Proofs by handling polynomials: a tool for teaching logic and metalogic

Walter Carnielli [*]
GTAL/CLE and Department of Philosophy
State University of Campinas
P.O. Box 6133, 13083-970
Campinas, SP, Brazil
e-mail: walter.carnielli@cle.unicamp.br

Abstract

1 Polynomials as proof devices

Algebraic proof systems based on formal polynomials over algebraically closed fields (the “polynomial ring calculus”) were introduced in [9] (see [10] and [11] for recent developments). Formal polynomials work as a powerful tool for logical derivation in classical and non-classical logics, in particular for propositional many-valued logics, paraconsistent logics and modal logics. Although the case of first-order logic (FOL) is still work in progress, polynomial ring calculus have been obtained for the monadic fragment of FOL and offer a nice view of syllogistic logic that permits to reassess ideas of G. Boole on the unity between algebra and logic.

For the particular case of classical propositional calculus (PC) a direct formulation of propositional derivability can be obtained by translating the usual Boolean connectives as follows: Let $At = \{p_1, p_2, \ldots\}$ be the atomic sentences of **PC**, and $\neg, \vee, \wedge, \to$ the usual connectives. The translation is part of the logic folklore, and perhaps because it is so intuitive its generalization towards other logics has never been explored in full generality.

The polynomial rules over $Z_2[X]$ for the case of **PC** are just $x + x \vdash_{\approx} 0$ and $x \cdot x \vdash_{\approx} x$. Based on such rules and on the elementary algebraic and combinatorial properties of the ring $Z_2[X]$ it can be easily shown that φ is a **PC**-tautology iff $\Pi(\varphi) \vdash_{\approx} 1$, or, in other words, φ is a PC-tautology iff such reduction rules end up at the element 1. For instance, the sentence $\alpha \to (\neg\alpha)$, supposing α atomic, is translated by Π above into $x \cdot (x + 1) + x + 1$. The reduction rules

[*] Supported by CNPq and Project LogCons-FAPESP (process 10/51038-0)

and polynomial handling obtains the following sequence of reductions (where $a \approx b$ mean that a is reduced t b): $(x \cdot (x+1) + x + 1) \approx (x^2 + x + x + 1) \approx (x + x + x + 1) \approx (x+1)$ which shows only that it is equivalent to $\neg\alpha$, but not any tautology.

This result represents, at the same time, a (constructive) semantical completeness and a decision procedure for **PC**. A generalization of this idea to many-valued logics, considering that a completeness result with respect to the polynomial ring calculus can be obtained for any finitely-valued logic by using appropriate finite fields, offers some promising possibilities for a method for checking the general satisfiability problem for many-valued logics (in particular for SAT), since the reductions performed by the polynomial ring calculus might (at least in some fortuitous cases) be subexponential in the number of variables of a propositional formula.

By using rings over finite fields (a generalization of Boolean rings, rather than Boolean algebras)any finite-valued logic can be treated in similar terms. Taking Lukasiewicz's three-valued system L_3 as an example, recall that L_3 is sound and complete with respect to a couple of matrices for → and ¬ (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: $x \to y = 2x(y+1)(xy+y+1)$ and $\neg(x) = 2x$. As an 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 L_3. The method is obviously also useful as a decision procedure (it is clear that any logic characterizable by polynomial calculus is recursively decidable).

An interesting characteristic of using formal polynomials is that the method can be also used in non-truth functional logics (as modal and paraconsistent logics) by using extra (hidden) variables. A new sound and complete polynomial ring calculus for $S5$, which we called the *least hidden-variables calculus*, was obtained in [1]; as an example:

Example 1.1. $\mid\!\approx_{S5} (\Diamond p \to p) \vee (\Diamond p \to \Box\Diamond p)$*:*

$$((\Diamond p \to p) \vee (\Diamond p \to \Box\Diamond p))^* \tag{1}$$

$$= (\Diamond p \to p)^*(\Diamond p \to \Box\Diamond p)^* + (\Diamond p \to p)^* + (\Diamond p \to \Box\Diamond p)^* \tag{2}$$

$$\approx (\Diamond p \to \Box\Diamond p)^*((\Diamond p \to p)^* + 1) + (\Diamond p \to p)^* \tag{3}$$

$$\approx ((\Diamond p)^*((\Box\Diamond p)^* + 1) + 1)((\Diamond p)^*(p^* + 1)) + (\Diamond p)^*(p^* + 1) + 1 \tag{4}$$

$$\approx ((x_{\Box\neg p} + 1)(x_{\Box\neg\Box\neg p} + 1) + 1)((x_{\Box\neg p} + 1)(x_p + 1)) + (x_{\Box\neg p} + 1)(x_p + 1) + 1 \tag{5}$$

$$\approx ((x_{\Box\neg p} + 1)(x_{\Box\neg p}) + 1)((x_{\Box\neg p} + 1)(x_p + 1)) + (x_{\Box\neg p} + 1)(x_p + 1) + 1 \tag{6}$$

$$\approx (x_{\Box\neg p} + 1)(x_p + 1) + (x_{\Box\neg p} + 1)(x_p + 1) + 1 \tag{7}$$

$$\approx 1. \tag{8}$$

In [1] we show a keen relationship between the polynomial ring calculus and modal algebras, as well as with equational logics and 'rewriting rules' (the

Dijkstra-Scholten method). We also show how the methods can be extended to other modal logics.

2 Some historical connections

Formal polynomials as algebraic proof procedures are reminiscent of the tradition of using algebraic methods to express logic properties, already implicit in the work of Leibniz, Boole, De Morgan, Peirce, Schröder, Hilbert and Tarski.

The Russian mathematician Ivan Ivanovich Zhegalkin had already proposed in 1927, however, a method (cf. [19]) to translate and decide propositions from A. Whitehead and B. Russell's *Principia Mathematica* by using polynomials with coefficients in the two-element field $\mathbf{Z}_2$.

Zhegalkin was concerned with sums and products of propositions, as well as with arithmetical side of symbolic logic (cf. [20]), and thought also about extending his methods to quantified sentences, borrowing the Peirce-Schröder definition of universal quantification and existential quantification in terms of infinite sums and products, although he did not obtain a complete method; some intuitions in the same direction are also to be found in the work of the Russian/Ukrainian logician Platon Sergeevich Poretskij (cf. [3]).

In the proposal of [9], [10] and [11] 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). Formal definitions and further details can be found [10] and [11].

3 Polynomials as automatic proof systems

Polynomial ring calculus seem to be very 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 $Z_2[X]$.

The system *MUltlog*, within a project by the Vienna Group for Multiple-valued Logics, is an automatic system [1] which accepts as input the specification of a finitely-valued first-order logic and outputs a sequent calculus (as well as a natural deduction system and clause-formation rules) for this logic. *MUltlog* automatically transforms tables of an arbitrary finite-valued logic into a finite number of sequent rules, and it seems that a simple adaptation of *MUltlog* would automatically obtain polynomial ring calculus for arbitrary finite-valued logics. Interestingly enough, basic references for the *MUltlog* system (among others) are [7] and [8], which define, respectively, tableau systems and hypersequent systems that can be, for sure, transformed into polynomial format. This

[1] I am indebted to Josep Font (Barcelona) who called my attention to *MUltlog*, cf. `http://www.logic.at/multlog/JMUltlog/`, in a personal conversation in Dresden.

fact carries further evidence that *MUltlog* could automatically transform tables of an arbitrary finite-valued logic into polynomials over an appropriate finite field, thus automatically generating polynomial proof systems for finite-valued logics.

4 The algebraic side

Since polynomials represent the semantical setting for several logics already in purely algebraic form, the use of formal polynomials in logic may be an alternative to algebraic methods which basically correspond theorems on logical systems with identities on classes, characteristic of the spirit of the Polish school represented by A. Tarski, J. Lukasiewicz and A. Lindenbaum. In this way, using polynomials my be a useful tool for teaching, or at least for elucidating, certain metalogical properties of logic

The paradigmatic (and intuitive) cases are Boolean algebras (associated to classical propositional logic) and Heyting algebras (associated to Intuitionistic Logic). But to algebraize modal logics is harder, and the algebraization of paraconsistent logics offers a real challenge (see [5] for a discussion, and for a proposal, further refined in [6]). Considering that even some logics that have no finite-valued characterizable semantics, such as certain modal and paraconsistent logics, can be characterized by polynomial ring calculi over polynomial rings with extra variables (cf. [1] and [11]), a shift from Boolean algebras (or Boolean lattices) to polynomial rings may be a clue to some new algebraic characterizations.

For instance, the prime numbers of Z correspond to monic irreducible polynomials in the ring of polynomials in one variable over finite fields, a property with several interesting consequences (see [15]) that has never been explored in logic. Moreover, factorizing polynomials seems to be more tractable than factorizing integers, a fact that may have striking consequences in several areas.

Despite the fact that the categories of Boolean rings and Boolean algebras are equivalent, polynomial rings based upon finite fields have some finer combinatorial properties that may be of more interest for logicians, and working with commutative rings in general may offer some hints towards algebraizing non-classical logics.

5 Polynomials as heuristic devices

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

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

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. [10]).

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. [17]), 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 $\{\rightarrow, \rightharpoondown, \sim\}$.

Several of such "partial logics" can be discovered (cf. [13]), making polynomial handling a nice heuristic device. The polynomial ring calculi have obvious potentialities for automation, constitute one of the few devices for exploring the heuristic side of logic and are skillful engines to help understanding and explaining certain features of logic and metalogic. As argued in [2], the view that a mathematical proof reduces to just the guarantee of truth of a theorem fails to explain why new proofs of certain theorems are considered relevant. Methods such as our polynomial calculi may help to render proofs in logic more intelligible, and this is of course of paramount importance for teaching.

References

[1] Agudelo, J. C. and Carnielli, W. A. Polynomial ring calculus for modal logics: a new semantics and proof method for modalities. To appear in the *Review of Symbolic Logic*. 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] Avigad, J. Mathematical method and proof. *Synthese* 153 (1), 2006: 105-159.

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

[4] Béziau, J.-Y. Classical negation can be expressed by one of its halves. *Logic Journal of the Interest Group in Pure and Applied Logics* 7:145-151, 1999.

[5] Bueno-Soler, J. and Carnielli, W. A. Possible-translations algebraization for paraconsistent logics. *Bulletin of the Section of Logic*, v. 34, n. 2, p. 77-92, 2005.

[6] Bueno-Soler, J.; Carnielli, W. A. and Coniglio, M. E. Possible-translations algebraizability. In: J.-Y. Bziau, W.A. Carnielli, D. Gabbay. (Org.). Handbook of Paraconsistency. College Publications, London, p. 321-340, 2007.

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

[8] Carnielli, W. A. On sequents and tableaux for many-valued logics. *J. Non-Classical Logic* 8(1):59-76, 1991.

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

[10] 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`.

[11] 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. Preprint available under 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`.

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

[13] Carnielli, W. A. Formal polynomials, heuristics and proofs in logic. In: Alexander S. Karpenko. (Org.). Logical Investigations. 16 ed. Moscou: Institute of Philosophy- Russian Academy of Sciences, 2010, v. 1, p. 280-294.

[14] 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 15107. Springer, 2nd edition, 2007. Preprint available from *CLE e-Prints* 5(1), 2005 at `http://www.cle.unicamp.br/e-prints/vol5,n1,2005.htm`

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

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

[17] Humberstone, L. Béziaus Translation Paradox. *Theoria* 71: 138-181, 2005.

[18] Turquette, A. Minimal Axioms for Peirce's Triadic Logic. *Mathematical Logic Quarterly* 22(1): 169176, 1976.

[19] Zhegalkin, I. I. O tekhnike vychisleniya predlozhenii v simvolicheskoi logike (On a technique for the calculus of propositions in symbolic logic). *Matematicheskii Sbornik* 1(34): 928, 1927.

[20] Zhegalkin, I. I. Arifmetizatsiya simbolicheskoi logiki (The arithmetization of symbolic logic). *Matematicheskii Sbornik* (1):35 311-377, 1928 and (1):36 205-338, 1929.

Aristotle developed formal logic as a systematized method for reasoning about the meanings expressed in ordinary language. For the next two millennia, formal logic was expressed in a stylized or controlled subset of a natural language: originally Greek, then Latin, and later modern languages.Â In short, there are two equal and opposite fallacies about language and logic: at one extreme, logic is considered unnatural and irrelevant; at the opposite extreme, language is incurably vague and should be replaced by logic.Â Unfortunately, the tools for database design have been disjoint from expert-system tools; they use different notations that require different skills and often different specialists.