THE REVIEW OF SYMBOLIC LOGIC
Volume 4, Number 1, March 2011

POLYNOMIAL RING CALCULUS FOR MODAL LOGICS: A NEW SEMANTICS AND PROOF METHOD FOR MODALITIES

JUAN C. AGUDELO
State University of Campinas—UNICAMP
and
Eafit University

WALTER CARNIELLI
State University of Campinas—UNICAMP
and
SQIG—IT

Abstract. A new (sound and complete) proof style adequate for modal logics is defined from the *polynomial ring calculus (PRC)*. The new semantics not only expresses truth conditions of modal formulas by means of polynomials, but also permits to perform deductions through polynomial handling. This paper also investigates relationships among the PRC here defined, the algebraic semantics for modal logics, equational logics, the Dijkstra–Scholten equational-proof style, and rewriting systems. The method proposed is throughly exemplified for *S*5, and can be easily extended to other modal logics.

§1. Yet another semantics for modal logic? Besides its indisputable success, there may be reasons to doubt about the universal acceptability of the *possible-worlds semantics* (often called *relational semantics* or *Kripke semantics*) for modal logics, basically because they reduce (or equate) meaning to extensions of worlds.

Indeed, criticisms against possible-worlds semantics abound. For instance, Kuczynski (2007) purports to show that the very assumptions of possible-worlds semantics lead to the absurd conclusion that all propositions are necessarily true. Even if this critique would be perhaps circumscribed to uses of possible-worlds semantics in quantified modal logic, it is not easy to rebut the well-known Quine's criticisms about the difficulties in separating the notion of possibility within a world from the notion of consistency of the world's description (cf., Section 1 of Quine, 1953).

But there are other issues with regard to the possible-worlds account of modal notions. As argued in Fagin & Vardi (1985), the mathematics associated with such semantics may be quite complicated, besides the inappropriateness of the possible-worlds to formalizing knowledge, belief, and other nonalethic modal concepts.

Other interesting semantical approaches like *algebraic semantics*, *neighborhood semantics*, and *topological semantics* have been employed in the characterization of modal logics (see Blackburn & Benthem, 2006, and Goldblatt, 2005), which by itself suggests that the

Received: October 24, 2009

© Association for Symbolic Logic, 2010
doi:10.1017/S1755020310000213

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

issue of finding a satisfactory semantics for modal notions is far from closed. The *internal semantics* proposed in Fagin & Vardi (1985) is indeed quite simple, but here a new calculus is introduced which leads to an even simpler semantics. What is proposed is a new treatment for modal logics, which is based on the *polynomial ring calculus* (PRC) introduced in Carnielli (2005) (see also Carnielli, 2007, for further developments). This proposal has the technical advantage of providing not only a new semantics, but also an easy mechanical procedure to perform modal deductions, with the philosophical benefit of shedding some light on the *indeterministic* character of modal reasoning. This approach offers, we believe, a new insight to the investigation of modal logics, since it radically separates possibility and necessity from the possible-worlds standpoint.

In PRC logic formulas are translated into polynomials over a finite (Galois) field; elements of the field represent truth values, and polynomial equations express truth conditions (in a way similar to conditions in the specification of valuation semantics). In contrast to other methods, PRC has two great advantages: it permits to perform deductions in a mechanical way by means of simple polynomial operations and allows to express indeterminism by means of 'hidden variables' (in the way described below). PRC can, indeed, be regarded as an algebraic semantics, in which polynomials codify the truth-value conditions of logic formulas; but it can also be seen as a proof method (as much as a tableau calculus can be viewed as a proof-theoretical or as a model-theoretical device). In Carnielli (2005), PRC is described in detail and is applied to the classical propositional calculus, to many-valued logics, and to paraconsistent logics. Here we show that this method can be successfully applied to modal logics as well.

The structure of the paper is the following: in Section 2 a PRC for $S5$ is defined and some examples of deductions with the calculus are treated. Section 3 proves the soundness and completeness of PRC for $S5$. In Section 4 a strong relationship between modal algebras and the structure of polynomials in the PRC is discussed. In Section 5, an alternative definition of a PRC for $S5$ is presented. Connections with equational logic are described in Section 6. In Section 7 it is explained how equational proof systems (*à la* Dijkstra–Scholten and in terms of 'rewriting rules') can be defined via the PRC for $S5$, and the remarks in Section 8 explain how the methods here proposed can be extended to other modal logics.

If, as picturesquely put in (Blackburn & Benthem, 2006, p. 5), modal formulas talk about Kripke models from the inside, our method shows that modal formulas also talk about the invisible side of truth-values, and indeed, modal formulas do this by talking about the values that 'hidden variables' display, as it is described below.

§2. Defining a polynomial ring calculus for $S5$. The first step in defining a PRC for a logic L consists in selecting a field F (usually a finite Galois field $GF(p^n)$) to represent truth-values (choosing a subset of *designated values*). The second step consists in defining a translation function $*$: $For L \rightarrow F[X]$, from formulas of L to polynomials over F (with algebraic variables in a set X). In some cases, it is also necessary to define *polynomial constraints*, which consist in new polynomial conditions (polynomial equations or implications of polynomial equations) restricting the values that algebraic variables can take. The elements above must be defined in such a way that polynomial operations allow us to perform valid deductions.

In the context of a PRC for a logic L, we will use two different symbols: $\models\!\!\approx_L$ and $\approx_L$, the former to express the semantical consequence relation in terms of polynomials and the

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

other to express the 'reduction relation' which establishes the polynomial operations that can be use to perform deductions.

Before defining the semantical consequence relation $\models\!\!\approx_L$, it is necessary to define the notion of *valuation* in the context of PRC:

DEFINITION 2.1. (L-PRC-valuation) *Let F be the field and X be the set of algebraic variables used in a PRC for a logic L, an* L-PRC-valuation *is a function v: $X \to F$, under the condition of satisfying all polynomial constraints (if they exist).*

In order to simplify notation, the assignment of values by a valuation v to variables in a set X will be denoted by $\overrightarrow{X}_v$, and the value of a polynomial P under the valuation v will be denoted by $P[\overrightarrow{X}_v]$. Now, we will define the consequence relation $\models\!\!\approx_L$:

DEFINITION 2.2. (L-PRC-consequence-relation) *Let F be the field and X be the set of algebraic variables used in a PRC for a logic L, and let $*$: $For L \to F[X]$ be the translation function mapping formulas of L into polynomials in $F[X]$. Consider $D \subset F$ ($D \neq \emptyset$) as denoting the set of* designated values. *A formula α of L is an* L-PRC-consequence *of a set of formulas Γ of L (denoted by $\Gamma \models\!\!\approx_L \alpha$) if, for any L-PRC-valuation v, it is the case that $\alpha^*[\overrightarrow{X}_v] \in D$ whenever $\gamma^*[\overrightarrow{X}_v] \in D$ for every formula $\gamma \in \Gamma$.*

We now proceed to define the basic reduction relation $\approx$, which is the base of the reduction relation $\approx_L$ for any logic L. For some logics L the relation $\approx_L$ is just the basic relation $\approx$; the subindex L in the reduction relation will be specified only when polynomial constraints (extending the definition of $\approx$) are included.

Taking into account Galois fields denoted by $GF(p^n)$ (where p is a prime number, the *field characteristic*, and n is a natural number), the polynomial operations which permit to perform deductions in PRC are governed by the following rules, where capital letters are used to denote polynomials and $P \approx Q$ express that the polynomial P can be replaced by the polynomial Q:

- A first group of rules, the *ring rules*, corresponding to the ring properties of addition and multiplication (here we consider that the ring is commutative and has multiplicative identity):

$$P + Q \approx Q + P \text{ (additive commutativity)}, \tag{R1}$$

$$P + (Q + R) \approx (P + Q) + R \text{ (additive associativity)}, \tag{R2}$$

$$P + 0 \approx P \text{ (additive identity)}, \tag{R3}$$

$$P + (-P) \approx 0 \text{ (additive inverse)}, \tag{R4}$$

$$P \cdot Q \approx Q \cdot P \text{ (multiplicative commutativity)}, \tag{R5}$$

$$P \cdot (Q \cdot R) \approx (P \cdot Q) \cdot R \text{ (multiplicative associativity)}, \tag{R6}$$

$$P \cdot 1 \approx P \text{ (multiplicative identity)}, \tag{R7}$$

$$P \cdot (Q + R) \approx (P \cdot Q) + (P \cdot R) \text{ (distributivity)}. \tag{R8}$$

- A second group of rules, the *polynomial rules*:

$$\overbrace{x + \ldots + x}^{p \text{ times}} \approx 0, \tag{P1}$$

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

$$x^i \cdot x^j \approx x^k \tag{P2}$$

where $k \equiv i + j \pmod{(p^n - 1)}$.[1]

- There are also two inference metarules, the *uniform substitution*:

$$\frac{P \approx Q}{P[x : R] \approx Q[x : R]} \tag{US}$$

and the *Leibniz rule*:

$$\frac{P \approx Q}{R[x : P] \approx R[x : Q]} \tag{LR}$$

where $P[x : Q]$ denotes the result of uniformly substituting Q for the variable x in P.

Note that all the rules defining the reduction relation $\approx$ preserve truth conditions, due to the fact that polynomials on both sides of $\approx$ are equivalents (in the sense that they take the same values for all possible valuations).

In order to describe another important feature of $\approx$, we will say that a polynomial P is in *normal form* if P is a constant polynomial (i.e., if P is an element of the field F), $P = n_1 P_1 + \ldots + n_m P_m$ or $P = n_1 P_1 + \ldots + n_m P_m + n_{m+1}$, where all n_i are elements of F and all P_i are irreducible monomials.

THEOREM 2.3. *Any polynomial in $F[X]$ can be reduced to a unique polynomial in normal form (up to commutativity and associativity) by means of the reduction relation $\approx$, for any finite field F and any set of variables X.*

Proof. Since the finite 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 operations to any polynomial P in $GF(p^n)[X]$ obtains a class representative of P in $GF(p^n)[X]$ modulo $p(x)$ with minimum degree (note that the polynomial rules always decrease degrees). Now, suppose that there are two different normal forms Q and R to which the polynomial P can be reduced. Q and R must be equivalent polynomials, thus they cannot be two different constant polynomials, nor one of them a constant polynomial and the other a nonconstant polynomial. Suppose that $Q = n_1 Q_1 + \ldots + n_l Q_l$ and $R = m_1 R_1 + \ldots + m_s R_s$. As Q and R have to be both equivalent to P, then

$$Q + \overbrace{R + \ldots + R}^{n-1 \text{ times}} = 0.$$

Now group the equal monomials in this equation by adding their coefficients modulo n (which is a consequence of (P1)). In this way, one obtains a polynomial equation where all monomials are different. By selecting a 'minimal' monomial Q_i (i.e., a monomial with the least number of variables) and assigning values to variables in Q_i in such a way that $n_i Q_i$ equals a nonzero element k of $GF(p^n)$, and assigning 0 to all other variables, we obtain a contradiction ($k = 0$). The other cases of Q and R are similar. □

[1] This reduction is a consequence of the fact that $x^i \cdot x^j \approx x^k \pmod{q(x)}$ where $q(x)$ is a convenient primitive polynomial (i.e., and irreducible polynomial of degree n with coefficients in $\mathbb{Z}_p$).

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

An immediate consequence of Theorem 2.3 is the following:

COROLLARY 2.4. *If the set of designated values D is a singleton ($D = \{d\}$) and the PRC does not contain any polynomial constraints, then $\models_L \alpha$ if and only if $\alpha^* \approx d$, for any formula α.*

As a form of motivation, we will first present a PRC for the Classical Propositional Calculus (CPL), and then extend it to the modal system $S5$. In both cases, formulas are translated into polynomials over the field $\mathbb{Z}_2$ (the integers modulo 2) and the only designated value is 1. In this case, the polynomial rules are just $x + x \approx 0$ and $x \cdot x \approx x$.

DEFINITION 2.5. (PRC for CPL) *Let $ForCPL$ be the set of well-formed formulas of CPL, and let $X = \{x_{p_1}, x_{p_2}, \ldots\}$ be a set of algebraic variables. A* PRC for CPL *is determined by the translation function $*: ForCPL \to \mathbb{Z}_2[X]$ recursively defined by:*[2]

$$
\begin{aligned}
(p_i)^* &= x_{p_i} \text{ if } p_i \text{ is a propositional variable},\\
(\neg\alpha)^* &= \alpha^* + 1,\\
(\alpha \wedge \beta)^* &= \alpha^*\beta^*,\\
(\alpha \vee \beta)^* &= \alpha^*\beta^* + \alpha^* + \beta^*,\\
(\alpha \to \beta)^* &= \alpha^*\beta^* + \alpha^* + 1.
\end{aligned}
$$

It is easy to prove that the PRC for CPL in Definition 2.5 is sound and complete. Indeed, the translation function $*$ just specifies classical valuations (in the sense that for each assignment of values to variables in X we have a classical valuation), and thus the soundness and completeness of classical valuations for CPL implies at once the soundness and completeness of the PRC for CPL.

The following example shows how deductions are accomplished in the PRC for CPL:

EXAMPLE 2.6. $\models_{CPL} p \vee \neg p$:

$$
\begin{aligned}
(p \vee \neg p)^* &= p^*(\neg p)^* + p^* + (\neg p)^*\\
&= x_p(x_p + 1) + x_p + x_p + 1\\
&\approx x_p x_p + x_p + 1\\
&\approx x_p + x_p + 1\\
&\approx 1.
\end{aligned}
$$

The symbol $=$ is used in the first two lines of the deduction, instead of $\approx$, because there we only use the definition of the translation function $*$ (we do not accomplish any reduction in such lines).

We now proceed to extend to $S5$ the previously defined PRC for CPL.

$S5$ is usually defined by extending CPL, introducing a unary *necessitation* operator $\Box$ and a unary *possibility* operator $\Diamond$, and adding the following axioms and rule:

$$\Box(\alpha \to \beta) \to (\Box\alpha \to \Box\beta), \tag{K}$$

$$\Box\alpha \to \alpha, \tag{T}$$

[2] Products will be denoted by concatenation (avoiding the $\cdot$ symbol) as usual.

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

$$\alpha \to \Box\Diamond\alpha, \tag{B}$$

$$\Box\alpha \to \Box\Box\alpha, \tag{4}$$

$$\vdash \alpha \text{ implies } \vdash \Box\alpha. \tag{Nec}$$

In Carnielli (2005), the so-called *hidden variables* are introduced in the PRC for logics which are not characterizable by means of finite matrices. Hidden variables are extra algebraic variables, distinct to those associated with propositional variables, and they are supposed to take values in the field in a random manner. In this way, the nondeterminism of *non-truthfunctional bivalued semantics* is captured by the random assignment of values to hidden variables. The presence of hidden variables, in the polynomial corresponding to a specific formula, indicates that the truth-values of that formula do not functionally depend on the truth-values of its propositional variables. By following this strategy and introducing *polynomial constraints* as additional rules governing the nondeterminism, we define a PRC for $S5$:

DEFINITION 2.7. (PRC for $S5$) *Let For$S5$ be the set of well-formed formulas of $S5$, and let $X = \{x_{p_1}, x_{p_2}, \ldots\}$ and $X' = \{x_{\Box\alpha_1}, x_{\Box\alpha_2}, \ldots\}$ be disjoint sets of algebraic variables; indexed, respectively, by propositional variables p_i and by $S5$-formulas $\Box\alpha_i$. Variables in X' are called* hidden variables. *The* PRC for $S5$ *is determined by the translation function $\star$: For$S5 \to \mathbb{Z}_2[X \cup X']$ recursively defined by:*

$$\begin{aligned}
(p_i)^\star &= x_{p_i} \text{ if } p_i \text{ is a propositional variable},\\
(\neg\alpha)^\star &= \alpha^\star + 1,\\
(\alpha \wedge \beta)^\star &= \alpha^\star\beta^\star,\\
(\alpha \vee \beta)^\star &= \alpha^\star\beta^\star + \alpha^\star + \beta^\star,\\
(\alpha \to \beta)^\star &= \alpha^\star\beta^\star + \alpha^\star + 1,\\
(\Box\alpha)^\star &= x_{\Box\alpha},\\
(\Diamond\alpha)^\star &= x_{\Box\neg\alpha} + 1.
\end{aligned}$$

There is a different hidden variable $x_{\Box\alpha}$ for each $S5$-formula α; however, the values they can take are correlated by the following polynomial constraints *(extending the definition of the relation $\approx$):*

$$x_{\Box(\alpha\to\beta)}(x_{\Box\alpha}(x_{\Box\beta} + 1)) \approx_{S5} 0, \tag{cK}$$

$$x_{\Box\alpha}(\alpha^\star + 1) \approx_{S5} 0, \tag{cT}$$

$$\alpha^\star(x_{\Box\Diamond\alpha} + 1) \approx_{S5} 0, \tag{cB}$$

$$x_{\Box\alpha}(x_{\Box\Box\alpha} + 1) \approx_{S5} 0, \tag{c4}$$

$$\alpha^\star \approx_{S5} 1 \text{ implies } x_{\Box\alpha} \approx_{S5} 1. \tag{cNec}$$

Note that the polynomial constraints (cK)–(cNec) are straightforward translations of (K)–(Nec). With such constraints, Definition 2.7 does not provide a mechanical proof procedure and does not represent great advantages with respect to the semantical understanding of modalities. However, Definition 2.7 allows us to prove soundness and completeness in quite a direct way (see Section 3) and is useful as an intermediate step. In the rest of this

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

section we will gradually show some more elaborate relations between hidden variables, so as to obtain a complete set of reductions allowing mechanical proofs and providing a new valuable semantical understanding of modalities.

FACT 2.8.

(a) $x_{\Box(\alpha\wedge\beta)} \approx_{S5} x_{\Box\alpha}x_{\Box\beta}$,

(b) $x_{\Box\neg\neg\alpha} \approx_{S5} x_{\Box\alpha}$,

(c) $x_{\Box\neg(\alpha\wedge\beta)} \approx_{S5} x_{\Box(\neg\alpha\vee\neg\beta)}$,

(d) $x_{\Box\neg(\alpha\vee\beta)} \approx_{S5} x_{\Box\neg\alpha}x_{\Box\neg\beta}$,

(e) $x_{\Box\neg\Box\alpha} \approx_{S5} x_{\Box\alpha} + 1$,

(f) $x_{\Box(\alpha\vee\neg\neg\beta)} \approx_{S5} x_{\Box(\alpha\vee\beta)}$,

(g) $x_{\Box(\alpha\vee\neg(\beta\wedge\delta))} \approx_{S5} x_{\Box(\alpha\vee(\neg\beta\vee\neg\delta))}$

(h) $x_{\Box(\alpha\vee\neg(\beta\vee\delta))} \approx_{S5} x_{\Box(\alpha\vee\neg\beta)}x_{\Box(\alpha\vee\neg\delta)}$,

(i) $x_{\Box(\alpha\vee\neg\Box\beta)} \approx_{S5} x_{\Box\alpha}x_{\Box\beta} + x_{\Box\beta} + 1$,

(j) $x_{\Box(\alpha\vee(\beta\wedge\delta))} \approx_{S5} x_{\Box(\alpha\vee\beta)}x_{\Box(\alpha\vee\delta)}$,

(k) $x_{\Box(\alpha\vee\Box\beta)} \approx_{S5} x_{\Box\alpha}x_{\Box\beta} + x_{\Box\alpha} + x_{\Box\beta}$,

(l) $x_{\Box(\alpha\vee\beta)} \approx_{S5} x_{\Box(\beta\vee\alpha)}$,

(m) $x_{\Box(\alpha\vee(\beta\vee\delta))} \approx_{S5} x_{\Box((\alpha\vee\beta)\vee\delta)}$,

(n) $x_{\Box\Box\alpha} \approx_{S5} x_{\Box\alpha}$.

Proof. We only present the proofs of items (a) and (b) in order to illustrate how deductions are performed taking into account polynomial constraints (cK)-(cNec), the other items can be proved in a similar way:

(a) (i) From the above defined PRC for CPL, we have that $((\alpha \wedge \beta) \rightarrow \alpha)^\star \approx_{S5} 1$, and polynomial constraint (cNec) implies that $x_{\Box((\alpha\wedge\beta)\rightarrow\alpha)} \approx_{S5} 1$. Moreover, by polynomial constraint (cK) we have that $x_{\Box((\alpha\wedge\beta)\rightarrow\alpha)}(x_{\Box(\alpha\wedge\beta)}(x_{\Box\alpha} + 1)) \approx_{S5} 0$, then $(x_{\Box(\alpha\wedge\beta)}(x_{\Box\alpha} + 1)) \approx_{S5} 0$, that is, $x_{\Box(\alpha\wedge\beta)}x_{\Box\alpha} \approx_{S5} x_{\Box(\alpha\wedge\beta)}$. In a similar way it can be shown that $x_{\Box(\alpha\wedge\beta)}x_{\Box\beta} \approx_{S5} x_{\Box(\alpha\wedge\beta)}$.

(ii) We also have that $(\alpha \rightarrow (\beta \rightarrow (\alpha \wedge \beta)))^\star \approx_{S5} 1$ and, by polynomial constraint (cK), $x_{\Box(\alpha\rightarrow(\beta\rightarrow(\alpha\wedge\beta)))}(x_{\Box\alpha}(x_{\Box(\beta\rightarrow(\alpha\wedge\beta))}+1)) \approx_{S5} 0$. Then, $x_{\Box\alpha}x_{\Box(\beta\rightarrow(\alpha\wedge\beta))} \approx_{S5} x_{\Box\alpha}$. In a similar way it can be proven that $x_{\Box\beta}x_{\Box(\alpha\rightarrow(\alpha\wedge\beta))} \approx_{S5} x_{\Box\beta}$.

On the other hand, by polynomial constraint (cK), we have that $x_{\Box(\alpha\rightarrow(\alpha\wedge\beta))}(x_{\Box\alpha}(x_{\Box(\alpha\wedge\beta)} + 1)) \approx_{S5} 0$, that is, $x_{\Box(\alpha\rightarrow(\alpha\wedge\beta))}x_{\Box\alpha}x_{\Box(\alpha\wedge\beta)} \approx_{S5} x_{\Box(\alpha\rightarrow(\alpha\wedge\beta))}x_{\Box\alpha}$. In a similar way it can be obtained that $x_{\Box(\beta\rightarrow(\alpha\wedge\beta))}x_{\Box\beta}x_{\Box(\alpha\wedge\beta)} \approx_{S5} x_{\Box(\beta\rightarrow(\alpha\wedge\beta))}x_{\Box\beta}$. Finally, by multiplying both sides of the last two reductions obtained and using reductions obtained in (i) and (ii), $x_{\Box(\alpha\wedge\beta)} \approx_{S5} x_{\Box\alpha}x_{\Box\beta}$.

(b) From the above defined PRC for CPL, we have that $(\alpha \rightarrow \neg\neg\alpha)^\star \approx_{S5} 1$. Then, by polynomial constraint (cNec) it follows that $x_{\Box(\alpha\rightarrow\neg\neg\alpha)} \approx_{S5} 1$. On the other hand, by polynomial constraint (cK), we have that $x_{\Box(\alpha\rightarrow\neg\neg\alpha)}(x_{\Box\alpha}(x_{\Box\neg\neg\alpha} + 1)) \approx_{S5} 0$, thus $x_{\Box\alpha}(x_{\Box\neg\neg\alpha} + 1) \approx_{S5} 0$, that is, $x_{\Box\alpha}x_{\Box\neg\neg\alpha} \approx_{S5} x_{\Box\alpha}$. In a similar way, starting from $(\neg\neg\alpha \rightarrow \alpha)^\star \approx_{S5} 1$, it can be proven that $x_{\Box\alpha}x_{\Box\neg\neg\alpha} \approx_{S5} x_{\Box\neg\neg\alpha}$. Consequently $x_{\Box\neg\neg\alpha} \approx_{S5} x_{\Box\alpha}$. □

With the reductions in Fact 2.8 it is possible to establish the following lemma:

LEMMA 2.9. *Let α be an S5-formula; then either $x_{\Box\alpha} \approx_{S5} \sum_{i=1}^{n}\prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}$ or $x_{\Box\alpha} \approx_{S5} (\sum_{i=1}^{n}\prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}) + 1$ where all $\alpha_{i,j}$ are literals or disjunctions of literals.*[3]

[3] Notice that $\sum_{i=1}^{n}\prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}$ can be zero, and in such cases $x_{\Box\alpha} \approx_{S5} 1$ or $x_{\Box\alpha} \approx_{S5} 0$.

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

Moreover, such reductions can be accomplished by using reductions in Fact 2.8 instead of polynomial constraints (cK)–(cNec).

Proof. In order to use Fact 2.8 and to avoid the necessity of introducing more relations between hidden variables, the operators $\rightarrow$ and $\Diamond$ in the subindex of hidden variables will be replaced by using the definitions $\alpha \rightarrow \beta \stackrel{\text{def}}{=} \neg\alpha \vee \beta$ and $\Diamond\alpha \stackrel{\text{def}}{=} \neg\Box\neg\alpha$. Taking into account this consideration, the proof proceeds by induction on the degree of α (i.e., on the level of connectives nesting in α). For literals the lemma is trivially satisfied. In the induction step: (i) for the case in which $\alpha = \beta \wedge \delta$ the reduction is obtained by item (a); (ii) for $\alpha = \beta \vee \delta$, the reduction is obtained by items (f)-(m); (iii) for formulas of the form $\alpha = \neg\beta$, items (b)-(e) obtain the reduction; (iv) for formulas $\alpha = \Box\Box\beta$, the reduction is achieved by applying item (n). Note that on the right side of all reductions (a)-(n) the indexing formulas are subformulas of the original formula, are negated subformulas, or disjunctions of them. □

The following examples show how the reductions in Fact 2.8 allow us to perform some proofs in a mechanical way.

EXAMPLE 2.10. $\models_{S5} (\Diamond p \rightarrow p) \vee (\Diamond p \rightarrow \Box\Diamond p)$*:*

$$
\begin{aligned}
&((\Diamond p \rightarrow p) \vee (\Diamond p \rightarrow \Box\Diamond p))^\star \\
&\quad = (\Diamond p \rightarrow p)^\star(\Diamond p \rightarrow \Box\Diamond p)^\star + (\Diamond p \rightarrow p)^\star + (\Diamond p \rightarrow \Box\Diamond p)^\star \\
&\quad = ((\Diamond p)^\star p^\star + (\Diamond p)^\star + 1)((\Diamond p)^\star(\Box\Diamond p)^\star + (\Diamond p)^\star + 1) + (\Diamond p)^\star p^\star + (\Diamond p)^\star + 1 \\
&\qquad + (\Diamond p)^\star(\Box\Diamond p)^\star + (\Diamond p)^\star + 1 \\
&\quad = ((x_{\Box\neg p} + 1)x_p + x_{\Box\neg p} + 1 + 1)((x_{\Box\neg p} + 1)x_{\Box\neg\Box\neg p} + x_{\Box\neg p} + 1 + 1) \\
&\qquad + (x_{\Box\neg p} + 1)x_p + x_{\Box\neg p} + 1 + 1 + (x_{\Box\neg p} + 1)x_{\Box\neg\Box\neg p} + x_{\Box\neg p} + 1 + 1 \\
&\quad \approx_{S5} (x_{\Box\neg p}x_p + x_p + x_{\Box\neg p})((x_{\Box\neg p} + 1)(x_{\Box\neg p} + 1) + x_{\Box\neg p}) \\
&\qquad + x_{\Box\neg p}x_p + x_p + x_{\Box\neg p} + (x_{\Box\neg p} + 1)(x_{\Box\neg p} + 1) + x_{\Box\neg p} \\
&\quad \approx_{S5} x_{\Box\neg p}x_p + x_p + x_{\Box\neg p} + x_{\Box\neg p}x_p + x_p + x_{\Box\neg p} + 1 \\
&\quad \approx_{S5} 1.
\end{aligned}
$$

EXAMPLE 2.11. $\models_{S5} \Box(\Box(p \rightarrow \Box p) \rightarrow p) \rightarrow \Box(\Diamond\Box p \rightarrow p)$*:*

$$
\begin{aligned}
&(\Box(\Box(p \rightarrow \Box p) \rightarrow p) \rightarrow \Box(\Diamond\Box p \rightarrow p))^\star \\
&\quad = (\Box(\Box(p \rightarrow \Box p) \rightarrow p))^\star(\Box(\Diamond\Box p \rightarrow p))^\star + (\Box(\Box(p \rightarrow \Box p) \rightarrow p))^\star + 1 \\
&\quad = x_{\Box(\neg\Box(\neg p\vee\Box p)\vee p)}x_{\Box(\neg\neg\Box\neg\Box p\,\vee p)} + x_{\Box(\neg\Box(\neg p\vee\Box p)\vee p)} + 1 \\
&\quad \approx_{S5} x_{\Box(p\vee\neg\Box(\neg p\vee\Box p))}x_{\Box(p\vee\neg\neg\Box\neg\Box p)} + x_{\Box(p\vee\neg\Box(\neg p\vee\Box p))} + 1 \\
&\quad \approx_{S5} (x_{\Box p}x_{\Box(\neg p\vee\Box p)} + x_{\Box(\neg p\vee\Box p)} + 1)x_{\Box(p\vee\Box\neg\Box p)} + x_{\Box p}x_{\Box(\neg p\vee\Box p)} \\
&\qquad + x_{\Box(\neg p\vee\Box p)} + 1 + 1 \\
&\quad \approx_{S5} (x_{\Box p}(x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p} + x_{\Box p}) + x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p} + x_{\Box p} + 1)(x_{\Box p}x_{\Box\neg\Box p}
\end{aligned}
$$

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

$$+ x_{\Box p} + x_{\Box\neg\Box p}) + x_{\Box p}(x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p} + x_{\Box p}) + x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p} + x_{\Box p}$$

$$\approx_{S5} (x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p}x_{\Box p} + x_{\Box p} + x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p} + x_{\Box p} + 1)(x_{\Box p}(x_{\Box p} + 1)$$

$$+ x_{\Box p} + x_{\Box p} + 1) + x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p}x_{\Box p} + x_{\Box p} + x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p} + x_{\Box p}$$

$$\approx_{S5} x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p} + 1 + x_{\Box\neg p}x_{\Box p} + x_{\Box\neg p}$$

$$\approx_{S5} 1.$$

Reductions in Fact 2.8 are, however, still incomplete if we intend to replace the original polynomial constraints: for instance, a simple $S5$-theorem like $\Box(p \vee \neg p)$ cannot be reduced to the constant polynomial 1. For the purpose of completing the calculus by replacing polynomial constraints (cK), (cB), (c4), and (cNec), we have to introduce additional reductions (which is done in Fact 2.12 and Fact 2.14).

FACT 2.12.

(o) $x_{\Box(\alpha\vee\neg\alpha)} \approx_{S5} 1$, (p) $x_{\Box(\alpha\vee(\beta\vee\neg\beta))} \approx_{S5} 1$.

Proof. Similar to the proof of Fact 2.8. □

With these new reductions the following lemma can be established:

LEMMA 2.13. *Let be* $P = \prod_{i=1}^{n} x_{\Box\alpha_i}$ *where all* α_i *are literals or disjunctions of literals. If* P *is equivalent to the constant polynomial* 1 *(i.e., if* P *takes the value* 1 *for all* $S5$*-PRC-valuations) then* $P \approx_{S5} 1$ *by using only reductions in Fact 2.12.*

Proof. $\prod_{i=1}^{n} x_{\Box\alpha_i}$ is equivalent to the constant polynomial 1 if and only if for any $S5$-PRC-valuation v and all $i = 1, \ldots, n$ we have that $v(x_{\Box\alpha_i}) = 1$, but this is possible only if all α_i have contradictory literals (it is the only way in which a disjunction of literals is a tautology). Then, by applying reductions (0)-(p), all $x_{\Box\alpha_i}$ can be reduced to 1. □

It is also necessary to define reductions obtaining the constant polynomial 0 for products corresponding to contradictory formulas.

FACT 2.14.

(q) $x_{\Box(\alpha\vee\alpha)} \approx_{S5} x_{\Box\alpha}$, (t) $x_{\Box\alpha}x_{\Box(\neg\alpha\vee\beta)} \approx_{S5} x_{\Box\alpha}x_{\Box\beta}$,

(r) $x_{\Box\alpha}x_{\Box(\alpha\vee\beta)} \approx_{S5} x_{\Box\alpha}$, (u) $x_{\Box\neg\alpha}x_{\Box(\alpha\vee\beta)} \approx_{S5} x_{\Box\neg\alpha}x_{\Box\beta}$,

(s) $x_{\Box\alpha}x_{\Box\neg\alpha} \approx_{S5} 0$, (w) $x_{\Box(\alpha\vee\beta)}x_{\Box(\neg\alpha\vee\delta)} \approx_{S5} x_{\Box(\alpha\vee\beta)}x_{\Box(\neg\alpha\vee\delta)}x_{\Box(\beta\vee\delta)}$.

Proof. Similar to the proof of Fact 2.8. □

These reductions lead to the following lemma.

LEMMA 2.15. *Let be* $P = \prod_{i=1}^{n} x_{\Box\alpha_i}$ *where all* α_i *are literals or disjunctions of literals. If* P *is equivalent to the constant polynomial* 0 *(i.e., if* P *takes the value* 0 *for all* $S5$*-PRC-valuations) then* $P \approx_{S5} 0$ *by using only reductions in Fact 2.14.*

Proof. The problem of reducing $P = \prod_{i=1}^{n} x_{\Box\alpha_i}$ to the constant polynomial 0 can be viewed as the process of determining if the clauses α_i are contradictory (or unsatisfiable). Thus, reduction (i) can be viewed as avoiding duplicated literals, reduction (r) eliminates redundant clauses, and reductions (s)-(w) simulate the well-known resolution method for CPL, which is known to be refutation complete. □

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

Now we can proof that reductions in Facts 2.8, 2.12, and 2.14 can replace polynomial constraint (cNec).

LEMMA 2.16. *Let α be an S5-formula such that $\alpha^\star \approx_{S5} 1$, then $x_{\Box\alpha} \approx_{S5} 1$ by using reductions (a)-(w) instead of* (cNec).

Proof. By Lemma 2.9 we have that $x_{\Box\alpha} \approx_{S5} \sum_{i=1}^{n}\prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}$ or $x_{\Box\alpha} \approx_{S5} \left(\sum_{i=1}^{n} \prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}\right) + 1$ (where all $\alpha_{i,j}$ are literals or disjunctions of literals), and reductions (a)-(n) have been used instead of (cK)-(cNec). By Lemmas 2.13 and 2.15 monomials in such polynomials reduce to 1, to 0, or to products of hidden variables whose values are not correlated,[4] and only reductions (o)-(w) have been used. Since reductions (a)-(w) are consequences of the PRC for *S*5 they validate the polynomial constraints (cK)-(cNec). Then, by the presupposition that $\alpha^\star \approx_{S5} 1$ and taking into account the polynomial constraint (cNec), the polynomial in which $x_{\Box\alpha}$ reduces needs to be equivalent to the constant polynomial 1. Consequently, option $x_{\Box\alpha} \approx_{S5} \sum_{i=1}^{n} \prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}$ is avoided. The reason is that sums of irreducible monomials (by any reduction rules) never produce 1 (unless at least a monomial is already 1, but in this situation we would be in the case $x_{\Box\alpha} \approx_{S5} \left(\sum_{i=1}^{n} \prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}\right) + 1$). Then $x_{\Box\alpha} \approx_{S5} \left(\sum_{i=1}^{n} \prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}\right) + 1$ and $\sum_{i=1}^{n} \prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}$ necessarily reduces to 0 (otherwise the polynomial $\left(\sum_{i=1}^{n} \prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}\right) + 1$ is not equivalent to the constant polynomial 1). Therefore, $x_{\Box\alpha} \approx_{S5} \left(\sum_{i=1}^{n} \prod_{j=1}^{m_i} x_{\Box\alpha_{i,j}}\right) + 1 \approx_{S5} 1$ using reductions (a)-(w) instead of (cNec). □

Polynomial constraints (cK), (cB), and (c4) can be also replaced by reductions in Facts 2.8, 2.12, and 2.14 (as it can be easily checked). The PRC obtained by replacing, in Definition 2.7, the polynomial constraints (cK), (cB), (c4), and (cNec) by reductions in Facts 2.8, 2.12, and 2.14 (maintaining (cT)) provides a new sound and complete PRC for *S*5 which we will call the *least hidden variables calculus*, in the sense that only a minimal number of hidden variables is kept (hidden variables $x_{\Box\alpha}$ where α is a literal or a disjunction of literals, this hidden variables will be called *irreducible hidden variables*, due to the fact that they can not be expressed in terms of other variables).

Theorem 2.3 can be generalize to the least hidden-variables calculus:

THEOREM 2.17. *Any polynomial in $F[X \cup X']$ (where X and X' are the sets in Definition 2.7) can be reduced to a unique polynomial in normal form (up to commutativity and associativity), containing only irreducible hidden variables, by means of the reduction relation $\approx_{S5}$ (as defined in the least hidden-variables calculus), for any finite field F.*

Proof. It can be proven, by induction on the complexity of α, that the reduction of $x_{\Box\alpha}$ to polynomials containing only irreducible hidden variables (Lemma 2.9) is unique (up to commutativity and associativity), for any $x_{\Box\alpha}$. By considering this fact, this theorem can be proven in a similar way that Theorem 2.3. □

In contrast with Theorem 2.3, a corollary analogue to Corollary 2.4 cannot be deduced from Theorem 2.17. This is due to the fact that polynomial constraint (cT) imposes a restriction in the assignation of values to irreducible hidden variables. Note, by instance,

[4] If values for hidden variables $x_{\Box\alpha_{i,j}}$ and $x_{\Box\alpha_{i,k}}$ were correlated, they would have a propositional variable in common and all reductions for such cases are contemplated in items (r)-(w).

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

that $(\Box p \rightarrow p)^\star = x_{\Box p}x_p + x_{\Box p} + 1$ always evaluate to 1 due to polynomial constraint (cT). However, $x_{\Box p}x_p + x_{\Box p} + 1$ is a polynomial in normal form and has only irreducible hidden variables. This anomaly can be avoided by replacing the polynomial constraint (cT) by the following equivalent condition:

$$x_{\Box\alpha} \approx_{S5} x_{\Box\alpha}\alpha^\star, \tag{x}$$

which allows to perform deductions in a mechanical way:

THEOREM 2.18. *If polynomial constraint* (cT) *is replaced by* (x) *in the least hidden-variables calculus, then* $\models_{S5} \alpha$ *if and only if* $\alpha^\star \approx_{S5} 1$, *for any formula* α*; without needing the inference metarules* (US) *and* (LR).

Proof. By Theorem 2.17, in the least hidden-variables calculus any formula α can be reduced to a unique polynomial P in normal form containing only irreducible hidden-variables. By applying (x) once to each irreducible hidden variable in P, it is obtained a polynomial Q in which products $x_{\Box\alpha}\alpha^\star$ codify the polynomial constrain (cT) for all hidden variables in P, thus valuations of variables in Q without considering any constraint produce the same results that valuations of P taking into account the polynomial constrain (cT). By reducing Q it is obtained a unique polynomial in normal form, which needs to be the constant polynomial 1 if $P[\overrightarrow{X \cup X'}_v] = 1$ for any valuation v. □

The least hidden-variables calculus contributes to a deeper semantical understanding of modalities: the nondeterminism of modal reasoning is expressed by means of irreducible hidden variables. Moreover, the final polynomial obtained by means of the reduction method described in the proof of Theorem 2.18 can be translated into a CPL formula with 'hidden' propositional variables p'_i, by considering an inverse translation from polynomials into logic formulas (like the function f in Definition 4.3 below, but translating hidden variables to new propositional variables p'_i). This gives a conservative translation from $S5$ into CPL (with hidden propositional variables). This way to understand modal logics has the same spirit of hidden-variable theories for quantum mechanics, whose purpose is to explain the nondeterminism of such physical theories by means of postulating hidden properties.

§3. Soundness and completeness. It is well known, by a clever argument due to James Dugundji (see for instance Carnielli & Pizzi, 2008) that $S5$ and other modal logics cannot be characterized by means of truthfunctional finite-valued matrices—and until now no non-truthfunctional bivalued semantics for this modal logic had been proposed. And indeed, proving soundness and completeness of the PRC for $S5$ cannot be expected to be so easy as in the case of CPL. Moreover, there is not any direct connection between the PRC for $S5$ and other appropriate semantics for this logic, and therefore soundness and completeness must be proven directly.[5]

THEOREM 3.1. (Weak soundness) *If* $\vdash_{S5} \alpha$ *then* $\models_{S5} \alpha$.

Proof. Note that polynomial constraints (cK)-(c4) just establish the validity of, respectively, axioms (K), (T), (B), and (4), and that the polynomial constraint (cNec) establishes

[5] As shown in Section 4, the structure of polynomials in the PRC for $S5$ corresponds to a modal algebra in the class of modal algebras characterizing $S5$, but this does not directly entail the completeness for the PRC. Indeed, completeness results for modal algebras refer to a class of algebras, not to a specific algebra.

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

validity preservation under the necessitation rule (Nec). This, in conjunction with the fact that all CPL formulas are valid (because the PRC for $S5$ is an extension of the PRC for CPL), leads to the weak soundness. □

THEOREM 3.2. (Strong soundness) *If* $\Gamma \vdash_{S5} \alpha$ *then* $\Gamma \models_{S5} \alpha$.

Proof. The result is a consequence of the finite character of proofs, the validity of the metatheorem of deduction for $S5$ and the weak soundness above. □

The strong completeness theorem is proven by adapting the familiar Lindenbaum–Asser argument for CPL. Before establishing the theorem, a definition and some lemmas are in order.

DEFINITION 3.3. (φ-$S5$-saturated set) *Let* Γ *be a set of S5-formulas and let* φ *and* α *be S5-formulas.* Γ *is a* φ-$S5$-saturated set *if satisfies the following two conditions:*

1. $\Gamma \nvdash_{S5} \varphi$,
2. *if* $\alpha \notin \Gamma$ *then* $\Gamma, \alpha \vdash_{S5} \varphi$.

LEMMA 3.4. *Let* Γ *be a set of S5-formulas and let* φ *be an S5-formula. If* $\Gamma \nvdash_{S5} \varphi$ *then there exists a set* Δ *such that* $\Gamma \subseteq \Delta$ *and* Δ *is* φ-$S5$-*saturated.*

Proof. The proof is the same as for CPL. □

LEMMA 3.5. *Let* Γ *be a* φ-$S5$-*saturated set and let* $Y = \{x_{\alpha_1}, x_{\alpha_2}, \ldots\}$ *be a set of algebraic variables indexed by S5-formulas. We define the function* $v\colon Y \to \{0,1\}$ *by* $v(x_{\alpha_i}) = C_\Gamma(\alpha_i)$ *(where* C_Γ *is the characteristic function of* Γ*, i.e.,* $C_\Gamma(\alpha_i) = 1$ *if* $\alpha_i \in \Gamma$*, and* $C_\Gamma(\alpha_i) = 0$ *otherwise). Thus, for any S5-formulas* α *and* β*,* Γ *and* v *satisfy the following properties:*

1. $\alpha \in \Gamma$ *if and only if* $\Gamma \vdash_{S5} \alpha$,
2. $\neg\alpha \in \Gamma$ *if and only if* $\alpha \notin \Gamma$,
3. $(\alpha \to \beta) \in \Gamma$ *if and only if* $\alpha \notin \Gamma$ *or* $\beta \in \Gamma$,
4. *if* $\vdash_{S5} \alpha$ *then* $\Box\alpha \in \Gamma$,
5. *the restriction of* v *to variables in* $X \cup X'$ *is a S5-PRC-valuation.*

Proof. Items 1, 2, and 3 are proven as in CPL, while other items are proven below. In some places of the proof we will use the fact that $v(x_\alpha) = \alpha^\star[\overrightarrow{X \cup X'_v}]$; this fact can be easily proven by induction.

4. Suppose that $\vdash_{S5} \alpha$, by (Nec) it is obtained that $\vdash_{S5} \Box\alpha$. Then, by monotonicity and Item 1 we have that $\Box\alpha \in \Gamma$.
5. We will prove that v validates, respectively, polynomial constraints (cK)-(cNec):

   (i) If $\Box(\alpha \to \beta) \notin \Gamma$, by definition of v, $v(x_{\Box(\alpha\to\beta)}) = 0$. Then, independently of the values of $v(x_{\Box\alpha})$ and $v(x_{\Box\beta})$, we have that $v(x_{\Box(\alpha\to\beta)})(v(x_{\Box\alpha})(v(x_{\Box\beta}) + 1)) = 0$.
   If $\Box(\alpha \to \beta) \in \Gamma$ by Item 1 it follows that $\Gamma \vdash_{S5} \Box(\alpha \to \beta)$. Moreover, $\Box(\alpha \to \beta) \vdash_{S5} \Box\alpha \to \Box\beta$, then $\Gamma \vdash_{S5} \Box\alpha \to \Box\beta$. Then, by Item 1 we have that $(\Box\alpha \to \Box\beta) \in \Gamma$, and by Item 3 it follows that $\Box\alpha \notin \Gamma$ or $\Box\beta \in \Gamma$. Consequently, by definition of v, $v(x_{\Box\alpha}) = 0$ or $v(x_{\Box\beta}) = 1$, and in both cases $v(x_{\Box(\alpha\to\beta)})(v(x_{\Box\alpha})(v(x_{\Box\beta}) + 1)) = 0$.

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

(ii) If $\Box\alpha \notin \Gamma$, by definition of v, $v(x_{\Box\alpha}) = 0$. Then, independently of the value of $v(x_\alpha)$, we have that $v(x_{\Box\alpha})(v(x_\alpha) + 1) = 0$ (i.e., $v(x_{\Box\alpha})(\alpha^\star[\overrightarrow{X \cup X'}_v] + 1) = 0$).
If $\Box\alpha \in \Gamma$ by Item 1 it follows that $\Gamma \vdash_{S5} \Box\alpha$. Moreover, we have that $\Box\alpha \vdash_{S5} \alpha$, then $\Gamma \vdash_{S5} \alpha$ and Item 1 imply that $\alpha \in \Gamma$. Therefore, by definition of v, $v(x_\alpha) = 1$. Consequently, $v(x_{\Box\alpha})(v(x_\alpha) + 1) = 0$ (i.e., $v(x_{\Box\alpha})(\alpha^\star[\overrightarrow{X \cup X'}_v] + 1) = 0$).

(iii) If $\alpha \notin \Gamma$, by definition of v, $v(x_\alpha) = 0$. Then, independently of the value of $v(x_{\Box\Diamond\alpha})$, we have that $v(x_\alpha)(v(x_{\Box\Diamond\alpha}) + 1) = 0$ (i.e., $\alpha^\star[\overrightarrow{X \cup X'}_v](v(x_{\Box\Diamond\alpha}) + 1) = 0$).
If $\alpha \in \Gamma$, by Item 1 $\Gamma \vdash_{S5} \alpha$. Moreover, we have that $\alpha \vdash_{S5} \Box\Diamond\alpha$, then $\Gamma \vdash_{S5} \Box\Diamond\alpha$ and by Item 1 it follows that $\Box\Diamond\alpha \in \Gamma$. Therefore, by definition of v, $v(x_{\Box\Diamond\alpha}) = 1$. Consequently, $v(x_\alpha)(v(x_{\Box\Diamond\alpha}) + 1) = 0$ (i.e., $\alpha^\star[\overrightarrow{X \cup X'}_v](v(x_{\Box\Diamond\alpha}) + 1) = 0$).

(iv) If $\Box\alpha \notin \Gamma$, by definition of v, $v(x_{\Box\alpha}) = 0$. Then, independently of the value of $v(x_{\Box\Box\alpha})$, we have that $v(x_{\Box\alpha})(v(x_{\Box\Box\alpha}) + 1) = 0$.
If $\Box\alpha \in \Gamma$, Item 1 implies that $\Gamma \vdash_{S5} \Box\alpha$. Moreover, as $\Box\alpha \vdash_{S5} \Box\Box\alpha$, then $\Gamma \vdash_{S5} \Box\Box\alpha$ and, by Item 1, $\Box\Box\alpha \in \Gamma$. Therefore, by definition of v, $v(x_{\Box\Box\alpha}) = 1$. Consequently, $v(x_{\Box\alpha})(v(x_{\Box\Box\alpha}) + 1) = 0$.

(v) Suppose that $v(x_{\Box\alpha}) = 0$, then by definition of v, $\Box\alpha \notin \Gamma$; and therefore, by Item 1, $\nvdash_{S5} \alpha$. This, in conjunction with Lemma 3.4 implies the existence of a α-$S5$-saturated set Δ such that $\alpha \notin \Delta$. Let the function v' be defined as v, but considering the set Δ instead of Γ. Then, $v'(\alpha^\star) = 0$ and consequently $\alpha^\star[\overrightarrow{X \cup X'}_{v'}] = 0$, that is, $\alpha^\star \not\approx_{S5} 1$. □

THEOREM 3.6. (Strong completeness) *If* $\Gamma \not\approx_{S5} \alpha$ *then* $\Gamma \vdash_{S5} \alpha$.

Proof. Suppose that $\Gamma \nvdash_{S5} \alpha$. By Lemma 3.4 there exists a α-$S5$-saturated set Δ such that $\Gamma \subseteq \Delta$. Then, by Lemma 3.5, the function $v\colon Y \to \{0, 1\}$ (where $Y = \{x_{\alpha_1}, x_{\alpha_2}, \ldots\}$) defined by $v(x_{\alpha_i}) = C_\Delta(\alpha_i)$, when restricted to variables in $X \cup X'$, is a $S5$-valuation. Therefore, by definition of v and by the fact that $v(x_\alpha) = \alpha^\star[\overrightarrow{X \cup X'}_v]$, we have that $\gamma^\star[\overrightarrow{X \cup X'}_v] = 1$ for all $\gamma \in \Gamma$ and that $\alpha^\star[\overrightarrow{X \cup X'}_v] = 0$. Then, $\Gamma \not\approx_{S5} \alpha$. □

§4. A connection to modal algebras. In Lemmon (1966a, 1966b), Edward J. Lemmon defines a series of *modal algebras* (also called *Boolean algebras with operators* in other contexts) characterizing different modal logics, where the strongest system is $S5$. We show here how the polynomials in the PRC for $S5$ can be regarded as a modal algebra (in the class of modal algebras characterizing $S5$). Before that, we will present the required definitions and a theorem from Lemmon (1966a, 1966b). Definitions are adapted to consider the operator **n** (for necessity) as primitive, instead of **p** (for possibility). The operator **n** is used to interpret $\Box$ and **p** is defined by $\mathbf{p}(x) \stackrel{\text{def}}{=} -\,\mathbf{n}(-\,x)$, so as to interpret $\Diamond$:

DEFINITION 4.1. *A structure* $\mathcal{M} = \langle M, \sqcup, \sqcap, -, \mathbf{n}\rangle$ *is a* modal algebra *if* M *is a set of elements closed under operations* $\sqcup$, $\sqcap$, $-$ *and* **n** *such that:*

1. $\langle M, \sqcup, \sqcap, -\rangle$ *is a Boolean algebra, and*
2. $\mathbf{n}(x \sqcap y) = \mathbf{n}(x) \sqcap \mathbf{n}(y)$, *for all* $x, y \in M$.

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

A modal algebra is *normal* if $\mathbf{n}(1) = 1$. A normal modal algebra is *epistemic* if $\mathbf{n}(x) \leq x$, *symmetric* if $x \leq \mathbf{n}(\mathbf{p}(x))$ and *transitive* if $\mathbf{n}(\mathbf{n}(x)) = \mathbf{n}(x)$, for all $x \in M$.

THEOREM 4.2. *$\vdash_{S5} \alpha$ if and only if α is satisfied by all (finite) normal epistemic symmetric and transitive modal algebras.*

Proof. Cf., in Lemmon (1966b). □

In order to regard the structure of polynomials in $\mathbb{Z}_2[X \cup X']$ as an (infinite) normal-epistemic-symmetric and transitive modal algebra, we first define a function relating polynomials with $S5$-formulas:

DEFINITION 4.3. *Let P, Q and R be polynomials in $\mathbb{Z}_2[X \cup X']$, we recursively define the function $f\colon \mathbb{Z}_2[X \cup X'] \to For S5$ by:*

$$f(P) = \begin{cases} p \vee \neg p \text{ if } P = 1 \text{ (the constant polynomial } 1), \\ p \wedge \neg p \text{ if } P = 0 \text{ (the constant polynomial } 0), \\ \alpha \text{ if } P = x_\alpha, \\ f(Q) \wedge f(R) \text{ if } P = QR, \\ f(Q) \veebar f(R) \text{ if } P = Q + R. \end{cases} \tag{1}$$

where the connective $\veebar$ represents the exclusive or (i.e., $\alpha \veebar \beta \stackrel{\text{def}}{=} (\alpha \vee \beta) \wedge \neg(\alpha \wedge \beta)$).

The following operations on $\mathbb{Z}_2[X \cup X']$ are thus defined:

DEFINITION 4.4. *Let P and Q be polynomials in $\mathbb{Z}_2[X \cup X']$, operations $\sqcup$, $\sqcap$, $-$ and $\mathbf{n}$ are defined by:*

- $P \sqcup Q = PQ + P + Q$,
- $P \sqcap Q = PQ$,
- $- P = P + 1$,
- $\mathbf{n}(P) = x_{\Box f(P)}$.

The following relations are also defined:

DEFINITION 4.5. *Let P and Q be polynomials in $\mathbb{Z}_2[X \cup X']$; then, relations $\lesssim$ and $\cong$ are defined by:*

- $P \lesssim Q$ *if* $Q[\overrightarrow{X \cup X'}_v] = 0$ *implies* $P[\overrightarrow{X \cup X'}_v] = 0$ *for all S5-PRC-valuations v.*
- $P \cong Q$ *if* $P \lesssim Q$ *and* $Q \lesssim P$.

It is easy to show that $\lesssim$ is a preorder relation and that $\cong$ is an equivalence relation. Then $\cong$ partitions $\mathbb{Z}_2[X \cup X']$ in the quotient set $\mathbb{Z}_2[X \cup X']/\cong = \{[P] : P \in \mathbb{Z}_2[X \cup X']\}$, where $[P] = \{Q \in \mathbb{Z}_2[X \cup X'] : Q \cong P\}$ denotes the equivalence class of P. Moreover, $\cong$ is a congruence with respect to the operations in Definition 4.4. The following operations can thus be defined on $\mathbb{Z}_2[X \cup X']/\cong$:

DEFINITION 4.6. *Let $[P]$ and $[Q]$ be equivalence classes in $\mathbb{Z}_2[X \cup X']/\cong$, operations $\sqcup'$, $\sqcap'$, $-'$ and $\mathbf{n}'$ are defined by:*

- $[P] \sqcup' [Q] = [PQ + P + Q]$,
- $[P] \sqcap' [Q] = [PQ]$,
- $-' [P] = [P + 1]$,
- $\mathbf{n}'([P]) = [x_{\Box f(P)}]$.

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

The order relation $\lesssim'$ on $\mathbb{Z}_2[X \cup X']/\cong$ is defined by $[P] \lesssim' [Q]$ if $P \lesssim Q$.
Now, the following theorem can be proven:

THEOREM 4.7. *The structure* $\mathcal{Z} = \langle \mathbb{Z}_2[X \cup X']/\cong, \sqcup', \sqcap', -', \mathbf{n}' \rangle$, *with the order* $\lesssim'$, *is an (infinite) normal epistemic symmetric and transitive modal algebra.*

Proof.

- $\mathcal{Z}$ is a modal algebra:
  - It is easy to prove that $\langle \mathbb{Z}_2[X \cup X']/\cong, \sqcup', \sqcap', -' \rangle$ is a Boolean algebra, with [0] and [1] (the classes of the constant polynomials 0 and 1) being respectively the elements 0 and 1 of the algebra.
  - Let $[P]$ and $[Q]$ equivalence classes in $\mathbb{Z}_2[X \cup X']/\cong$; we have then:

$$\begin{aligned}
\mathbf{n}'([P] \sqcap' [Q]) &= \mathbf{n}'([PQ]) \text{ (by definition of } \sqcap') \\
&= [x_{\Box f(PQ)}] \text{ (by definition of } \mathbf{n}') \\
&= [x_{\Box(f(P) \wedge f(Q))}] \text{ (by definition of } f) \\
&= [x_{\Box f(P)} x_{\Box f(Q)}] \text{ (by item (a) in Fact 2.8)} \\
&= [x_{\Box f(P)}] \sqcap' [x_{\Box f(Q)}] \text{ (by definition of } \sqcap') \\
&= \mathbf{n}'([P]) \sqcap' \mathbf{n}'([Q]) \text{ (by definition of } \mathbf{n}').
\end{aligned}$$

- $\mathcal{Z}$ is normal, epistemic, symmetric and transitive, as a direct consequence of, respectively, the polynomial constraints (cNec), (cT), (cB), and (c4). □

The previous result shows that the structure $\mathcal{Z}$ defined on the algebra of polynomial classes in $\mathbb{Z}_2[X \cup X']$ is a particular modal algebra, so the PRC makes a very natural bridge between semantics and algebra. From this point of view, PRC is an almost organic extension of the 'Boolean setting', so characteristic of classical logic, to modal domains.

§5. A polynomial ring calculus with operators for *S5*. In Section 2 a PRC for *S5* was defined by using hidden variables and establishing polynomial constraints in order to reduce them to a minimal set, obtaining a mechanical proof method. In such a method subindexes of variables play an important role: they are not only a simple enumeration (like in the conventional way), but they identify algebraic variables with propositions, and permit to establish correlations among variables by using propositional schemas.

In this section, another way to define a polynomial ring calculus for *S5* is introduced. The new method is based on the definition of operators in modal algebras (see Section 4). The idea consists in replacing hidden variables by operators and in identifying operators applied to irreducible polynomials with (irreducible) hidden variables. In this calculus, contrary to the previous one, subindexes operate in the conventional way.

DEFINITION 5.1. (PRC with operators for *S5*) *Let* $For S5$ *be the set of well-formed formulas of S5, and let* $X = \{x_1, x_2, \ldots\}$ *and* $X' = \{x'_1, x'_2, \ldots\}$ *be disjoint sets of algebraic variables. Variables in* X' *are called* hidden variables. *The* PRC with operators for *S5 is determined by the translation function* †: $For S5 \to \mathbb{Z}_2[X \cup X']$, *recursively defined by:*

$$(p_i)^\dagger = x_i \text{ if } p_i \text{ is a propositional variable},$$

$$(\neg\alpha)^\dagger = \alpha^\dagger + 1,$$

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

$$(\alpha \wedge \beta)^\dagger = \alpha^\dagger \beta^\dagger,$$
$$(\alpha \vee \beta)^\dagger = \alpha^\dagger \beta^\dagger + \alpha^\dagger + \beta^\dagger,$$
$$(\alpha \to \beta)^\dagger = \alpha^\dagger \beta^\dagger + \alpha^\dagger + 1,$$
$$(\Box\alpha)^\dagger = \mathbf{n}(\alpha^\dagger),$$
$$(\Diamond\alpha)^\dagger = \mathbf{n}(\alpha^\dagger + 1) + 1.$$

where n is an operator on polynomials *subject to the following reduction conditions:*[6]

$$\mathbf{n}(PQ) \approx'_{S5} \mathbf{n}(P)\mathbf{n}(Q), \tag{n1}$$
$$\mathbf{n}(1) \approx'_{S5} 1, \tag{n2}$$
$$\mathbf{n}(P) \approx'_{S5} \mathbf{n}(P)P, \tag{n3}$$
$$\mathbf{n}(\mathbf{n}(P)) \approx'_{S5} \mathbf{n}(P), \tag{n4}$$
$$\mathbf{n}(P + \mathbf{n}(Q)) \approx'_{S5} \mathbf{n}(PQ) + \mathbf{n}((P+1)Q) + \mathbf{n}(P), \tag{n5}$$
$$\mathbf{n}(P + \mathbf{n}(Q)R) \approx'_{S5} \mathbf{n}(PQ + QR) + \mathbf{n}(PQ) + \mathbf{n}(P); \tag{n6}$$

and **n** *applied to a nonconstant polynomial in normal form can be considered to be a hidden variable, that is:*

$$\mathbf{n}(P) \approx'_{S5} x'_i, \text{ for some } i, \text{ if } P \text{ is in normal form, } P \neq 1 \text{ and } P \neq 0. \tag{n7}$$

Operators in the Definition 5.1 can be viewed as a mechanism to extract hidden variables.

The PRC with operator for *S*5 is equivalent to the least hidden variable calculus presented in Section 2:

THEOREM 5.2. $\approx_{S5} \alpha$ *if and only if* $\approx'_{S5} \alpha$, *and* $\alpha \approx_{S5} 1$ *if and only if* $\alpha \approx'_{S5} 1$.

Proof. In one direction, terms with operators $\mathbf{n}(P)$ can be translated into hidden variables $x_{\Box f(P)}$, and the polynomial constraints (a)-(x) can be obtained from the translation of the reduction conditions (n1)-(n7). In the other direction, hidden variables $x_{\Box\alpha}$ can be translated into terms with operators $\mathbf{n}(\alpha^\dagger)$, and the reduction conditions (n1)-(n7) can be obtained from the translation of the polynomial constraints (a)-(x). □

The following example illustrates how deductions can be performed in this new version of the PRC for *S*5:

EXAMPLE 5.3. $\approx'_{S5} \Box p_1 \to (\Box\Box(p_1 \vee (p_2 \wedge \neg p_2)))$:

$$\begin{aligned}
&(\Box p_1 \to (\Box\Box(p_1 \vee (p_2 \wedge \neg p_2))))^\dagger \\
&\quad = (\Box p_1)^\dagger (\Box\Box(p_1 \vee (p_2 \wedge \neg p_2)))^\dagger + (\Box p_1)^\dagger + 1 \\
&\quad = \mathbf{n}((p_1)^\dagger)\mathbf{n}(\mathbf{n}((p_1 \vee (p_2 \wedge \neg p_2))^\dagger)) + \mathbf{n}((p_1)^\dagger) + 1 \\
&\quad = \mathbf{n}(x_1)\mathbf{n}(\mathbf{n}(x_1(x_2(x_2+1)) + x_1 + (x_2(x_2+1)))) + \mathbf{n}(x_1) + 1
\end{aligned}$$

[6] With the objective to differentiate the calculus, symbols $\approx'_{S5}$ and $\approx'_{S5}$ will be used in the new calculus instead of $\approx_{S5}$ and $\approx_{S5}$.

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

$$\approx'_{S5} x'_1\mathbf{n}(\mathbf{n}(x_1)) + x'_1 + 1$$
$$\approx'_{S5} x'_1\mathbf{n}(x_1) + x'_1 + 1$$
$$\approx'_{S5} x'_1x'_1 + x'_1 + 1$$
$$\approx'_{S5} 1.$$

§6. Polynomial reductions as an equational theory. As it is defined by Tarski in Tarski (1968, p. 276), equational logic is "The part of predicate logic in which equations are the only admitted formulas." In such a logic, equations are treated as if all variables were universally quantified; the only axiom is $x = x$ and the deduction rules are uniform substitution and the replacing of equals by equals. Thus, by using equational logic, from a set of equations (in a given language) it is possible to deduce other equations. An *equational theory* is defined as a set θ containing all equations derivable from a set of equations Σ; such a set Σ is called a *basis* for θ. The *equational theory of an algebra* A is the set of all equations satisfied by A and the *equational theory of a class of algebras* K is the set of equations satisfied by all the algebras in K. Moreover, a class of algebras K is *equationally defined* if there exists a set of equations Σ such that $K = \text{Mod}\,\Sigma$, where Mod Σ is the class of models for the theory Σ. When *equational implications* (i.e., implications where antecedent and consequent are equations) are also considered as axioms such theories are called *quasi-equational*.[7]

The ring rules and the polynomial rules defined in the PRC, if treated as equations, can be viewed as defining a basis for an equational theory (where the uniform substitution and the Leibniz rule correspond, respectively, to the uniform substitution and the replacing of equals by equals in equational logic). In the case of CPL, the polynomial reductions in the PRC equationally define the class of Boolean rings. It is well known that Boolean rings and Boolean algebras are term-definitional equivalents, and that the Boolean algebra of two elements is a generic algebra for the class of Boolean algebras. These facts, in conjunction with the fact that Boolean algebras are an adequate semantic for CPL, imply the soundness and completeness of the PRC for CPL. The polynomial reductions of the PRC for $S5$ (Definition 2.7), containing polynomial constraints (cK)-(cNec), can be viewed as a quasi-equational theory extending the equational theory for Boolean rings. The PRC for $S5$ in the least hidden-variables calculus version, can be viewed as an equational theory extending the equational theory for Boolean rings.

In spite of Boolean rings and Boolean algebras being term-definitional equivalents, there are substantial distinctions between them. Indeed, as pointed out in Dershowitz *et al.* (2004), "The Boolean-ring formalism differs from Boolean algebra in that it defines a unique normal form (up to commutativity and associativity of the two operators) for every Boolean formula, called a *Boolean polynomial* (also known as a *Zhegalkin polynomial* or *Reed-Muller normal form*)." Such property is useful for the definition of proof methods for propositional logic and to test satisfiability (see Hsiang & Huang, 1997, and Dershowitz *et al.* , 2004). Another fundamental distinction between Boolean rings and Boolean algebras is that Boolean rings directly generalize toward many-valued logics (by means of polynomials over finite Galois fields, see e.g., Carnielli, 2005) while Boolean algebras do not. The PRC reduction rules extend the Boolean polynomials preserving their good properties,

[7] For a good survey of equational logic see Taylor (1979).

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

which permit to perform deductions in nonclassical logics. In the case of modal logics, the PRC here defined is naturally extensible to modal logics based on many-valued logics, paraconsistent logics, and other nonclassical logics characterized by PRC. But not only that, the PRC also establishes a relationship between syntactic deductions in propositional calculus and polynomial handling, in some cases showing how the 'nondeterminism' of logics noncharacterizable by finite matrices can be expressed by means of hidden variables, which represent a new insight in the study of nonclassical logics.

§7. Defining equational proof systems from PRC. In Dijkstra & Scholten (1990), Edsger W. Dijkstra and Carel S. Scholten introduce a proof format in which the replacement of logically equivalent formulas is emphasized (instead of using modus ponens), in such a way that deductions are fulfilled in an equational fashion. The Dijkstra–Scholten equational proof style is formalized for the propositional logic in Gries & Schneider (1995) (where some advantages of that method over the traditional Hilbert-style proofs are also pointed) and for the intuitionistic logic in Bohórquez (2008). Defining an equational proof system (*à la* Dijkstra-Scholten) for a specific logic basically consists of determining a complete set of logical equivalences from which all theorems of the logic can be deduced (by replacement of equivalent formulas and uniform substitution). As it was described in the previous section, the polynomial reductions of the PRC for $S5$ (in the least hidden-variables calculus version) can be viewed as equations. Such algebraic equations have a direct correspondence with equivalences between formulas in $S5$ (by the inverse translation from polynomials to formulas in Definition 4.3) which, by Theorems 2.18, 3.2, and 3.6, are adequate to axiomatize $S5$ in Dijkstra–Scholten style. Following such guidelines, equational proof systems can be defined for other logics, provided they are characterized by a PRC, as in the case of many-valued logics and some paraconsistent logics. Consequently, PRC can be regarded as a general framework to study equational proof systems.

On the other hand, *rewriting systems* are a kind of equational theories with directed equations, under the condition that the term on the left can be replaced by the term on the right (but not in the other direction). In Hsiang (1985) a rewriting system for CPL is defined, in which the rewriting rules are straightforward translations of the axioms of Boolean rings (except for the axioms concerning commutativity and associativity of the operators, because terms which are equivalent modulo such properties are considered as equals). It is then proven that the rewriting system is *canonical*, in the sense that any sequence of reductions always terminate in an irreducible term (systems with this property are called *Noetherian*) and that any sequence of rewrites lead to the same final term (systems with this property are called *confluent*). Note that this rewriting system can be easily obtained from the PRC for CPL, by avoiding reductions concerning commutativity and associativity and by establishing the equality of terms modulo such properties.

In Foret (1988), the rewriting system defined in Hsiang (1985) is extended to the modal propositional systems K, Q, T, and $S5$. The rewrite rules are defined by the axioms of Boolean rings with operators. Such extensions are natural for K and Q, but for T and $S5$ strange translations and operators are inserted in order to obtain canonical systems. The least hidden-variables calculus for $S5$ here defined can be used to define a more natural rewriting system for $S5$, where the polynomial reductions (a)-(x) correspond to rewriting rules.

PRC is thus an algebraic foundation for logic, general enough not only to define equational theories of proof and rewriting systems for a wide range of logics, but also useful to

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

providing a new perspective in the semantic understanding of nonclassical logics as logics of bounded nondeterminism.

§8. Assessing the new method. The PRC for $S5$ can be easily adapted to other modal logics: for the systems K, T, B, and $S4$ it is sufficient just to disregard the polynomial constraints corresponding to axioms not in the respective system (in all versions, with polynomial constraints (cK)-(cNec), in the least hidden-variables calculus as well as in the calculus with operators) and to make some adaptations on lemmas and theorems. For other modal logics extending the CPL the same translation function can be taken, and polynomial constraints can be defined by translating axioms to polynomials, equaling them to the constant polynomial 1, and defining implications between polynomials in order to validate deduction rules. This can be done without much ado by considering the well-known Lemmon–Scott axioms $\Diamond^k\Box^l\alpha \rightarrow \Box^m\Diamond^n\alpha$ and adding the constraint $x_{\Diamond^k\Box^l}(x_{\Box^m\Diamond^n} + 1) \approx 0$ (with $x_{\Diamond\alpha}$ meaning $x_{\Box\neg\alpha} + 1$) to the polynomial constraints (cK) and (cNec).[8] In this way, soundness and completeness theorems obtained for $S5$ can be adapted to other PRCs. Moreover, a relationship with their respective modal algebras can also be obtained: new polynomial constraints will correspond to algebraic conditions over the operator **n**. The PRC with operators can also be easily adapted, by considering new reduction conditions in accordance with the rules of operators in the respective modal algebra.

A PRC for $S4$ has an extra feature, since intuitionistic logic could in principle be also treated in polynomial terms keeping 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 the above defined PRC for $S5$, although for other calculi connections with the finite-model property would have to be established.

The PRC for modal logic is also related to the *nondeterministic matrices* (cf., Avron & Zamansky, 2007), a generalization of ordinary multivalued matrices in which the truth-value of a formula can be nondeterministically assigned: actually, our method can also be seen as the first example of nondeterministic semantics for modal logics. Such semantics constitutes a particular case of *possible-translations semantics* (cf., Carnielli *et al.*, 2007)—not by accident, since the latter are more expressive than the former, as argued in Carnielli & Coniglio (2005) (Theorem 38 and the following discussion).

There are some interesting problems left open. For instance, our PRC calculi are already cut-free, and in fact resolution amounts to solving polynomial systems. However, we have made no attempts to study the algorithmic properties therein. Another question is to generalize the underlying algebraic setting in order to treat other logics: as much as we assumed the 'ring rules' (cf., Section 2) one could investigate the interest of representing logical concepts by formal polynomials over semirings, Kleene algebras, or even groups.

Our PRC for modal logics can be also seen as a simple system of equational logic. It is not surprising that the quotient equational logic constitutes a modal algebra (cf., Section 4): as a slogan in Blackburn *et al.* (2002, p. xiv) defends, from the point of view of universal algebra modal logic is essentially the study of certain varieties of equational logic. What is surprising is how elementary the method is, and how easy it is to handle the resulting high school–fashion polynomial calculus.

[8] To define PRCs in terms of more elaborated polynomial reductions additional work is needed, following a similar way of gradually obtaining deeper relations between hidden variables, so as to obtain a complete set of reductions allowing mechanical proofs.

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

Acknowledgments. This research was supported by FAPESP, Fundação de Amparo à Pesquisa do Estado de São Paulo, Brazil, Thematic Research Project Grant 2004/14107-2. The first author has been also supported by a FAPESP Ph.D. Scholarship Grant 05/04123-3, and the second by a CNPq (Brazil) Research Grant 300702/2005-1 and by the Fonds National de la Recherche Luxembourg.

We would also like to thank several people who have heard about these ideas on several occasions, and have contributed with suggestions and criticisms: Roy Dickhoff, Justus Diller, J. Michael Dunn, Josep Font, Graham Priest, Heinrich Wansing, Jørgen Villadsen, and Didier Dubois. We thank, as well, a careful referee for his valuable remarks and comments on a previous version of the paper.

BIBLIOGRAPHY

Avron, A., & Zamansky, A. (2007). Generalized non-deterministic matrices and (n,k)-ary quantifiers. In Artemov, S., and Nerode, A., editors. *Proceedings of the Symposium on Logical Foundations of Computer Science, LNCS 4514*. Berlin/Heidelberg: Springer, pages 26–40.

Blackburn, P., & Benthem, J. v. (2006). Modal logic: A semantic perspective. In Blackburn, P., van Benthem, J., and Wolter, F., editors. *Handbook of Modal Logic*. Amsterdam: Elsevier North-Holland, pp. 1–82.

Blackburn, P., de Rijke, M., & Venema, Y. (2002). *Modal Logic*. Cambridge, UK: Cambridge University Press.

Bohórquez, J. A. (2008). Intuitionistic logic according to dijkstra's calculus of equational deduction. *Notre Dame Journal of Formal Logic*, **49**(4), 361–384.

Carnielli, W., & Pizzi, C. (2008). *Modalities and Multimodalities*. Amsterdam: Springer.

Carnielli, W. A. (2005). Polynomial ring calculus for many-valued logics. In Werner, B., editor. *Proceedings of the 35th International Symposium on Multiple-Valued Logic*. Los Alamitos: IEEE Computer Society, 2005, pp. 20–25. Preprint available at *CLE e-Prints* vol 5, n. 3: `www.cle.unicamp.br/e-prints/vol_5,n_3,2005.html`.

Carnielli, W. A. (2007). Polynomizing: Logic inference in polynomial format and the legacy of Boole. In Magnani, L., and Li, P., editors. *Model-Based Reasoning in Science, Technology, and Medicine*, Volume 64 of *Studies in Computational Intelligence*. Berlin/Heidelberg: Springer, pp. 349–364.

Carnielli, W. A., & Coniglio, M. E. (2005). Splitting logics. In *We Will Show Them! Essays in Honour of Dov Gabbay*. London: College Publications, pp. 389–414.

Carnielli, W. A., Coniglio, M. E., & Marcos, J. (2007). Logics of formal inconsistency. In Gabbay, D., and Guenthner, F., editors. *Handbook of Philosophical Logic* (second edition), Vol. 14. Berlin/Heidelberg: Springer, pp. 15–107. Preprint available at *CLE e-Prints* vol 5, n. 1. `www.cle.unicamp.br/e-prints/vol_5,n_1,2005.html`.

Dershowitz, N., Hsiang, J., Huang, G. S., & Kaiss, D. (2004). Boolean ring satisfiability. In Hoos, Holger H., & Mitchell, David C., editors. *Proceedings of the Seventh International Conference on Theory and Applications of Satisfiability Testing (SAT 2004)*. Berlin/Heidelberg: Springer, pp. 281–286.

Dijkstra, E. W., & Scholten, C. S. (1990). *Predicate Calculus and Program Semantics*. New York: Springer-Verlag.

Fagin, R., & Vardi, M. Y. (1985). An internal semantics for modal logic. In Sedgewick, Robert, editor. *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing (1985)*. New York: Association for Computing Machinery, pp. 305–315.

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press

Foret, A. (1988). Rewrite rule systems for modal propositional logic. In Grabowski, J., Lescanne, P., & Wechler, W., editors. *Proceedings of the International Workshop on Algebraic and Logic Programming*, Volume 343 of *Lecture Notes in Computer Science*. Berlin/Heidelberg: Springer Verlag, pp. 147–156.

Goldblatt, R. (2005). Mathematical modal logic: A view of its evolution. In Gabbay, D. M., and Woods, J., editors. *Handbook of the History of Logic*, Vol. 6. Amsterdam: Elsevier, pp. 1–98.

Gries, D., & Schneider, F. B. (1995). Equational propositional logic. *Information Processing Letters*, **53**, 145–152.

Hsiang, J. (1985). Refutational theorem proving using term-rewriting systems. *Artificial Intelligence*, **25**, 255–300.

Hsiang, J., & Huang, G. S. (1997). Some fundamental properties of Boolean ring normal forms. In Du, D., Gu, J., and Pardalos, P. M., editors. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, Vol. 35. Providence, RI, USA: American Mathematical Society, pp. 587–602.

Kuczynski, J.-M. (2007). Does possible world semantics turn all propositions into necessary ones? *Journal of Pragmatics*, **39**(5), 872–916.

Lemmon, E. J. (1966a). Algebraic semantics for modal logics I. *Journal of Symbolic Logic*, **31**(1), 46–65.

Lemmon, E. J. (1966b). Algebraic semantics for modal logics II. *Journal of Symbolic Logic*, **31**(2), 191–218.

Quine, W. V. O. (2006). From a logical point of view: Nine logico-philosophical essays. In *Two Dogmas of Empiricism*. Harvard University Press, pp. 20–46.

Tarski, A. (1968). Equational logic and equational theories of algebra. In Schmidt, H. A., Schütte, K., & Thiele, H. J. editors. *Contributions to Mathematical Logic*. Amsterdam: North Holland, pp. 275–288.

Taylor, W. (1979). Equational logic. *Houston Journal of Mathematics*, **5**, 1–51.

PH.D. PROGRAM IN PHILOSOPHY, AREA OF LOGIC,
IFCH AND GROUP FOR APPLIED AND THEORETICAL LOGIC—CLE,
STATE UNIVERSITY OF CAMPINAS—UNICAMP
BRAZIL
AND
LOGIC AND COMPUTATION RESEARCH GROUP
EAFIT UNIVERSITY
COLOMBIA
E-mail: juancarlos@cle.unicamp.br

DEPARTMENT OF PHILOSOPHY AND GROUP FOR APPLIED AND
THEORETICAL LOGIC,
CENTRE FOR LOGIC, EPISTEMOLOGY AND THE HISTORY OF SCIENCE—CLE
STATE UNIVERSITY OF CAMPINAS—UNICAMP
BRAZIL
AND
SQIG—INSTITUTE OF TECHNOLOGY, LISBON
PORTUGAL
E-mail: walter.carnielli@cle.unicamp.br

https://doi.org/10.1017/S1755020310000213 Published online by Cambridge University Press