just to mention some important predecessors. It is interesting to recall that we owe De Morgan in [15] a century-old pioneering remark that logical conjunction is just a particular case of composition of binary relations, a topic further developed as a full study of relation algebras by Tarski.

There is also a more recent idea of using this machinery to investigate proof complexity by means of the so-called Gröbner basis (cf. [14]), but this is surely no more than scratching the surface of the potentialities of algebraic methods in proofs (complexity among them).

Polynomial ring calculus are particularly appropriate for automatic proof systems not only for finitely many-valued logics, but also for non-truth-functional logics, including modal logics (cf. [1]): even logics that have no finite-valued characteristic semantics, as the paraconsistent logics, can be given a two-valued dyadic semantics expressed by multivariable polynomials over the ring $Z_2[X]$.

We survey below the basic ideas on polynomial ring calculus

(PRC) for (finitely) many-valued logics, following [7] and [8]. We suppose the logics to be explicitly given by means of a signature, designated truth-values, etc. (see [18]). All calculations are done within finite (Galois) fields, what is convenient in the case of p^n-valued logics, particularly to the most conspicuous three-, four-, and five-valued logics, considering that those are the overwhelming majority of many-valued logics in practice. It is simple to see, however, that for example 6-valued logics can be embedded into the next prime-valued logic, and treated in an analogous way.

Let F be any abelian ring (in most of the applications below, a finite field) with unity 1, and let 0 be the zero of F. Let $F[X]$ be the ring of all finite polynomials in the variables $x_1, x_2, \ldots, x_m, \ldots$ with arbitrary degree and characteristic p^n. A *polynomial ring proposition* for $\mathbb{L}$ is any polynomial $f \in F[X]$ on the variables $\vec{x}$; f is *satisfiable* if there exists a polynomial evaluation in F which produces $d \in D \subset F$ (denoted by $f(\vec{x}) = d$) where D is the set of designated truth-values of $\mathbb{L}$; see definition below). The notation is simplified to $f = d$, and $f \approx g$ means that $f = g$ for all evaluations in F. In particular, $f \approx d$ for $d \in F$ means, of course, that f coincides with the constant polynomial d.

The *ring rules* of PRC are the following for every $f, g, h \in F[X]$, $f + g \in F[X]$ and $f \cdot g \in F[X]$:

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. $f \cdot (g + h) \vdash_{\approx} f \cdot g + f \cdot h$

The letters $x, y, z, \ldots$ (with or without indices) are used as metavariables over variables, $f, g, h, \ldots$ as metavariables over polynomials.

The PRC based on F for $\mathbb{L}$ is defined in the following way:

1. Its terms are all variables, and its formulas are all polynomials of $F[X]$;

2. The bases are the ring rules plus the *polynomial rules* $p^n \cdot x = x + x + \ldots \vdash_{\approx} 0$(summing x exactly p^n times) and $x^i \cdot x^j \vdash_{\approx} x^k(\mathtt{mod}\ p(x))$ for $k \equiv i + j(\mathtt{mod}\ (p^n - 1))$ where $p(x)$ is a convenient primitive polynomial (i.e., an irreducible polynomial of degree n with coefficients in Z_p);

3. There are two inference (meta)rules, the Uniform Substitution (US): $f \vdash_{\approx} g/f[x:h] \vdash_{\approx} g[x:h]$ and the Leibnitz rule (LR): $f \vdash_{\approx} g/h[x:f] \vdash_{\approx} h[x:g]$ where $f[x:g]$ denotes the result of uniformly substituting g for the variable x in f.

The usual properties of the familiar consequence relations (as reflexivity, transitivity, etc.) follow from the (LR) properties.

If $\Delta \bigcup \{f\}$ is any collection of polynomial propositions, a derivation of f from Δ, denoted by $\Delta \vdash_{\approx} f$, is a finite sequence of (polynomial) formulas that are either in Δ or are obtained from previous terms through PRC rules; f is said to be a *theorem*, denoted by $\vdash_{\approx} f$, if $\emptyset \vdash_{\approx} f$.

Some concrete examples will be discussed below, and the following fact will be essential:

THEOREM 1. *Let p be a prime number; then there is an isomorphism between the set of all p^n-valued truth-functions of arity $\leq m$ and all the m-variable polynomials in GF(p^n)[X].*

Proof. By checking that each such polynomial defines a unique p^n-valued function in a field, and vice versa. ■

The preceding theorem can be strengthened to non-deterministic finite-valued functions as well (and this makes it possible to use polynomial functions with extra-variables to treat non-truth functional logics such as paraconsistent logics and modal logics, (cf. [8] and [1]). Moreover, for fixed p^n, there exists a polynomial-time transformation Π that outputs the corresponding polynomial of $GF_{p^n}[X]$ for each truth-function, as it can be computed by elementary linear algebra (systems of linear equations) over finite fields.

THEOREM 2. *Let f be a polynomial in $GF_{p^n}[X]$. Then $f \approx c$ for a constant c of $GF(p^n)$ if and only if $f \vdash_{\approx} c$ in PRC.*

Proof. Since the field $GF(p^n)$ is constructed as $GF(p^n) = Z_p[X]/ < p(x) >$ (that is, the quotient of the ring of all polynomials with

coefficients in Z_p by the ring ideal $< q(x) >$ generated by an irreducible polynomial $q(x)$), application of the PRC procedures to polynomials f in $GF_{p^n}[X]$ obtains a class representative of f in $GF_{p^n}[X]$ modulo $q(x)$ with minimum degree (note that the polynomial rules always decrease degrees). If $f \approx c$, then f is equivalent to the constant polynomial c and a finite number of PRC steps will end up with c. ■

The above theorems guarantee a completeness theorem with respect to PRC for p^n-valued logics. Let $\mathbb{L}$ be a p^n-valued logic (for p a prime number) and let D be the set of distinguished truth-values of $\mathbb{L}$. Actually, easy constructions (all well-known in the literature) obtain finite fields with 4, 8 and 9 elements (namely, $GF(2^2)$, $GF(2^3)$ and $GF(3^2)$). Indeed, in the above indicated construction $GF_{p^n}[X] = Z_p[X]/ < q(x) >$, x^2+x+1 is the only irreducible monic quadratic polynomial in $Z_2[x]$, which gives for $GF(2^2)$ in a unique way (this case is exemplified in more details for four-valued logics in Section 2).

For the case of 8 truth-values: the irreducible cubics in $Z_2[X]$ are just $x^3 + x + 1$ and $x^3 + x^2 + 1$, and both define isomorphic finite fields with 8 elements (viz., $GF(2^3)$). For the last case, concerning 9 truth-values, $x^2 + 1$, $x^2 + x + 2$ and $x^2 + 2x + 2$ are the only irreducible monic quadratic polynomials in $Z_3[X]$, and all of them produce isomorphic finite fields with 9 elements (viz., $GF(3^2)$).

We thus have a direct treatment of all finite-valued logics from 2 to 9 truth-values (with the exception of 6) in terms of polynomial ring calculus, independent of which truth-values (or how many of them) are taken as distinguished values. Since a 6-valued logic can be embedded in $Z_7[X]$, this virtually covers all cases of finitely many-valued logics with any pragmatic interest in the literature.

Moreover, since $GF(p^m)$ is a subfield of $GF(p^n)$ iff m divides n (another well-known elementary fact about Galois fields), then of course classical propositional logic can be entirely embedded into four-valued logic, a possibility which can make a difference when investigating complexity of proof procedures (cf. also Section 5).

Let $At = \{p_1, p_2, \ldots\}$ be a denumerable set of *atomic sentences*, and let $\Sigma = \{\Sigma_n\}_{n\in\mathbb{N}}$ be a *propositional signature*, where each Σ_n is a set of *connectives* of arity n, which defines the set $Con = \bigcup_{n\in\mathbb{N}} \Sigma_n$ be the set of connectives. The set of formulas of $\mathbb{L}$ is then defined

as the freely generated algebra by At over Σ. Thus, $p_k \in \mathbb{L}$, for any atomic sentence $p_k \in At$, and $\otimes(\varphi_1, \ldots, \varphi_m) \in \mathbb{L}$, for any m-ary connective $\otimes \in Con$, and any formulas $\varphi_1, \ldots, \varphi_m \in \mathbb{L}$.

Given a usual matrix interpretation to $\mathbb{L}$, which we call a *semantics* Sem for $\mathbb{L}$, denote by v the valuations from the formulas of $\mathbb{L}$ to $GF(p^n)$; a canonical *consequence relation* $\Vdash \subseteq \wp(\mathbb{L}) \times \mathbb{L}$ associated to Sem is defined by establishing that a formula $\varphi \in \mathbb{L}$ *follows from* a set of formulas $\Gamma \subseteq \mathbb{L}$ whenever $v(\Gamma) \in D$ implies that $v(\varphi) \in D$.

The above notion of consequence relation complies to what is known as a *Tarskian* logic. We can also suppose with no loss of generality that $\mathbb{L}$ is also compact, so $\Gamma \subseteq \mathbb{L}$ can be taken as finite.

THEOREM 3. *Let* $\Gamma = \{\gamma_1, \ldots, \gamma_n\}, \varphi$ *be a set of formulas of* $\mathbb{L}$*;*

$\Gamma \Vdash \varphi$ *iff there is an integer* k *and polynomials* $h_1, \ldots, h_m \in F[X]$ *such that* $f^k = \sum_{1 \leq i \leq n} h_i \cdot g_i$*, where* $f = \Pi(\varphi) - c, g_1 = \Pi(\gamma_1) - d_1, \ldots, g_n = \Pi(\gamma_n) - d_n$ *for truth-values* $d_1, \ldots, d_n \in D$ *and* $c \notin D$*.*

Proof. By the Nullstellensatz for arbitrary fields, $\Gamma \Vdash \varphi$ iff the polynomials $f = \Pi(\varphi) - c, g_1 = \Pi(\gamma_1) - d_1, \ldots, g_n = \Pi(\gamma_n) - d_n$ have a common zero. ■

The previous theorem grants a refutation proof method to many-valued logics based on the Nullstellensatz, in a way similar to the mentioned Gröbner calculus. Cases of special interest arise when the logic $\mathbb{L}$ is endowed with a connective, which we call $\circledast$, such that the Metatheorem of Deduction holds for $\mathbb{L}$. In this case, $\Gamma, \alpha \Vdash \varphi$ iff $\Gamma \Vdash \circledast(\alpha, \varphi)$. If this is the case, the procedure can be iterated,and in general $\Gamma \Vdash \varphi$ iff there exists a formula ψ such that $\Vdash \psi$, where ψ is construed from the formulas of Γ and the connective $\circledast$.

2 Example-cases: Post and Łukasiewicz logics in polynomial format

Although the idea of many-valued logics was present in the work of Charles Peirce already in the first decade of the 20th century (cf. [17]), Emil Post introduced in 1920 the first well-worked many-valued logical systems almost simultaneously (but independently) from Łukasiewicz. The primitive operators negation $\neg$ and disjunction $\vee$ introduced by Post are related to the fundamental operators of *Principia Mathematica*, and are defined as the following operations over Z_n, where $n-1$ is the only distinguished truth-value: $\neg(x) =$

$x+1(\mathtt{mod}\ n)$ and $x \vee y = max\{x, y\}$. Without any loss of generality we can consider an isomorphic variant of Post's system through the following operations over Z_n, where now 0 is the only distinguished truth-value: $\neg(x) = x + n - 1$ and $x \vee y = min\{x, y\}$. It is now easy to compute, for each p^n, two polynomials corresponding to $\neg$ and $\vee$. For example, for $n = 3$ the following polynomials over $Z_3[X]$ represent $\neg$ and $\vee$: $\neg(x) = x + 2$ and $x \vee y = min\{x, y\} = 2x2y2 + 2x^2y + 2xy^2 + xy$. Since any other formula in the many-valued Post logic can be written in terms of $\neg$ and $\vee$ (i.e, they form a functionally complete set of connectives) any other 3-valued function in one or two variables can be written as composition of these. A similar result holds for all p^n-valued logics.

Since Post's logics are functionally complete and the Deduction Metatheorem holds for them, provability in p^n-valued Post's logics can be directly treated via PRC proof theory. Here the polynomial rules reduce to $3 \cdot x \approx 0$ and $x^3 \approx x$, since we are dealing with the simple case $p = 3, n = 1$ and PRC reduces to simplifying polynomials in $Z_3[X]$.

Łukasiewicz's three-valued system L_3 is sound and complete with respect to the well-known matrices for $\rightarrow$ and $\neg$ (where 2,1,0 are used instead of the more common 1, 1/2 and 0, and 0 is the only designated truth-value). In polynomial form over the ring $Z_3[X]$ the corresponding connectives are expressed by: $x \rightarrow y = 2x(y+1)(xy+y+1)$ and $\neg(x) = 2x$.

Since Łukasiewicz's logic enjoys a form of Metatheorem of Deduction, the procedure also applies directly. As a simple example, $x \rightarrow x = 2x(x+1)(x^2+x+1) = 2x^4+4x^3+4x^2+2x$. Using the polynomial rules $3 \cdot x \approx 0$ and $x^3 \approx x$, we obtain immediately: $x \rightarrow x \approx 2x^4+4x^3+4x^2+2x \approx 2x^2+x+x^2+2x \approx 3x^2+3x \approx 0$. Hence, $\alpha \rightarrow \alpha$ is a theorem in the system L_3. The method is obviously also useful as a decision procedure (it is clear that any logic characterizable through polynomial calculus are recursively decidable).

Analogous results hold for all p^n-valued logics. As hinted in the previous section, four-valued logics, for example, can be easily dealt with by means of polynomials over $GF(4)$ (notice that we cannot use the ring $Z_4[X]$, which fails to be a unique factorization domain and in this cannot represent all four-valued connectives: for instance is is easy to see that a connective such as $x \vee y = max\{x, y\}$ is not

representable as a polynomial in $Z_4[X]$. The field $GF(4)$ can be defined (as previously remarked) as an extension field of $GF(2)$ by means of the primitive polynomial $q(x) = x^2 + x + 1$ of degree 2 in $Z_2[X]$, and by taking the successive powers of the roots of $p(x)$ to represent the non-zero elements in $GF(4$ as $\{0, 1, a, a^2 = a + 1\}$, on which addition and multiplication are defined as:

$+$	0	1	a	a^2
0	0	1	a	a^2
1	1	0	a^2	a
a	a	a^2	0	1
a^2	a^2	a	1	0

$\cdot$	0	1	a	a^2
0	0	0	0	0
1	0	1	a	a^2
a	0	a	a^2	1
a^2	0	a^2	1	a

Using polynomials with coefficients in $GF(4)$ and computing according to such tables, one can of course characterize *any* four-valued logic in the literature (and even the ones not yet invented).

For the particular case $n = 2$, n-valued Post logic reduces to classical propositional calculus. It is simpler to give a direct formulation, translating the usual boolean connectives as follows: Let $At = \{p_1, p_2, \ldots\}$ be the atomic sentences of PC, and $\neg, \vee, \wedge, \rightarrow$ the usual connectives. The translation Π is set as follows:

1. $\Pi(p_i) := x_1$
2. $\Pi(\varphi) := 1 + \Pi(\varphi)$
3. $\Pi(\varphi \wedge \psi) := \Pi(\varphi) \cdot \Pi(\psi)$
4. $\Pi(\varphi \vee \psi) := \Pi(\varphi) \cdot \Pi(\psi) + \Pi(\varphi) + \Pi(\psi) + 1$
5. $\Pi(\varphi \rightarrow \psi) := \Pi(\varphi) \cdot \Pi(\psi) + \Pi(\varphi) + 1$

The polynomial rules over $Z_2[X]$ in this case reduce to $x + x \vdash_{\approx} 0$ and $x \cdot x \vdash_{\approx} x$. As a consequence, φ is a PC-tautology iff $\Pi(\varphi) \vdash_{\approx} 1$. We thus obtain a promising method for checking the satisfiability problem for many-valued logics (in particular for SAT), since the reductions performed by the polynomial ring calculus might be subexponential in the number of variables of a propositional formula.

3 The heuristic stand: half-logics, quarter-logics and the laws of form

Logicians should not overlook what poets have to say: a four-line poem by Samuel Butler in the mid-19th century (cf. [5]) expresses a philosophy of heuristics better than some treatises:

All the inventions that the world contains
Were not by reason first found out, nor brains
But pass for theirs, who had the luck to light
Upon them by mistake or oversight.

But how can heuristic insights be considered along with the act of proving? Modern logicians virtually killed heuristics: indeed, the contemporary notion of proof completely expels the role of discovery and heuristics. Considering that problem solving and the heuristic method have been emphasized by some notable mathematicians, most of them Hungarians as George Pólya (famous references are [21] and [22]), there is no principled reason heuristic methods could not be shared by logicians. They were indeed shared by Greek geometers and philosophers as Euclid (circa 325-270 BC), Pappus (290-350) and Proclus (410-485), a tradition continued by Descartes and Leibniz. Discovery in logic is of course completely independent from whether there may be a logic of discovery[1], and I argue here that formal polynomials work in a quite remarkable way as a heuristic tool in logic. Two examples are reviewed below: the discovery of quarter-logics (as a generalization of half-logics) and the discovery of an appropriate formalism to express some ideas on the so-called "laws of form".

Classical implication $\rightarrow$ and negation $\sim$ are truth-functional connectives completely characterized by the familiar two-valued valuations v:

$$v(P \rightarrow Q) = 1 \text{ iff } v(P) = 0 \text{ or } v(Q) = 1 \text{ and } v(\sim P) = 0 \text{ iff } v(P) = 1$$

Non-truth-functional connectives, however, are abundant in the literature. Béziau in [4] defined a partial (non-truth-functional) negation $\neg_1$ characterized by:

$$v(\neg_1 P) = 0 \text{ if } v(P) = 1$$

[1] If there is, it would perhaps be an *algebra* of discovery rather than a logic of discovery; incidentally, this was a topics I was strongly interested in my Ph.D thesis, which I later decided to do in pure logic instead.

Albeit its non-truth-functional character, the negation $\neg_1$ is defined via a process of *bounded non-determinism* in the sense that $v(\neg_1 P) \in \{0,1\}$ if $v(P) = 0$, i.e., there are no truth-value gaps. As remarked, every finite-valued defined by a bounded non-deterministic definition can be represented by polynomial functions over Galois fields $GF_{p^n}[X]$ with extra (hidden) variables (cf. [8]).

Due to its bounded non-truth functionality, $\neg_1 P$ can is representable as a simple polynomial over $Z_2[X]$ with an extra variable x. Indeed, the "half " negation $\neg_1 P$ is computable by $x \cdot (p+1)$ and easily recovers classical negation with the help of $\rightarrow$: in polynomial format, $P \rightarrow \neg_1 P$ is computed as $p \cdot (x \cdot (p+1)) + p + 1 = p + 1$, but $p + 1$ represents $\sim$.

This was noted in [4] with the suggestion that it could be regarded as a certain "translation paradox" in the sense that PC can be strongly translated within a certain subclassical logic $K/2$ (in the language $\{\rightarrow, \neg_1\}$). The translation τ in question is:

1. $\tau(P) = P$, for P atomic;
2. $\tau(A \rightarrow B) = \tau(A) \rightarrow \tau(B)$;
3. $\tau(\sim A) = A \rightarrow \neg_1 A$.

Although this "phenomenon" deserved a paper by L. Humberstone (cf. [19]), our polynomial computation shows that this is nothing more than a mere consequence of function compositionality: $\sim$ belongs to the clone defined by $\rightarrow$ and $\neg_1$. Indeed, additional "half-logics" can be defined just by playing with polynomials, as for instance:

$$v(\neg_2 P) = 1 \text{ if } v(P) = 0$$

In polynomial terms $\neg_2 p$ is expressed by $p \cdot x + 1$ (when $p = 0$, $\neg_2 p = 1$, but when $p = 1$, then $\neg_2 p$ is undetermined)

Now consider a connective $P \overset{*}{\leftarrow} Q$ semantically defined in the polynomial form as $p \cdot (q+1)$; this expresses semantically the connective:

$$v(P \leftarrow Q) = 1 \text{ iff } v(P) = 1 \text{ and } v(Q) = 0$$

It is easy to see that $\neg_2$ and $\leftarrow$ define classical negation $\sim$ by $\neg_2(P) \overset{*}{\leftarrow} P$, computed as $(p \cdot x + 1) \cdot (p+1) = (p+1) \cdot p \cdot x + (p+1) = p + 1$.

Not only new half-logics, but also quarter-logics can be invented. Consider a binary connective semantically defined in p and q by $x \cdot (p+1) \cdot q$, corresponding to a non-truth-functional connective $\rightharpoonup$ whose valuation condition is:

$$v(P \rightharpoonup Q) = 0 \text{ if } v(P) = 1 \text{ or } v(Q) = 0$$

Consider a logic $K/4$ in the signature $\{\rightarrow, \rightharpoonup\}$.

This quarter logic recovers itself; indeed, classical negation $\sim$ can be defined by:

$$P \rightarrow (P \rightharpoonup Q)$$

In polynomial format this is computed as $p \cdot (x \cdot (p+1) \cdot q) + p + 1 = p + 1$, hence full PC is recovered in the signature $\{\rightarrow, \rightharpoonup, \sim\}$.

More quarter-logics can be defined, now departing from $x \cdot p \cdot (q+1)$, corresponding to $\rightharpoondown$ whose clause for valuation is:

$$v(P \rightharpoondown Q) = 0 \text{ if } v(P) = 0 \text{ or } v(Q) = 1$$

Consider now $K'/4$ in the signature $\{\rightarrow, \rightharpoondown\}$); classical negation $\sim$ is now definable by:

$$Q \rightarrow (P \rightharpoondown Q)$$

and again full PC is recovered in $\{\rightarrow, \rightharpoondown, \sim\}$.

It is not difficult to be convinced that there is a lot of other "paradoxical" connectives: at least 16 binary connectives can be defined as a basis for such "quarter" logics, and many more in other arities. Exploring this aspect of non-truth-functional connectives is more than performing a clever algebraic trick; it is a contribution to understanding which are the laws of logical form.

Another interesting application of the expressivity of formal polynomials as heuristic devices is in the analysis of the so-called "laws of form". In a booklet of 1969 (cf. [24]) George Spencer-Brown attempted to formalize what he thought to be "the laws of form" by means of a sort of exoteric calculus, praised by Bertrand Russell as "a new calculus of great power and simplicity". The idea, with its proposal of starting from nothing and drawing a distinction, has some connections with Brower's "two-oneness", which he considered to be the basal intuition of mathematics. It has also some remarkable

coincidences with C. Peirce's "alpha-existential graphs"; indeed, Peirce's "streamer" is like Spencer Brown's symbol ⌐. It was proven in [2] that part of Spencer-Brown's system for the "laws of form" (namely, his so-called "primary algebra") is just Boolean algebra in disguise. However, the same proof can be obtained in a much simpler way by interpreting Spencer-Brown's symbology as polynomials over boolean rings, as shown in [6].

4 Modal logics in polynomial format

In [1] a polynomial ring calculus (PRC) for the familiar modal logic **S5** was designed, which permits to perform modal deductions through polynomial handling. The paper also investigated the relationships among the PRC here defined, the algebraic semantics for modal logics, equational logics and the Dijkstra-Scholten equational-proof style. The method proposed can be easily extended to other modal logics.

The definition of PRC for **S5** can be easily adapted to other modal logics: for the systems **K**, **T**, **B** and **S4** it is only necessary to adjust certain polynomial constraints corresponding to axioms in the respective system. In particular, the polynomial representation of provability for **S4** can be immediately extended to intuitionist logic **Int**, due to the well-known Gödel's embedding of **Int** into **S4**.

These extensions can be done without much ado by considering the well-known Lemmon-Scott axioms for modal logics. Moreover, a relationship with their respective modal algebras can also be obtained: new polynomial constraints will correspond to algebraic conditions over operators.

A PRC for **S4** has an extra interest, as this means that intuitionistic logic can in principle be also treated in polynomial terms (bearing in mind the well-known correspondence between **S4** and the propositional intuitionistic calculus). Issues on decidability of modal logics can also be treated through polynomials: this is, for instance, immediate for **S5**, although for other calculi connections with the finite-model property would have to be established.

The PRC for modal logics is also related to the *non-deterministic matrices*, a generalization of ordinary multi-valued matrices, in which the truth-value of a formula can be non-deterministically assigned: actually, the methods in [1] constitute the first example

of non-deterministic semantics for modal logics. It constitutes also a particular case of *possible-translations semantics* (see, e.g. [11]) — not by accident, since the latter are more expressive than the former, as proven in [12] (Theorem 38 and the following discussion).

5 Expectations concerning heuristics and complexity

Boole's "algebra of logic", re-shaped by E. Schröder and later subsumed in the propositional and predicate calculus (cf. [20]), is not coincident with Boolean algebra; indeed, the "algebra of logic" is more a commutative ring with unity, partly because Boole's disjunction was exclusive (instead of contemporary exclusive "or"). The use of formal polynomials in logic sharply expresses such a distinction between Boole's algebra and Boolean algebra. In this sense, the real "algebra of logic" would be the one which approaches itself towards algebraic geometry, as exemplified by our discussion above concerning the Hilbert's Nullstellensatz.

To gain full access to algebraic geometry, however, logics represented by infinite fields seem to be more appropriate than the ones restricted to finite fields. So, for instance, as shown in [13], there are some limitations for expressing certain metamathematical properties of logics by means of polynomials over finite fields: Craig Interpolation Lemma, for example, cannot be proven directly by manipulating polynomials over finite fields. Some challenging open problems are to represent infinite-valued Łukasiewicz logics, full first-order logic and higher-order logics by means of polynomials over GF_{p^n} (in such cases,polynomials over the field of rational numbers $\mathbb{Q}$ seem to be more adequate).

The ring $GF_{p^n}[X]$ of polynomials with coefficients in the Galois field of order p^n, which is used in the polynomial ring calculus for many-valued logics, paraconsistent logics and modal logics, share strikingly similar properties with the commutative ring $\mathbf{Z}$ of the integer numbers. Indeed, both are unique factorization domains, and they have very accordant number theories: the prime numbers of $\mathbf{Z}$ correspond to monic irreducible polynomials in $GF_{p^n}[x]$, the ring of polynomials in one variable x (several interesting consequences of this similarity are discussed in [16]).

This makes the polynomial ring calculus a kind of abstract number theory, with promising consequences for logical consequence: as

noted in [16]) (pages 28 and 29), irreducibility testing in $GF_{p^n}[x]$ seems to be more tractable than primality test in $\mathbf{Z}$, and the problem of factorization for polynomials seems to be, equally, more tractable than factorization for integers. So there is hope that treating logics by means of formal polynomials *might* lead to some new insights regarding complexity of theorem-proving procedures.

Independently from issues on complexity and from any relevant connections to algebraic geometry and to the problems found therein, the polynomial formatting of logics has another tantalizing feature: by using the powerful representation given by polynomials we not only shape new proof methods, but we come upon one of the very few heuristic artifacts in logic. In this direction, as well, there is much to be explored.

References

[1] *Agudelo, J. C. and Carnielli, W. A.* Polynomial ring calculus for modal logics: a new semantics and proof method for modalities. Pre-print available at *CLE e-Prints* 9(4), 2009, at `http://www.cle.unicamp.br/e-prints/vol_9,n_4,2009.html`.

[2] *Banaschewski, B.* On G. Spencer Brown's Laws of Form. *Notre Dame Journal of Formal Logic* 18(3):507-509, 1977.

[3] *Bazhanov, V. A.* New archival materials concerning P. S. Poretskij. *Modern Logic* 3(1) pp. 80-81, 1992.

[4] *Béziau, J.-Y.* Classical negation can be expressed by one of its halves. *Logic Journal of IGPL* 7(2):145-151, 1999.

[5] *Butler, S.* Miscellaneous Thoughts, in: The Poems of Samuel Butler, Vol. II. (Chiswick: C. Willingham, 1822), p. 281

[6] *Carnielli, W. A.* Formal polynomials and the laws of form. In "The Multiple Dimensions of Logic", Coleзro CLE volume 54, UNICAMP, Brazil (Eds. Jean-Yves Béziau and Alexandre Costa-Leite), pp. 202-212, 2009.

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

[8] *Carnielli, W. A.* Polynomial ring calculus for many-valued logics. Proceedings of the 35th International Symposium on Multiple-Valued Logic. IEEE Computer Society. Calgary, Canada. IEEE Computer Society, pp. 20-25, 2005. Pre-print available at *CLE e-Prints* 6(3), 2006, at `http://www.cle.unicamp.br/e-prints/vol_6,n_3,2006.html`.

[9] *Carnielli, W. A.* Polynomizing: Logic inference in polynomial format and the legacy of Boole. In: Model-Based Reasoning in Science, Technology, and Medicine (Editors, L. Magnani and P. Li). Series "Studies in Computational Intelligence", volume 64, pp. 349-364. Springer Berlin-Heidelberg, 2007. Pre-print available under the title "Polynomial ring calculus for logical inference" at *CLE e-Prints* 5(3), 2005, at `http://www.cle.unicamp.br/e-prints/vol_5,n_3,2005.html`.

[10] *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.

[11] *Carnielli, W. A., Coniglio, M. E. and Marcos, J.* Logics of formal inconsistency. In D. Gabbay and F. Guenthner, editors, Handbook of Philosophical Logic, volume

14, pages 15–107. Springer, 2nd edition, 2007. Preprint available from *CLE e-Prints* 5(1), 2005 at `http://www.cle.unicamp.br/e-prints/vol5,n1,2005.html`.

[12] *Carnielli, W. A. and Coniglio, M. E.* Splitting Logics. In "We Will Show Them! Essays in Honour of Dov Gabbay" pages 389–414. College Publications, 2005.

[13] *Carolino, P. K.* Polinomization of Logics: Problems and Perpscrives. Master Dissertation (in Portuguese). IFCH- UNICAMP, Campinas, SP, Brazil, 2009.

[14] *Clegg, M., Edmonds, J., and R. Impagliazzo, R.* Using the Gröbner basis algorithm to find proofs of unsatisfiability. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, pages 174-183, Philadelphia, PA, May 1996.

[15] *De Morgan, A.* On the syllogism, no. IV, and on the logic of relations. *Trans. Cambridge Philosophical Soc* 10:331-358, 1860.

[16] *Effinger, G., Hicks, K, and Mullen, G. L.* Integers and polynomails: comparing the close cousins $\mathbf{Z}$ and $F_q[x]$. *The Mathematical Intelligencer* 27(2):26-34, 2005.

[17] *Fisch, M. and Turquette, A.* Peirce's Triadic Logic. *Transactions of the Charles S. Peirce Society* 11:71-85, 1966.

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

[19] *Humberstone, L.* Béziau's translation paradox. *Theoria* 71:138-18, 2005.

[20] *Kneebone, G.T.* Mathematical Logic and the Foundation of Mathematics: An introductory Survey. Courier Dover Publications, 2001.

[21] *Pólya, G.* How to Solve It: A New Aspect of Mathematical Method. Princeton, NJ: Princeton University Press, 1945.

[22] *Pólya, G.* Mathematical discovery: on understanding, learning, and teaching problem solving. New York, NY: John Wiley and Sons, Inc., 1981

[23] *Paturi, R., Pudlбk, P., Saks, M. and Zane, F.* An improved exponential time algorithm for k-sat. Annual IEEE Symposium on Foundations of Computer Sience, 1998.

[24] *Spencer-Brown, G.* The Laws of Form. Allen & Unwin, London, 1969.

[25] *van der Waerden, B. L.* Modern Algebra, Julius Springer, Berlin, 1931.

[26] *Zhegalkin, I. I.* On the Technique of Calculating Propositions in Symbolic Logic. *Matematicheskii Sbornik* 43: 9–28, 1927.