ELSEVIER

Mathematics and Computers in Simulation 45 (1998) 83–99

MATHEMATICS AND COMPUTERS IN SIMULATION

# A polynomial model for multi-valued Logics with a touch of Algebraic Geometry and Computer Algebra[1]

Eugenio Roanes-Lozano[a,*], Luis M. Laita[b], Eugenio Roanes-Macías[a]

[a] Dept. Algebra, Univ. Complutense de Madrid, Madrid, Spain
[b] Dept. Artificial Intelligence, Univ. Politécnica de Madrid, Madrid, Spain

**Abstract**

In this paper, a polynomial model (residue class ring) for a given $p$-valued propositional Logic ($p$ prime), is constructed. This will allow the study of logical deductions using Computer Algebra techniques (Gröbner Bases). Also, an interesting interpretation of $\models$ and Kleene's style $\rightarrow$ and their relation from the point of view of Algebraic Geometry (in terms of algebraic varieties) will be given. Only modest requirements about the good behaviour of the Logic will be assumed. This approach makes it possible to move a step forward and treat Knowledge Based Systems (KBSs) based on multi-valued Logics.


## 1. The polynomial model

### 1.1. The multi-valued propositional logic

Let $p$ be a prime number. Let us suppose that we want to obtain a polynomial model for a certain $p$-valued propositional logic ($\mathscr{C}$, $F_1,\ldots, F_n$), where $\mathscr{C}$ is the set of propositions and $F_1,\ldots, F_n$ are the logical connectives (binary or unary). If the propositional variables are $X_1, X_2,\ldots, X_m$, then $\mathscr{C}$ is the set of well-constructed formulas using $F_1,\ldots, F_n$ and $X_1, X_2,\ldots, X_m$.

The connectives $F_i$ are usually defined by a truth table or in a functional way (for instance: maximum), using valuations. I.e., what is given is a mapping[2]

$$\tilde{F}_i : \{0,1,\ldots,p-1\}^2 \rightarrow \{0,1,\ldots,p-1\}; \quad \text{if } arity(F_i) = 2$$
$$\tilde{F}_i : \{0,1,\ldots,p-1\} \rightarrow \{0,1,\ldots,p-1\}; \quad \text{if } arity(F_i) = 1$$

and the following definitions:

* Corresponding author. E-mail: eroanes@eucmos.sim.ucm.es. Author partially supported by NSA (USA)
[1]Work partially supported by DGES, Spain.
[2]Let us observe that, although 0 is the value for 'False', there is no problem in considering either 1 as the value for 'True' (as usual in Lukasiewicz's and Kleene's three-valued Logics) or $p-1$ (what is more common in general multi-valued modal Logics). Obviously, the polynomial forms that will be obtained will depend on how this assignment is made.


PII S0378-4754(97)00088-8

**1.1.1 Definition.** *A valuation of the propositional variables is a mapping*

$$v: \{X_1, X_2, \ldots, X_m\} \to \mathbb{Z}_p$$

**1.1.2 Definition.** *For each valuation of the propositional variables, v, a valuation of the formulas is obtained*

$$v^*: \mathscr{C} \to \mathbb{Z}_p$$

*This mapping* $v^*$ *is the natural extension of v and can be defined recursively: let* $Q \in \mathscr{C}$

$$v^*(Q) = \begin{cases} v(Q), & \text{if } Q \in \{X_1, X_2, \ldots, X_m\} \\ \tilde{F}_i(v^*(Q')), & \text{if } F_i \text{ is unary and } Q = F_i(Q') \\ \tilde{F}_i(v^*(Q'), v^*(Q'')), & \text{if } F_i \text{ is binary and } Q = F_i(Q', Q'') \end{cases}$$

**1.1.3 Remark.** Therefore, to give the truth table of a connective $F_i$ is to give its value for all the possible valuations of the entries of the corresponding $\tilde{F}_i$.

**1.1.4 Definition.** *As a valuation determines a propositional formula, and once* $\mathscr{C}$ *is constructed, a logical connective* $F_i$ *can be identified with a function*

$$F_i: \mathscr{C} \times \mathscr{C} \to \mathscr{C} \quad (\textit{if } F_i \textit{ is binary})$$
$$F_i: \mathscr{C} \to \mathscr{C} \quad (\textit{if } F_i \textit{ is unary})$$

In this paper, such $F_i$ are called 'logical functions'.

**1.1.5 Remark.** *The definition of logical functions uses an abuse in the notation, because each* $F_i$ *will represent both a logical connective and a logical function. Observe that this usage is the same as when a polynomial ring R is constructed from some polynomial variables using the operators* $+$ *and* $\cdot$ *(that are defined prior to the definition of R). The usual addition of polynomials* $+$: $R \times R \to R$ *is made after the definition of R but is represented with the same symbol* $+$.

### *1.2. The polynomial ring* $\mathscr{A}$

As $p$ is supposed to be prime, $\mathbb{Z}_p$ is a field. Let $x_1, x_2, \ldots, x_m$ be polynomial variables, and let us consider the residue class ring

$$\mathscr{A} = \mathbb{Z}_p[x_1, x_2, \ldots, x_m] / \langle x_1^p - x_1, x_2^p - x_2, \ldots, x_m^p - x_m \rangle$$

The polynomials of $\mathscr{A}$ are of the form

$$\sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p-1} \cdots \sum_{i_m=0}^{p-1} a_{i_1, i_2, \ldots, i_m} x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}; \quad a_{i_1, i_2, \ldots, i_m} \in \mathbb{Z}_p$$

This ring provides a polynomial frame that is a model for $\mathscr{C}$ (as will be seen in Section 1.4). As $F_1, \ldots, F_n$ are functions defined for the elements of $\mathscr{C}$, their polynomial forms can be understood as functions defined for the elements of $\mathscr{A}$. Obtaining these polynomial forms is detailed in [14].

### 1.3. Some remarks about this polynomial ring

**1.3.1 Remark.** Let us observe that this is a finite (and consequently Noetherian) ring, but is not a domain. For example: $x_1 \cdot (x_1^{p-1} - 1) = x_1^p - x_1 = x_1 - x_1 = 0$

**1.3.2 Remark.** In these rings, all ideals are radical. Let us consider the polynomial ring $\mathscr{A}$ mentioned above and an ideal $J$ in that polynomial ring. Let $w \in \mathscr{A}$ and let us suppose that, for a certain $\alpha \in \mathbb{N}$, $w^\alpha \in J$. As $w^p = w$, there exists $\beta \in \mathbb{N}$, $0 \leq \beta < p$, such that $w^\alpha = w^\beta$. Consequently, $w = w^p = w^\beta \cdot w^{p-\beta} = w^\alpha \cdot w^{p-\beta} \in J$ (as: $w^\alpha \in J$).

**1.3.3 Example.** Let us consider the ideal $\langle x^2 \rangle \subset \mathbb{Z}_3[x]/\langle x^3 - x \rangle$. We have: $x = x^3 = x \cdot x^2 \in \langle x^2 \rangle \Rightarrow \langle x^2 \rangle = \langle x \rangle$

**1.3.4 Remark.** Although the definition of these residue class rings is simple, their behaviour is not intuitive. Let us consider the ideal $\langle x^2 - 2 \rangle$ of $\mathbb{Z}_3[x]/\langle x^3 - x \rangle$. As

$$(x^2 - 2)(x^2 + 2) = x^4 - 4 = x^3 \cdot x - (3 + 1) = x^2 - 1 \Rightarrow x^2 - 1 \in \langle x^2 - 2 \rangle$$

and therefore, surprisingly, $\langle x^2 - 2 \rangle = \langle 1 \rangle$. Let us observe that the variety of the ideal $\langle x^2 - 2 \rangle$ is $\emptyset$.

**1.3.5 Remark.** The base fields are not algebraically closed. For instance, $x^2 + x + 1 \in \mathbb{Z}_2[x]$ has no root in $\mathbb{Z}_2$ and $x^2 + 1 \in \mathbb{Z}_3[x]$ has no root in $\mathbb{Z}_3$. But there is an important difference. Polynomials in $\mathbb{Z}_2[x]$ that do not have roots are of degree $\geq 2$, and therefore, are simplified when moving to the residue class ring $\mathbb{Z}_2[x]/\langle x^2 - x \rangle$. Meanwhile, there exist polynomials in $\mathbb{Z}_3[x]$ that do not have roots and are of degree $<3$, and therefore, they are not simplified when moving to the residue class ring $\mathbb{Z}_3[x]/\langle x^3 - x \rangle$.

### 1.4. The homomorphism $\varphi$: $(\mathscr{C}, \vee, \wedge, \neg) \rightarrow (A, f_\vee, f_\wedge, f_\neg)$

**1.4.1 Definition.** *Let* $(\mathscr{C}, \vee, \wedge, \neg)$ *be a multi-valued Logic, given by the propositional variables* $X_1, X_2, \ldots, X_m$, *for* $\underline{0}$ *and* $\underline{1}$, *respectively, denoting 'Contradiction' and 'Tautology'. Let us consider the polynomial residue class ring*

$$\mathscr{A} = \mathbb{Z}_2[x_1, x_2, \ldots, x_m]/\langle x_1^2 - x_1, x_2^2 - x_2, \ldots, x_m^2 - x_m \rangle$$

*We define*

$$\varphi : (\mathscr{C}, \vee, \wedge, \neg) \rightarrow (\mathscr{A}, f_\vee, f_\wedge, f_\neg)$$

*in the following way:*

$$\varphi(X_i) = x_i; \quad i = 1, 2, \ldots, m$$

*and for any* $Q, R \in \mathscr{A}$, *if* $\varphi(Q) = q$ *and* $\varphi(R) = r$

$$\begin{aligned}\varphi(Q \vee R) &= f_\vee(q, r)\\ \varphi(Q \wedge R) &= f_\wedge(q, r)\\ \varphi(\neg Q) &= f_\neg(q)\end{aligned}$$

*In general, for any logical function* $F_i$:

$$\begin{aligned}\varphi(F_i(Q, R)) &= f_i(q, r), \quad \text{if } F_i \text{ is binary}\\ \varphi(F_i(Q)) &= f_i(q), \quad \text{if } F_i \text{ is unary}\end{aligned}$$

**1.4.2 Remark.** From now onwards, we shall consider that the image by $\varphi$ of a certain proposition represented by an upper case letter is the same letter in lower case.

**1.4.3 Theorem.** $\varphi$ *is well defined, i.e.*:
*The truth tables of* $Q$ *and* $R$ *are equal* $\Rightarrow q=r$ (in $\mathscr{A}$).
*The reciprocal also holds, i.e.,* $\varphi$ *is injective.*

**Proof.** Let us denote by $Q_{X_j=i_j}$ the result of substituting in the proposition $Q$ the propositional variable $X_j$ by the value $i_j$.

The truth tables of $Q$ and $R$ are equal $\Leftrightarrow$

$$\begin{aligned}&\Leftrightarrow \forall i_1, i_2, \ldots, i_m \in \mathbb{Z}_p :\ Q_{X_1=i_1, X_2=i_2, \ldots, X_m=i_m} = R_{X_1=i_1, X_2=i_2, \ldots, X_m=i_m} \Leftrightarrow\\ &\Leftrightarrow \forall i_1, i_2, \ldots, i_m \in \mathbb{Z}_p :\ q(i_1, i_2, \ldots, i_m) = r(i_1, i_2, \ldots, i_m) \Leftrightarrow\\ &\Leftrightarrow \forall i_1, i_2, \ldots, i_m \in \mathbb{Z}_p :\ (q - r)(i_1, i_2, \ldots, i_m) = 0 \Leftrightarrow\\ &\Leftrightarrow q - r = 0 \ (\text{in } \mathscr{A}) \Leftrightarrow q = r \ (\text{in } \mathscr{A})\end{aligned}$$

**1.4.4 Consequence.** $\varphi$ *is an injective homomorphism.*

**1.4.5 Proposition.** *If any truth table corresponds to a formula of the given Logic,* $\varphi$ *is surjective and consequently* $\varphi$ *is an isomorphism.*

**Proof.** Let $q \in \mathscr{A}$. The values $q(i_1, i_2, \ldots, i_m)$ are known $\forall i_1, i_2, \ldots, i_m \in \mathbb{Z}_p$. By hypothesis, a formula $Q$ s.t.

$$\forall i_1, i_2, \ldots, i_m \in \mathbb{Z}_p,\ Q(i_1, i_2, \ldots, i_m) = q(i_1, i_2, \ldots, i_m)$$

must exist. But then, according to the previous Theorem, $\varphi(Q)=q$, q.e.d.

**1.4.6 Remark.** Let us observe that $\varphi$ is not usually surjective. For instance, in Kleene's three-valued Logic, there is no assumed 'undetermined' constant (that would correspond to the constant 2 of $\mathscr{A}$). It seems interesting to complete Kleene's Logic with this constant (the same way as the Tautology and the Contradiction are assumed as constants).

**1.4.7 Remark.** $\varphi(\underline{1}) = 1,\ \varphi(\underline{0}) = 0.$

**1.4.8 Remark.** To be precise, we will not consider $\mathscr{C}$ and $\mathscr{A}$ but $\mathscr{C}/\mathscr{R}$ (where $\mathscr{R}$ is the relation 'to have the same truth table') and $\mathscr{A}/=$.

## 2. To be tautological consequence and the ideal membership problem

### 2.1. Tautologies and to be tautological consequence in multi-valued Logics

Let 0 be the value corresponding to *False*, and let $\mu \in \{1, \ldots, p-1\}$ be the value corresponding to *True* (usually, $\mu$=1 or $\mu$=$p-1$).

**2.1.1 Definition.** *Let $W \in \mathscr{C}$. W is a Tautology (to be denoted $\models W$) iff for any valuation of propositional variables, v, the correspondent valuation of formulas, $v^*$, satisfies*

$$v^*(W) = \mu.$$

**2.1.2 Definition.** Let $Q, R, \ldots, S, W \in \mathscr{C}$. *W is a tautological consequence of $\{Q, R, \ldots, S\}$ (to be denoted $\{Q, R, \ldots, S\} \models W$) iff for any valuation of propositional variables, v, the correspondent valuation of formulas, $v^*$, satisfies*

$$v^*(Q) = v^*(R) = \ldots = v^*(S) = \mu \Rightarrow v^*(W) = \mu$$

(*i.e., iff for any valuation of propositional variables s.t. Q is True and R is True and* ... *and S is True, then W is True*).

### 2.2. To be a tautological consequence and the ideal membership problem

Let us denote by $\varphi$ a mapping from $\mathscr{C}$ in $\mathscr{A}$ that maps a proposition into a polynomial form of it.

**2.2.1 Axioms.** *It will be supposed that the given Logic satisfies*:

- *For any $Q \in \mathscr{C}$, if Q is True then $\neg Q$ is False and if Q is False then $\neg Q$ is True.*
- *For any $Q, R \in \mathscr{C}$ and for any valuation v,*

$$v^*(Q \wedge R) = \mu \Leftrightarrow v^*(Q) = \mu \wedge_b v^*(R) = \mu$$

(*let us observe that the last $\wedge_b$ is the classical bivalued one and that $\mu$ is the value assigned to True*).

**2.2.2 Proposition.** *For any $Q, R, \ldots, S, W \in \mathscr{C}$*

$$\{Q, R, \ldots, S\} \models W \Leftrightarrow \{Q \wedge R \wedge \ldots \wedge S\} \models W$$

**Proof.** As a consequence of one of the axioms in 2.2.1, $Q, R, \ldots, S$ are all True iff $Q \wedge_b R \wedge_b \ldots \wedge_b S$ is True. The result follows.

**2.2.3 Theorem.** *Let $Q$, $R$,. . ., $S$, $W\in\mathscr{C}$. Then,*

$$\{Q, R, \ldots, S\} \models W \Leftarrow \varphi(\neg W) \in \langle \varphi(\neg Q), \varphi(\neg R), ..., \varphi(\neg S)\rangle$$

**Proof.** $\Leftarrow$) Let us suppose that $\varphi(\neg W)\in\langle\varphi(\neg Q), \varphi(\neg R),\ldots, \varphi(\neg S)\rangle$ and that $v$ is a valuation verifying

$$v^*(Q) = v^*(R) = \ldots = v^*(S) = \mu$$

Then, by 2.2.1

$$v^*(\neg Q) = v^*(\neg R) = ... = v^*(\neg S) = 0$$

In polynomial form, if $\Omega$ is the point corresponding to the valuation $v$ (i.e., $\Omega\in\{0, 1,\ldots, p-1\}^m$; $m$=number of propositional variables)

$$\varphi(\neg Q)(\Omega) = \varphi(\neg R)(\Omega) = ... = \varphi(\neg S)(\Omega) = 0 \qquad (**)$$

As the hypothesis is

$$\varphi(\neg W) \in \langle \varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S)\rangle$$

$\varphi(\neg W)$ is a linear algebraic combination of $\varphi(\neg Q)$, $\varphi(\neg R)$,. . ., $\varphi(\neg S)$, i.e.:

$$\exists pol_q, pol_r, \ldots, pol_s \in \mathscr{A}\ s.t.:$$

$$\varphi(\neg W) = pol_q \cdot \varphi(\neg Q) + pol_r \cdot \varphi(\neg R) + \cdots + pol_s \cdot \varphi(\neg S)$$

and therefore:

$$\begin{aligned}\varphi(\neg W)(\Omega) &= pol_q(\Omega) \cdot \varphi(\neg Q)(\Omega) + pol_r(\Omega) \cdot \varphi(\neg R)(\Omega) + \cdots + pol_s(\Omega) \cdot \varphi(\neg S)(\Omega)\\ &= pol_q(\Omega) \cdot 0 + pol_r(\Omega) \cdot 0 + \cdots + pol_s(\Omega) \cdot 0 = 0\end{aligned}$$

Returning to propositions, this means

$$v^*(\neg W) = 0 \Leftrightarrow v^*(W) = \mu, \text{ q.e.d.}$$

**2.2.4 Remark.** Let us observe that the previous proof can also be obtained by dealing with varieties. If the variety of an ideal $J$ of $\mathscr{A}$ is denoted $V(J)$, condition (**) is equivalent to

$$\Omega \in V(\langle\varphi(\neg Q)\rangle) \cap V(\langle\varphi(\neg R)\rangle) \cap \ldots \cap V(\langle\varphi(\neg S)\rangle) = V(\langle\varphi(\neg Q), \varphi(\neg R), ..., \varphi(\neg S)\rangle)$$

and from the hypothesis it follows that this variety is contained in $V(\varphi(\neg W))$. Therefore,

$$v^*(\neg W) = 0 \ \Leftrightarrow\ v^*(W) = \mu$$

**2.2.5 Remark.** The reciprocal of Theorem 2.2.3 is not easy to prove.

**Idea.** Let us try a proof of $\Rightarrow$). Let us suppose that $\{Q, R,\ldots, S\}\models W$. Then, for any valuation $v$

$$v^*(Q) = v^*(R) = \ldots = v^*(S) = \mu \Rightarrow v^*(W) = \mu.$$

Or, what is equivalent, for any valuation $v$

$$v^*(\neg Q) = v^*(\neg R) = \ldots = v^*(\neg S) = 0 \Rightarrow v^*(\neg W) = 0$$

In polynomial form, for any point $\Omega \in \{0, 1, \ldots, p-1\}^m$ ($m$=number of propositional variables) we have

$$\varphi(\neg Q)(\Omega) = \varphi(\neg R)(\Omega) = \ldots = \varphi(\neg S)(\Omega) = 0 \Rightarrow \varphi(\neg W)(\Omega) = 0$$

Denoting by $V(J)$ the variety of the ideal $J$, the previous implication can be written

$$\forall \Omega \in \{0, 1, \ldots, p-1\}^m : \Omega \in V(\langle \varphi(\neg Q) \rangle) \wedge_b \Omega \in V(\langle \varphi(\neg R) \rangle) \wedge_b \ldots \wedge_b \Omega \in V(\langle \varphi(\neg S) \rangle)$$
$$\Rightarrow \Omega \in V(\langle \varphi(\neg W) \rangle)$$

i.e.

$$V(\langle \varphi(\neg Q) \rangle) \cap V(\langle \varphi(\neg R) \rangle) \cap \ldots \cap V(\langle \varphi(\neg S) \rangle) \subseteq V(\langle \varphi(\neg W) \rangle)$$

and consequently

$$V(\langle \varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S) \rangle) \subseteq V(\langle \varphi(\neg W) \rangle)$$

Denoting by $I(\nu)$ the ideal of the variety $\nu$, we have

$$I(V(\langle \varphi(\neg W)) \rangle) \subseteq I(V(\langle \varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S) \rangle))$$

and therefore,

$$\varphi(\neg W) \in I(V(\langle \varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S) \rangle)).$$

It is a pity that Hilbert's Nullstellensatz is not directly applicable here (as the base field is not algebraically closed). In such a case, we would have

$$\varphi(\neg W) \in Radical\,(\langle \varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S) \rangle))$$

and, as mentioned in Section 1.3, all ideals are radical and therefore,

$$\varphi(\neg W) \in \langle \varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S) \rangle$$

We shall prove it another way in Section 2.4.

**2.2.6 Example.** The previous failed attempt of proof suggests the idea to try to find an example where the implication $\Rightarrow$) does not hold. Let us consider Lukasiewicz's Logic (see [15] for details). Let us look for a formula $Q$, not equivalent to Contradiction, that can never be True (i.e., such that the variety of its image by $\varphi$ is empty). For instance,

$$X_1 \wedge \neg L(X_1)$$

(where $L$ means 'necessary') can only have the values 0 (False) and 2 (Indeterminate). Its polynomial image in $\mathbb{Z}_3[x_1, x_2]/\langle x_1^3 - x_1, x_2^3 - x_2 \rangle$ is $\varphi(X_1 \wedge \neg L(X_1)) = x_1^2 + 2x_1$ (see [11] for details). Let us now consider the proposition

$$X_2 \vee (X_1 \wedge \neg L(X_1)).$$

This proposition is True iff $X_2$ is True, and therefore:

$$\begin{array}{r} \{X_2 \vee (X_1 \wedge \neg L(X_1))\} \models X_2 \\ X_2 \models (X_2 \vee X_1 \wedge \neg L(X_1)) \end{array} \qquad (*)$$

If the other implication of the previous Theorem was True, from (*) we would have:

$$\varphi(\neg(X_2)) \in \langle \varphi(\neg(X_2 \vee X_1 \wedge \neg L(X_1)))\rangle$$

i.e.

$$1 - x_2 \in \langle x_1^2 x_2^2 - x_1 x_2^2 - x_1^2 + x_1 - x_2 + 1\rangle$$

what surprisingly, despite its appearance, holds in $\mathbb{Z}_3[x_1, x_2]/\langle x_1^3 - x_1, x_2^3 - x_2\rangle$. The Normal Form of $1-x_2$ modulo $\langle x_1^2 x_2^2 - x_1 x_2^2 - x_1^2 + x_1 - x_2 + 1\rangle$ is 0 in that residue class ring.

### *2.3. Kleene's style multi-valued Logics and the ideal membership problem*

**2.3.1 Axioms.** *It will be supposed that the given Logic satisfies*:

- *For any $Q$, $R \in \mathscr{C}$ and for any valuation $v$,*

  $$v^*(Q \wedge R) = 0 \Leftrightarrow v^*(Q) = 0 \vee_b v^*(R) = 0$$

  (*observe that $\vee_b$ is the classical bivalued 'or'*).

- *For any $Q \in \mathscr{C}$,*

  $$\varphi(\neg(Q)) = \mu - \varphi(Q)$$

  (*let us remember that $\mu$ is the value assigned to True*; *usually $\mu$=1 or $\mu$=$p-1$*). Consequently, as $\varphi$ is injective, $\neg(\neg Q) \leftrightarrow Q$.

- *The De Morgan's laws.*

**2.3.2 Lemma.** (*In the polynomial ring $\mathscr{A}$*) *If the variety of an ideal $J$ is the whole affine space* $\{0, 1, \ldots, p-1\}^m$, *then* $J = \langle 0\rangle$.

**Proof.** $J \subseteq IV(J) = I(\{0, 1, \ldots, p-1\}^m) = \langle 0\rangle$

**2.3.3 Lemma.** *For any* $Q\in\mathscr{C}$,

$$\langle\varphi(Q)\rangle + \langle\varphi(\neg Q)\rangle = \langle 1\rangle$$

**Proof.** $\langle\varphi(Q)\rangle + \langle\varphi(\neg Q)\rangle = \langle\varphi(Q)\rangle + \langle\mu - \varphi(Q)\rangle = \langle\mu\rangle$. But $\mu$ is in the base field, so it is invertible, and consequently $\langle\mu\rangle=\langle 1\rangle$.

**2.3.4 Lemma.** *For any* $Q$, $W\in\mathscr{C}$:

$$\langle\varphi(Q)\rangle \cap \langle\varphi(\neg W)\rangle = \langle 0\rangle \Rightarrow \varphi(\neg W) \in \langle\varphi(\neg Q)\rangle$$

**Proof.** Obviously

$$\langle\varphi(\neg W)\rangle = \langle\varphi(\neg W)\rangle \cap \langle 1\rangle$$

and, according to Lemma 2.3.3, it can be written

$$\langle\varphi(\neg W)\rangle = \langle\varphi(\neg W)\rangle \cap [\langle\varphi(Q)\rangle + \langle\varphi(\neg Q)\rangle] = [\langle\varphi(\neg W)\rangle \cap \langle\varphi(Q)\rangle] + [\langle\varphi(\neg W)\rangle \cap \langle\varphi(\neg Q)\rangle]$$

and therefore, by hypothesis

$$\begin{aligned}\langle\varphi(\neg W)\rangle &= \langle 0\rangle + [\langle\varphi(\neg W)\rangle \cap \langle\varphi(\neg Q)\rangle] = \langle\varphi(\neg W)\rangle \cap \langle\varphi(\neg Q)\rangle \Leftrightarrow \langle\varphi(\neg W)\rangle \subseteq \langle\varphi(\neg Q)\rangle \\ &\Leftrightarrow \varphi(\neg W) \in \langle\varphi(\neg Q)\rangle\end{aligned}$$

**2.3.5 Definition.** *Let us denote by* $\rightarrow$ *the implication in Kleene's style*, *i.e.*:

$$\textit{for any } Q, W \in \mathscr{C} : \models Q \rightarrow W \Leftrightarrow (\neg Q \vee W) \textit{ is a Tautology}.$$

**2.3.6 Theorem.** *Let* $Q$, $W\in\mathscr{C}$. *Then*,

$$\models Q \rightarrow W \Rightarrow \varphi(\neg W) \in \langle\varphi(\neg Q)\rangle$$

**Proof.** $\models Q\rightarrow W$ means that, for any valuation $v$, $v^*$ verifies:

$$v^*(Q \rightarrow W) = \mu$$

or, what is equivalent by the previous definition,

$$v^*(\neg Q \vee W) = \mu$$

i.e., by one of the axioms in 2.3.1

$$v^*(\neg(\neg Q \vee W)) = 0.$$

As the De Morgan's laws are supposed to hold, it is equivalent to

$$v^*(Q \wedge \neg W) = 0$$

and by one of the axioms in 2.3.1, it is equivalent to

$$v^*(Q) = 0 \vee_b v^*(\neg W) = 0$$

Let us remember that the previous expression holds for any valuation $v^*$, and therefore, it can be written in polynomial form: $\forall\Omega \in \{0, 1,\ldots, p-1\}^m$

$$\varphi(Q)(\Omega) = 0 \vee_b \varphi(\neg W)(\Omega) = 0$$

($\Omega$ is the point corresponding to the valuation $v$).

Thus, denoting by $V(J)$ the variety of the ideal $J$, $\forall\Omega \in \{0, 1,\ldots, p-1\}^m$

$$\Omega \in V(\langle\varphi(Q)\rangle) \cup V(\langle\varphi(\neg W)\rangle)$$

i.e., $\forall\Omega \in \{0, 1,\ldots, p-1\}^m$

$$\Omega \in V(\langle\varphi(Q)\rangle \cap \langle\varphi(\neg W)\rangle)$$

that is, this variety is the whole affine space

$$V(\langle\varphi(Q)\rangle \cap \langle\varphi(\neg W)\rangle) = \{0, 1, \ldots, p-1\}^m$$

From the previous expression, by Lemma 2.3.2

$$\langle\varphi(Q)\rangle \cap \langle\varphi(\neg W)\rangle = \langle 0\rangle$$

and, by Lemma 2.3.4

$$\varphi(\neg W) \in \langle\varphi(\neg Q)\rangle, \text{ q.e.d.}$$

**2.3.7 Remark.** The reciprocal of the previous theorem does not hold.

**2.3.8 Example.** Let us consider Kleene's three-valued Logic [15] and let $Q$ be a proposition. Then: $\not\models Q\to Q$ (if the truth value for $Q$ is 'Undecided', the truth value for $Q\to Q$, i.e., for $\neg Q\vee Q$, is also 'Undecided', instead of 'True'). But $\varphi(\neg Q) \in \langle\varphi(\neg Q)\rangle$.

**2.3.9 Remark.** Let us remember that $\models Q\to W$ is a strong form of $Q\models W$, i.e.,

$$(\models Q \to W) \Rightarrow (Q \models W)$$

but

$$(Q \models W) \not\Rightarrow (\models Q \to W)$$

**Proof.** If $\models Q\to W$, then $(\neg Q\models W)$ is a Tautology, i.e., for any valuation, $v$,

$$v^*(\neg Q \vee W) = 1 \Leftrightarrow v^*(\neg(\neg Q \vee W)) = 0$$

or what is equivalent (by the De Morgan laws, included in Axioms 2.3.1), for any valuation, $v$,

$$v^*(Q \wedge \neg W) = 0.$$

Therefore, by some of the axioms in 2.3.1 and 2.2.1,

$$v^*(Q) = 0 \vee_b v^*(\neg W) = 0 \Leftrightarrow v^*(Q) = 0 \vee_b v^*(W) = \mu$$

and consequently, in any case, $Q \models W$ holds.

**2.3.10 Example.** The same as in 2.3.8: $(Q \models Q)$ but $((\not\models Q \rightarrow Q)$

**2.3.11 Remark.** Let us observe that 2.3.6 is almost the reciprocal of 2.2.3.

### *2.4. Kleene's style → and to be tautological consequence*

**2.4.1 Axiom**. *It will be supposed that there are two unary functions in the given Logic*: $L$ (*'necessary'*) *and* $\Diamond$ (*'possible'*), *verifying*

| $Q$ | $LQ$ | $\Diamond Q$ |
|---|---|---|
| 0 | 0 | 0 |
| $\mu$ | $\mu$ | $\mu$ |
| *other* | 0 | $\mu$ |

(*'other' means here a value different from* 0 *and* $\mu$). *Observe that, according to Fermat's Minor Theorem*

$$\forall k \in \mathbb{Z}_p,\ k \neq 0 :\ k^{p-1} = 1$$

*Therefore, if* $\mu=1$ *then* $\forall Q \in \mathscr{C}$ *it can be considered*

$$\varphi(\Diamond Q) = \varphi(Q)^{p-1}$$

*For instance, in Lukasiewicz's Logic*: $\varphi(\Diamond Q)=q^2$. *If* $\mu=p-1$, *then*

$$\varphi(\Diamond Q) = (p-1) \cdot \varphi(Q)^{p-1}$$

*can be considered instead. For instance, in Lukasiewicz's Logic*: $\varphi(\Diamond Q)=2 \cdot q^2$

**2.4.2 Theorem.** *For any* $Q$, $W \in \mathscr{C}$: $Q \models W \Leftrightarrow \models LQ \rightarrow W$.

**Proof.** $\Rightarrow$) Let us suppose that $Q \models W$. Then, whenever $Q$ is True, $W$ is True. Let us consider the following truth table

| $Q$ | $LQ$ | $\neg LQ$ |
|---|---|---|
| 0 | 0 | $\mu$ |
| $\mu$ | $\mu$ | 0 |
| *other* | 0 | $\mu$ |

As $Q \models W$ is supposed by hypothesis, whenever $Q$ is True, $W$ is True, so we can partially fill the column corresponding to $W$ (? means it cannot be assured which value goes there), and the column corresponding to $\neg LQ \vee W$

| $Q$ | $LQ$ | $\neg LQ$ | $W$ | $\neg LQ \vee W$ |
|---|---|---|---|---|
| 0 | 0 | $\mu$ | ? | $\mu$ |
| $\mu$ | $\mu$ | 0 | $\mu$ | $\mu$ |
| *other* | 0 | $\mu$ | ? | $\mu$ |

Therefore, $\neg LQ \vee W$ is a Tautology, q.e.d.

$\Leftarrow$) By definition of $\rightarrow$:

$$\models LQ \rightarrow W \Leftrightarrow \neg LQ \vee W \text{ is a Tautology.}$$

Therefore, if $Q$ is True $\Rightarrow$ $LQ$ is True $\Rightarrow$ $\neg LQ$ is False. But $\neg LQ \vee W$ is a Tautology $\Rightarrow$ $W$ is True (as a consequence of the axioms in 2.3.1 and the De Morgan's laws (2.3.1)).

**2.4.3 Lemma.** *For any* $Q \in \mathscr{C}$, $\varphi(\neg LQ)=\varphi(\Diamond\neg Q)$.

**Proof.**

| $Q$ | $LQ$ | $\neg LQ$ | $\neg Q$ | $\Diamond\neg LQ$ |
|---|---|---|---|---|
| 0 | 0 | $\mu$ | $\mu$ | $\mu$ |
| $\mu$ | $\mu$ | 0 | 0 | 0 |
| *other* | 0 | $\mu$ | *other* | $\mu$ |

The result follows now from 1.4.3.

**2.4.4 Proposition.** *For any* $Q, R, \ldots, S, W \in \mathscr{C}$

$$\langle \varphi(\neg L(Q \wedge R \wedge \ldots \wedge S)) \rangle \subseteq \langle \varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S)) >$$

**Proof.** $\langle \varphi(\neg L(Q \wedge R \wedge \ldots \wedge S)) \rangle$ is equal, by the previous Lemma, to

$$\langle \varphi(\Diamond\neg(Q \wedge R \wedge \ldots \wedge S)) \rangle$$

that according to the polynomial forms of $\varphi(\Diamond(Q))$ given in 2.4.1, is equal to the ideal

$$\langle \varphi(\neg(Q \wedge R \wedge \ldots \wedge S))^{p-1} \rangle$$

but every ideal is radical (1.3.2), so this is the ideal

$$\langle \varphi(\neg(Q \wedge R \wedge \ldots \wedge S)) \rangle$$

and by the De Morgan's laws (that holds by hypothesis) is equal to

$$\langle \varphi(\neg Q \vee \neg R \vee \ldots \vee \neg S)) \rangle$$

And, as $\varphi(\neg Q \vee \neg R \vee \ldots \vee \neg S)$ is an algebraic combination of $\varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S))$ that ideal is contained in $\langle \varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S)) \rangle$, q.e.d.

*2.5. To be a tautological consequence and the ideal membership problem (more results)*

Let us observe what we have proven (up to now): If the Logic verifies Axioms 2.2.1, 2.3.1, 2.4.1, then for all $Q$, $R$,. . ., $S$, $W \in \mathscr{C}$

$$\begin{array}{lcl} \{Q, R, ..., S\} \models W & \overset{2.2.3}{\Leftarrow} & \varphi(\neg W) \in \langle \varphi(\neg Q), \varphi(\neg R), ..., \varphi(\neg S) \rangle \\ (2.2.2) & & \\ \{Q \wedge R \wedge ... \wedge S\} \models W & & \Uparrow (2.4.4) \\ (2.4.2) & & \\ \models L(Q \wedge R \wedge ... \wedge S) \rightarrow W & \underset{2.3.6}{\Rightarrow} & \varphi(\neg W) \in \langle \varphi(\neg L(Q \wedge R \wedge ... \wedge S) \rangle \end{array}$$

**2.5.1 Theorem.** *If the Logic verifies Axioms* 2.2.1, 2.3.1, 2.4.1 *then: For all* $Q$,$R$,. . .,$S$,$W \in \mathscr{C}$

$$\{Q, R, \ldots, S\} \models W \Leftrightarrow \varphi(\neg W) \in \langle \varphi(\neg Q), \varphi(\neg R), \ldots, \varphi(\neg S) \rangle$$

(*and the right hand side of this implication can effectively be checked with Gröbner Bases* [2,3]).

**Proof.** It follows immediately from the diagram above.

**2.5.2 Remark.** Now it is possible to extend the study to KBSs based on multi-valued Logics. As done in [8], the residue class ring $\mathscr{A}/J$, where $J$ is the ideal generated by the negation of the facts, rules and constraints, is a polynomial model for the KBS.

## 3. Implementation

CoCoA (COmputational COmmutative Algebra) is a tiny but very powerful specific purpose Computer Algebra System [4]. It is specialized in calculating Gröbner Bases and reductions modulo an ideal in polynomial rings over a finite characteristic field[3].

**3.0.1 Example.** A CoCoA 3 implementation of a seven-valued Logic will be detailed below. The truth values considered are 0 (representing 'False'), 1, 2, 3, 4, 5 and 6 (representing 'True'). Greater values represent greater degrees of certainty. The logical functions that have been implemented are:

- negation (unary): `NEG` (that 'reverses' the certainty)
- disjunction (binary): `O` (OR is a reserved word in CoCoA)
- conjunction (binary): `Y` (AND is a reserved word in CoCoA)
- possibility (unary): `POS` (the truth value is always 6 except for 0, that is 0)
- necessity (unary): `NEC` (the truth value is always 0 except for 6, that is 6).

We shall consider the propositional variables to be `x[1], x[2], ..., x[8]` plus an extra variable z. In CoCoA syntax

[3] Its developers can be reached at cocoa@dima.unige.it. There are versions available for 32-bit PC-compatibles and Macs.

```
A ::= Z/(7)[x[1..8],z];
USE A;
I := Ideal(x[1]^7 - x[1], x[2]^7 - x[2], x[3]^7 - x[3], x[4]^7 - x[4], x[5]^7
  -x[5], x[6]^7 - x[6], x[7]^7 - x[7], x[8]^7 - x[8], z^7 - z);
```

(really what we have called $\mathscr{A}$ in the theory shown in the previous sections is `A/I` in this implementation, because unfortunately CoCoA 3 still cannot fix a residue class ring as the ring where the calculations have to take place; therefore, all the time reductions modulo `I` will have to be explicitly mention and `I` will have to be added to all the ideals considered).

Let `M`, `N` be any propositions. Polynomial forms of the logical functions are in this case:

```
NEG(M) := NF(6*M + 6, I);
POS(M) := NF(6*M^6, I);
NEC(M) := NF(M^6 + 6*M^5 + M^4 + 6*M^3 + M^2 + 6*M, I);
O(M,N) := NF(3*M^6*N^6 + M^5*N^3 + 4*M^4*N^4 + M^3*N^5 + 3*M^2*N^6
  +3*M^6*N + 3*M*N^6 + 6*M^5*N + 3*M^4*N^2 + 3*M^3*N^3 + 3*M^2*N^4
  +6*M*N^5 + 3*M^3*N + M^2*N^2 + 3*M*N^3 + 2*M*N + M + N, I);
Y(M,N) := NF(4*M^6*N^2 + 6*M^5*N^3 + 3*M^4*N^4 + 6*M^3*N^5 + 4*M^2*N^6
  +4*M^6*N + 4*M*N^6 + M^5*N + 4*M^4*N^2 + 4*M^3*N^3 + 4*M^2*N^4 + M*N^5
  +4*M^3*N + 6*M^2*N^2 + 4*M*N^3 + 5*M*N, I);
IMP(M,N) := NF(3*M^6*N^2 + 6*M^5*N^3 + 4*M^4*N^4 + 6*M^3*N^5
  +3*M^5*N^6 + 3*M^6*N + 4*M^5*N^2 + 2*M^4*N^3 + 2*M^3*N^4 + 4*M^2*N^5
  +3*M*N^6 + 5*M^5*N + 6*M^4*N^2 + M^2*N^3 + 6*M^2*N^4 + 5*M*N^5 + M^4*N
  +2M^3*N^2 + 2*M^2*N^3 + M*N^4 + 4*M^3*N + M^2*N^2 + 4*M*N^3 + 4*M^2*N
  +4*M*N^2 + 5*M*N + 6*M + 6, I)
```

(for details about how these polynomials can be obtained, see [14]).

For example, let us check that $X[1]\vee X[2]$ is a tautological consequence of $\{X[1], X[2]\}$. According to 2.5.1, it is equivalent to $\varphi(\neg(X[1]\vee X[2]))\in\langle\varphi(\neg X[1]),\ \varphi(\neg X[2])\rangle$, what is equivalent to $\langle\varphi(\neg(X[1]\vee X[2]))\rangle=\langle\varphi(\neg(X[1]\vee X[2])),\ \varphi(\neg(X[1])),\ \varphi(\neg(X[2]))\rangle$.

```
Q1 := x[1];
Q2 := x[2];
```

(the letter R is not used, as it is a reserved variable in CoCoA: it represents the ring where calculations take place)

```
W:=O(x[1],x[2]);
J:=Ideal(NEG(Q1),NEG(Q2));
GBasis(I+J);
[...]
GBasis(I+J+Ideal(NEG(W)));
[...]
```

Both ideals are equal (the resulting bases are omitted for the sake of brevity), and therefore, $X[1]\vee X[2]$ is a tautological consequence of $\{X[1], X[2]\}$.

A smarter way to check the ideal membership problem is well known. A new variable ($z$) is needed and it has to be checked whether or not adding $1-z\cdot\varphi(\neg(X[1]\vee X[2]))$ to the ideal makes it degenerate into the whole ring. In CoCoA

```
GBasis(I + J + Ideal(1-z*NEG(W)));
[1]
```

and therefore, $X[1]\vee X[2]$ is a tautological consequence of $\{X[1], X[2]\}$.

Let us check now a slightly more difficult example. In the same Logic, let

```
S1:=O(POS(x[1]),NEC(Y(x[7],x[8])));
S2:=NEG(x[3]);
S3:=NEC(x[5]);
S4:=O(NEC(NEG(x[1])),POS(x[8]));
W1:=O(POS(x[8]),NEC(Y(x[7],x[8])));
J:=Ideal(NEG(S1),NEG(S2),NEG(S3),NEG(S4));
```

then

```
GBasis(I + J + Ideal(1 - z*NEG(W1)));
```

is the whole ring, and therefore, `W1` follows from `{S1, S2, S3, S4}`. But if

```
W2 := Y(POS(x[8]), NEC(Y(x[7], x[8])));
```

is considered instead,

```
GBasis(I + J + Ideal(1 - z*NEG(W2)));
```

is not the whole ring, and therefore, `W2` does not follow from `{S1, S2, S3, S4}`.

The calculations above have been performed in a few seconds in CoCoA, running on a 32 MB RAM Pentium PC. Unfortunately, with values for $p$ greater than 5, polynomial calculations can soon be so complicated that computations take long times and sometimes collapse the computer. On the other hand, the same occurs if the problem is treated for example constructing the corresponding truth tables.

## 4. Related works. Conclusions

In [6], it was shown how logical deduction in classical bivalued Logic could be translated into terms of polynomial ideal membership, that could be decided using Gröbner Bases. In [5,1], the ideas of [9] were extended to multi-valued Logics.

In [7], we presented a polynomial model for propositional Boolean algebras (a residue class ring) where decision could be taken without using GB. Later, it was adapted to check the forward reasoning consistency of Knowledge Based Systems (KBSs) based on classical bivalued Logic, by moving to the residue class ring over another ideal ([8–10]). It was also adapted to check tautological consequences in KBSs based on classical bivalued Logics [13].

Both lines were merged in [11,12], in order to check the forward reasoning consistency of KBSs based on Lukasiewicz's three-valued logic (moving again to a certain residue class ring).

In this article, an algebraic structure (polynomial residue class ring) for $p$-valued propositional Logics ($p$ prime) is given. As shown in [5,1], logical deduction can be translated into an ideal membership problem, that can be decided using Gröbner Bases.

Although the goals are similar, this approach differs strongly with that of [5,1]. Providing an algebraic structure (residue class ring) allows us to give completely different explanations and proofs (algebraic instead of logic). These proofs only need the use of elementary techniques from Commutative Algebra. We think that this geometric interpretation is itself very interesting. Also, the following curious interpretation of $\models$ and Kleene's style $\rightarrow$ and their relation in terms of algebraic varieties are proved in this paper:

- $\models$ holds if the point corresponding to the valuation for which the antecedent is *True* belongs to a certain algebraic variety (2.2.4).
- $\rightarrow$ is equivalent to the equality of a certain algebraic variety to the whole affine space (proof of 2.3.6).

Another advantage of this approach is that this way it is possible to move a step forward and treat KBSs based on multi-valued Logics.

## References


[1] J.A. Alonso, E. Briales, Lógicas Polivalentes y Bases de Gröbner, in: C. Martin (Ed.), Actas del V Congreso de Lenguajes Naturales y Lenguajes Formales, 1989, pp. 307–315.

[2] B. Buchberger, Applications of Gröbner Bases in non-linear Computational Geometry, in: J.R. Rice (Ed.), Mathematical Aspects of Scientific Software, IMA Volumes in Math. and its Applications, vol. 14, Springer, Berlin, 1988.

[3] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, Springer, Berlin, 1991.

[4] A. Capani, G. Niesi, CoCoA User's Manual, Dept. Mathematics, Univ. of Genova, 1996.

[5] J. Chazarain, A. Riscos, J.A. Alonso, E. Briales, Multi-valued Logic and Gröbner Bases with Applications to Modal Logic, J. Symbolic Computation 11 (1991) 181–194.

[6] D. Kapur, P. Narendran, An Equational Approach to Theorem Proving in First-order Predicate Calculus, Proceedings of the 9th International Joint Conference on Artificial Intelligence (IJCAI-85), vol. 2, pp. 1146–1153.

[7] L.M. Laita, L. de Ledesma, E. Roanes L., E. Roanes M., An Interpretation of the Propositional Boolean Algebra as a k-algebra, Effective Calculus, in: J. Campbell, J. Calmet (Eds.), Proceedings of the Second International Workshop/ Conference on Artificial Intelligence and Symbolic Mathematical Computing (AISMC-2), Lecture Notes in Computer Science, vol. 958, Springer, Berlin, 1995, pp. 255–263.

[8] L.E. Roanes, L.M. Laita, M.E. Roanes, Maple V in A.I.: The Boolean Algebra Associated to a KBS, CAN Nieuwsbrief 14 (1995) pp. 65–70.

[9] E. Roanes L., L.M. Laita, Verification of Knowledge Based Systems with Commutative Algebra and Computer Algebra Techniques, Proceedings of the 1st International Conference on Applications of Computer Algebra (IMACS), New Mexico University, USA, 1995 (electronic book).

[10] L.M. Laita, E. Roanes L., Verification of Knowledge Based Systems: An Algebraic Interpretation, Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI-95) (Workshop on Verification and Validation of Knowledge Based Systems), McGill University, Montreal, Canadá, 1995, pp. 91–95.

[11] L.M. Laita, E. Roanes L., J.A. Alonso, E, Briales, Algebraic Verification of KBSs, Proceedings of the 13th National Conference on Artificial Intelligence (AAAI-96) (Workshop on Verification and Validation of Knowledge Based Systems and Subsystems), Portland, USA, 1996, pp. 122–129.

[12] L.M. Laita, E. Roanes L., A Computer Algebraic Method for Verification and Deduction in KBSs: Theory and Implementation, Proceedings of the 12th European Conference on Artificial Intelligence (ECAI-96), Budapest University, Hungary, 1996, pp. 5–10.

[13] E. Roanes L., L.M. Laita, E. Roanes M., An Inference Engine for Propositional Two-valued Logic Based on the Radical Membership Problem, in: J. Campbell, J. Calmet, J. Pfalzgraf (Eds.), Proceedings of the Third International Workshop/ Conference on Artificial Intelligence and Symbolic Mathematical Computing (AISMC-3), Lecture Notes in Computer Science, vol. 1138, Springer, Berlin, 1996, pp. 71–86.

[14] E. Roanes L., L.M. Laita, E. Roanes M., Effective Calculus of Polynomial Forms of the Logical Functions of a given Multi-valued Logic with a CAS, Preprint.

[15] R. Turner, Logics for Artificial Intelligence, Ellis Horwood, Chichester, 1984.