Formal polynomials and the laws of form

Walter Carnielli
Centre for Logic and Epistemology and the History of Science- CLE
UNICAMP
P.O. Box 6133, 13081-970
Campinas, SP, Brazil
walter.carnielli@cle.unicamp.br

Abstract

This paper discusses the role of formal polynomials as a representation method for logical derivation, as well as their potentialities for expressing certain meta-logical properties and as heuristic devices. We treat as example-cases two intriguing episodes in logical folklore: the 'laws of form' of Spencer-Brown and the 'paradoxes of half -logics' of J.-Y. Béziau.

Keywords: algebraic proof systems, polynomial proof systems, laws of form, half-logics, quarter-logics.

1 Formal polynomials as algebraic proof procedures: a brief survey

Algebraic proof systems based on formal polynomials over finite fields (the “polynomial ring calculus”) were introduced in [Car01] (see also [Car05] and [Car07]). 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 will be related to the Hilbert’s Nullstellensatz (cf. for instance, [vdW31]), 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 result are related to obtaining proofs in many-valued logics can be found in [Car05] and [Car07].

Formal polynomials as algebraic proof procedures revamp the idea of using algebraic methods to obtain proofs, already implicit in Leibniz, Boole, and Hilbert, just to mention distinguished company, but there is also a more recent
idea of using this machinery to investigating proof complexity by means of the
so-called Gröbner basis (cf. [CEI96]).

Polynomial ring calculus are an interesting candidate for automatic proof
systems not only for finitely many-valued logics, but also for non-truth-functional
logics, including modal logics (cf. [AC]): even logics that have no finite-valued
characrisitic semantics, as the paraconsistent logics, can be given a two-valued
dyadic semantics expressed by multivariable polynomials over the ring \( \mathbb{Z}_2[X] \).

A short survey of the polynomial ring calculus (PRC) for \( p^n \)-valued logics
\( L \) is given below, closely following [Car01] and [Car05]. We suppose the log-
ics explicitly given by means of a signature, designated truth-values, etc. (see
[Got01]). All calculations are done within finite (Galois) fields, what is con-
venient in the case of three-, four-, and five-valued logics, which are the over-
whelming majority of logics considered 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 0 be the zero of \( F \). Let \( F[X] \) be the ring of all finite polyno-
mials in the variables \( x_1, x_2, \ldots, x_m, \ldots \) with arbitrary degree and characteristic
\( p^n \). A polynomial ring proposition for \( L \) 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 \( L \); 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 \( d \in F \) 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. \( f + (g + h) \vdash (f + g) + h \)
2. \( f + g \vdash g + f \)
3. \( f + 0 \vdash f \)
4. \( f + (-f) \vdash 0 \)
5. \( f \cdot (g \cdot h) \vdash (f \cdot g) \cdot h \)
6. \( f \cdot (g + h) \vdash f \cdot g + f \cdot h \)

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 \( L \) 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 \( p^n \cdot x = x + x + \ldots \vdash 0 \) (summing \( x \) exactly \( p^n \) times) and \( x^i \cdot x^j \vdash x^k \) (mod \( p(x) \)) for
   \( k \equiv i + j \mod (p^n - 1) \) 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 (LR) properties.

If \( \Delta \cup \{ f \} \) is any collection of polynomial propositions, a derivation of \( f \) from \( \Delta \), denoted by \( \Delta \vdash \approx f \), is a finite sequence of (polynomial) formulas that are either in \( \Delta \) 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 1.1.** 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 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. [Car05] and [AC]). Moreover, for fixed \( p^n \), there exists a polynomial-time transformation \( \Pi \) 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 1.2.** 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 \( <p(x)> \) generated by \( p(x) \)), application of the PRC procedures to polynomials \( f \) in \( GF(p^n)[X] \) obtain a class representative of \( f \) in \( GF(p^n)[X] \) modulo \( p(x) \) 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 \( L \) be a \( p^n \)-valued logic (for \( p \) a prime number) and let \( D \) be the set of distinguished truth-values of \( L \).

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 \( \Sigma_n \) 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 \( L \) is then defined as the freely generated algebra by \( At \) over
Let $\Sigma$. 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 $\text{Sem}$ for $\mathbb{L}$, denote by $v$ the valuations from the formulas of $\mathbb{L}$ to $\mathbb{GF}(p^n)$: a canonical consequence relation $\vdash \subseteq \mathbb{L} \times \mathbb{L}$ associated to $\text{Sem}$ 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 1.3.** 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 $h_1, \ldots, h_m \in \mathbb{F}[X]$ 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. \(\square\)

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 $\otimes$, such that the Metatheorem of Deduction holds for $\mathbb{L}$. In this case, $\Gamma, \alpha \vdash \varphi$ iff $\Gamma \vdash \otimes(\alpha, \varphi)$. If this is the case, the procedure can be iterated, and in general $\Gamma \vdash \varphi$ iff there exists a formula $\psi$ such that $\vdash \psi$, where $\psi$ is construed from the formulas of $\Gamma$ and the connective $\otimes$.

## 2 Notable example-cases: Post logics and Łukasiewicz logics in polynomial form

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. [FT]), Emil Post introduced in 1920 the first well-worked many-valued logical systems almost simultaneously (but independently) of Łukasiewicz. The primitive operators negation $\neg$ and disjunction $\lor$ introduced by Post are related to the fundamental operators of *Principia Mathematica*, and are defined as the following operations over $\mathbb{Z}_n$, where $n = 1$ is the only distinguished truth-value: $\neg(x) = x + 1 \mod n$ and $x \lor y = \max\{x, y\}$. Without any loss of generality we can consider an isomorphic variant of Post’s system through the following operations over $\mathbb{Z}_n$, where now $0$ is the only distinguished truth-value: $\neg(x) = x + n - 1$ and $x \lor y = \min\{x, y\}$. It is now easy to compute, for each $p^n$, two polynomials corresponding to $\neg$ and $\lor$. For example, for $n = 3$ the following polynomials over $\mathbb{Z}_3[X]$ represent $\neg$ and $\lor$:

\[
\neg(x) = x + 2 \quad \text{and} \quad x \lor y = \min\{x, y\} = 2x2y2 + 2x^2y + 2xy^2 + xy.
\]

Because any other formula in the many-valued Post logic can be written in terms of $\neg$ and $\lor$ (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. An analogue 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 $\mathbb{Z}_3[X]$.

Lukasiewicz three-valued system $L_3$ is sound and complete with respect to the well-known matrices for $\to$ and $\neg$ (where 2, 1/2 and 0, and 0 is the only designated truth-value). In polynomial form over the ring $\mathbb{Z}_3[x, y]$ the corresponding connectives are: $x \to y = 2x(y + 1)(xy + y + 1)$ and $\neg(x) = 2x$.

Since Lukasiewicz logics enjoys a form of Metatheorem of Deduction, the procedure also applies directly. As a simple example, $x \to x = 2x(x + 1)(x^2 + x + 1) = 2x^4 + 4x^3 + 4x^2 + 2x$. Using the polynomial rules $3 \cdot x \approx 0$ and $x^3 \approx x$, we obtain immediately: $x \to x \approx 2x^4 + 4x^3 + 4x^2 + 2x \approx 2x^2 + x + x^2 + 2x \approx 3x^2 + 3x \approx 0$. Hence, $\alpha \to \alpha$ 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 by polynomial calculus are recursively decidable).

Analogue results hold for all $p^n$-valued logics. Four-valued logics, for example, can be dealt with by means of polynomials over $\mathbb{GF}(4)$. The field $\mathbb{GF}(4)$ can be defined as an extension field of $\mathbb{GF}(2)$ by means of the primitive polynomial $p(x) = 1 + x + x^2$ of degree 2 in $\mathbb{Z}_2[X]$, and by taking the successive powers of the roots of $p(x)$ to represent the non-zero elements in $\mathbb{GF}(4)$ as $\{0, 1, a, a^2 = a + 1\}$, on which addition and multiplication are defined as:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>a</th>
<th>a^2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>a</td>
<td>a^2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>a^2</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>a^2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>a^2</td>
<td>a^2</td>
<td>a</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>·</th>
<th>0</th>
<th>1</th>
<th>a</th>
<th>a^2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>a</td>
<td>a^2</td>
</tr>
<tr>
<td>a</td>
<td>0</td>
<td>a</td>
<td>a^2</td>
<td>1</td>
</tr>
<tr>
<td>a^2</td>
<td>0</td>
<td>a^2</td>
<td>1</td>
<td>a</td>
</tr>
</tbody>
</table>

Using polynomials with coefficients in $\mathbb{GF}(4)$ and computing according to such tables, one can of course characterize any four-valued logic in the literature (and 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 $\neg, \lor, \land, \to$ the usual connectives. The translation $\Pi$ is set as follows:

1. $\Pi(p_i) := x_1$
2. $\Pi(\phi) := 1 + \Pi(\phi)$
3. $\Pi(\phi \land \psi) := \Pi(\phi) \cdot \Pi(\psi)$
4. $\Pi(\phi \lor \psi) := \Pi(\phi) \cdot \Pi(\psi) + \Pi(\phi) + \Pi(\psi) + 1$
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, \( \varphi \) 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 laws of form

In a booklet of 1969 (cf. [SB69]) George Spencer-Brown tried 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 \( \downarrow \).

If we understand the logical form of a proposition as its formal-algebraic structure with the implicit purpose of revealing those features which matter to the validity of propositions, we start to doubt about Wittgenstein’s simplistic view (see [Witt]) that logical form is given by mere truth-tables (his Proposition 4.31), and cannot be stated or spoken, only shown.

Although we may agree with Wittgenstein that philosophy is the activity of clarifying language, and that most philosophical confusion arises from trying to speak about things that can only be shown, it is an oversimplification to believe that logical form makes itself apparent, without the need for logical relations or objects. As we shall see, looking not only to static truth-tables but to functions endowed with a richer algebraic structure, as polynomials over rings, makes a difference.

The attempts by Spencer-Brown to express abstract concepts as laws of form in compact combinatorial notation (if his “the laws of form” coincide or generalize the notion of “logical form” in the above sense) seem also to have been preceded by Leibniz’s efforts to formalize the traditional Chinese divinatory hexagrams known as I Ching (or Yijing), forging a correspondence between 0 and 1, and, respectively, the \( (yin) \) and \( (yang) \) lines in the Fu Hsi (or Fuxi) diagrams.

But “the laws of form” of Spencer-Brown do not reduce to Peirce’s existential graphs, nor do just a 0-1 encoding as Leibniz’s; his calculus actually derive the constants 0 and 1, and also a third “imaginary” truth-value that surpasses the capacity of the Boolean universe (and has some obvious connections, never explored, to paracomplete thinking).

The most relevant material of “The Laws of Form” is contained in the following topics:
1. “The Primary Arithmetic” (Chapter 4): basically, arithmetic modulo 2;

2. “The Primary Algebra” (Chapter 6): two-element Boolean algebra and classical propositional calculus (PC);


A good part of his work is considered by some as just camouflage. B. Banaschewski, in [Ban], for instance, showed that the “The Primary Algebra” is just Boolean algebra in disguise. Although this is a correct observation, the “The Primary Algebra” is Boolean algebra regarded from a very different perspective, and the polynomial ring calculus described in the previous section reveals this aspect in a neat way. Indeed, by reading the empty space as 0, meaning “falsity”, an equation like \( x = \) simply means “\( x \) is false”.

In addition, the “The Primary Algebra” is obtained by adding two equational identities governing the symbol \( k \):

1. Position: \( \overline{pr} pr = 0 \)
2. Transposition: \( \overline{(pq)r} \overline{qr} = \overline{pr} pr r \)

Now what precisely the symbol \( \overline{ } \) and the juxtaposition operation mean is far from obvious, but the following is an illuminating interpretation:

- Interpret juxtaposition \( pq \) as \( p \lor q \), corresponding to the polynomial form \( p \cdot q + p + q \) in \( \mathbb{Z}_2[X] \);
- Interpret \( \overline{p} \) as \( \neg p \), corresponding to the polynomial form \( p + 1 \) in \( \mathbb{Z}_2[X] \).

Consequently, \( \overline{pq} \) will be, of course, interpreted as \( p \rightarrow q \), corresponding to \( p \cdot q + p + 1 \), which leads to the following understanding:

- For Position: \( \overline{pq} = \text{iff} ((p \cdot p) + p + 1) + 1 = 0 \), which is obviously the case;
- For Transposition (where \( p \odot q = p \cdot q + p + q \)): \( \overline{(pq)r} \odot (qr) = \overline{pr} pr r \) iff \( ((p \odot r) + 1) \odot ((q \odot r) + 1) = ((p + 1) \odot (q + 1) + 1) \odot r \), which is just an easy polynomial handling.

So the “Primary Algebra” is just the Boolean ring \( \langle \{0, 1\}, \lor, +, 1 \rangle \) (up to isomorphism). This basically recovers the work of [Ban] in a very direct way.

This interpretation, however, makes calculations in “The Laws of Form ” much complicated; polynomial handling suggests a dual interpretation. As a matter of fact, a second interpretation is:

- Interpret juxtaposition \( pq \) as \( p \land q \), corresponding to \( p \cdot q \);

\(^1\)Some informal biographies of Spencer-Brown point that in 1950-51 he has worked together with Wittgenstein in foundations of philosophy.
• Interpret $\overline{p}$ as $\neg p$, corresponding to $p + 1$, as in the first interpretation;

• Now, read the empty space (for falsity) as 1.

• Consequently $\overline{p} q$ corresponds now to $\neg p \land q$, represented by $(p + 1) \cdot q$.

It is easy to check that Position and Transposition are satisfied. Why is the second interpretation better? Simply because most results in [SB69] (page numbers indicated) become immediate:

1. “Reflection” (p. 28): $\overline{\overline{a}} = a$. The proof is immediate, translating the formula to $(a + 1) + 1 = a$ (but takes two pages in [SB69]).

2. “Generation” (p. 32): $\overline{a b} = \overline{a} b$. Translating the formula to $(a \cdot b + 1) \cdot b = (a + 1) \cdot b$ the verification is obvious: $(a \cdot b + 1) \cdot b = a \cdot b^2 + b = a \cdot b + b = (a + 1) \cdot b$.

3. “Occultation” (p. 33): $\overline{\overline{a} b} a = a$. Translating the formula to $((a + 1) \cdot b + 1) \cdot a = a$ the verification is also easy: $((a + 1) \cdot b + 1) \cdot a = (a \cdot b + 1) \cdot a = a \cdot b + a \cdot b + a = a$.

Now, the “Primary Arithmetic” is governed by the following laws:

1. Number (or Condensation): $\overline{\overline{k}} = \overline{\overline{k}}$

2. Order (or Cancellation): $\overline{\overline{k}} = \overline{k}$

The second interpretation also offers an illustrative understanding for the “Primary Arithmetic” by means of polynomials over $\mathbb{Z}_2$:

1. For Number: $\overline{\overline{1}} = 1 + 1 = 0$, thus $\overline{\overline{1}}$ is the element 0. Now, $\overline{\overline{1}} = 0 \cdot 0 = 0$. Hence $\overline{\overline{1}} = \overline{\overline{1}}$

2. For Order: $\overline{\overline{1}} = \overline{\overline{0}} = 1 + 1 = 0$, thus $\overline{\overline{1}}$ is exactly 0, and therefore $\overline{\overline{1}} = 1$.

Hence, $\overline{\overline{1}} = 0$ and $\overline{\overline{1}} = 1$

This permits to see the main bulk of the “laws of form” of Spencer-Brown as Boolean algebra (the “Primary Algebra”) plus a bit of arithmetic (the “Primary Arithmetic”), which act together as to define the totality of a Boolean ring from the empty, much in the spirit of Brower’s “two-oneness”. The polynomial interpretation can be also extended to encode the “Equations of the Second Degree”, (but this technically more involved and will not be pursued here). What is relevant to remark is that the polynomial handling work as a demystifier, and quite readily reveals that the “laws of form” are not any transcendental calculus, as some wish to see it, neither mere Boolean algebra in disguise as implied by [Ban].
4 Half-logics and quarter-logics: on some laws of logical form

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

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

$$v(\sim P) = 0 \text{ iff } v(P) = 1$$

Non-truth-functional connectives, however, are abundant in the literature. Béziau in [Bez] defined a partial (non-truth-functional) negation $\sim_1$ characterized by:

$$v(\sim_1 P) = 0 \text{ if } v(P) = 1$$

Albeit its non-truth-functional character, the negation $\sim_1$ is defined via a process of bounded non-determinism in the sense that $v(\sim_1 P) \in \{0, 1\}$ 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 $GF_p[X]$ with extra (hidden) variables (cf. [Car05]).

Due to its bounded non-truth functionality, $\sim_1 P$ can is representable as a simple polynomial over $Z_2[X]$ with an extra variable $x$. Indeed, the “half” negation $\sim_1 P$ is computable by $x \cdot (p + 1)$ and easily recovers classical negation with the help of $\rightarrow$: in polynomial format, $P \rightarrow \sim_1 P$ is computed as $p \cdot (x \cdot (p + 1)) + p + 1 = p + 1$, but $p + 1$ represents $\sim$.

This was noted in [Bez] 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 $\{\rightarrow, \sim_1\}$). The translation $\tau$ in question is:

1. $\tau(P) = P$, for $P$ atomic;
2. $\tau(A \rightarrow B) = \tau(A) \rightarrow \tau(B)$;
3. $\tau(\sim A) = A \rightarrow \sim_1 A$

Although this “phenomenon” deserved a paper by L. Humberstone (cf. [Hum]), 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 $\sim_1$. Indeed, additional “half-logics” can be defined just by playing with polynomials, as for instance:

$$v(\sim_2 P) = 1 \text{ if } v(P) = 0$$

In polynomial terms $\sim_2 p$ is expressed by $p \cdot x + 1$ (when $p = 0$, $\sim_2 p = 1$, but when $p = 1$, then $\sim_2 p$ is undetermined).

Now consider a connective $P \leftarrow Q$ 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 $\leftrightarrow$ define classical negation $\sim$ by $\neg_2(P) \leftrightarrow P$, 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 $\rightarrow$ whose valuation condition is:

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

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

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

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

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 $\{\sim, \rightarrow\}$.

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

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

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

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

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

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 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.

Boole’s “algebra of logic”, re-shaped by E. Schröder and later subsumed in the propositional and predicate calculus (cf. [K01]), 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 expresses such a distinction between Boole’s algebra and Boolean algebra; in this respect, they do convey interesting aspects of the laws of form and of the logical form, even if nobody knows precisely which laws govern neither of them.

References


