LÓGICAS POLIVALENTES Y BASES DE GRÖBNER

José Antonio Alonso Jiménez
Emilio Briales Morales

Departamento de Algebra
Facultad de Matemáticas
Universidad de Sevilla

The aim of this paper is to describe the application of the Gröbner bases to automated theorem proving in Many–Valued Logic

INTRODUCCIÓN

El objetivo de la comunicación es presentar una aplicación de las bases de Gröbner a la demostración automática en lógicas proposicionales polivalentes.

La estructura de la comunicación es la siguiente: En la sección 1, recordamos conceptos sintácticos y semánticos de las lógicas polivalentes. A continuación, reducimos el problema de la validez en lógicas polivalentes al de pertenencia a un ideal (sección 2) y al de cálculo de una base de Gröbner (sección 3). Finalmente, en la sección 4 damos algoritmos para resolver los anteriores problemas.

1 LÓGICAS POLIVALENTES

1.1 Notaciones. En lo que sigue:

(1) n, s son dos números enteros positivos.
(2) $\{X_1, \ldots, X_n\}$ es un conjunto cuyos elementos se interpretarán como **variables proposicionales**.
(3) $\{f_1, \ldots, f_s\}$ es un conjunto, disjunto con $\{X_1, \ldots, X_n\}$, cuyos elementos se interpretarán como **conectivas**.
(4) Para cada $j \in \{1, \ldots, s\}$, $\delta(j)$ es un número entero positivo que se interpretará como la **aridad** de la conectiva f_j.

1.2 Definición. El conjunto $\mathbf{P}(X_1, \ldots, X_n)$ de las **proposiciones** en las variables $X_1, \ldots, X_n$ y las conectivas $f_1, \ldots, f_s$ se define recursivamente por:

(1) Para todo $i \in \{1, \ldots, n\}$, $X_i \in \mathbf{P}(X_1, \ldots, X_n)$.
(2) Si $j \in \{1, \ldots, s\}$ y $A_1, \ldots, A_{\delta(j)} \in \mathbf{P}(X_1, \ldots, X_n)$, entonces $f_j(A_1, \ldots, A_{\delta(j)}) \in \mathbf{P}(X_1, \ldots, X_n)$.

1.3 Notaciones. En lo que sigue:

(1) Usaremos las letras A, B (posiblemente con subíndices) como variables para proposiciones.
(2) p es un número primo.
(3) $\mathbf{Z}_p$ es el cuerpo de los enteros módulo p, cuyos elementos se interpretarán como **valores de verdad**. En particular, 0 se interpretará como **falso** y 1 como **verdadero**.

(4) Para cada $j \in \{1, \ldots, s\}$, H_j es una aplicación de $\mathbf{Z}_p^{\delta(j)}$ en $\mathbf{Z}_p$ que se interpretará como la **tabla de verdad** de la conectiva f_j.

1.4 Ejemplo. En el sistema trivalente de Lukasiewicz, L_3, $p = 3$; 2 se interpreta como indeterminado; las conectivas son $f_1 = \neg$ (negación), $f_2 = \Diamond$ (posibilidad), $f_3 = Ł$ (necesidad), $f_4 = \vee$ (disyunción), $f_5 = \wedge$ (conjunción), $f_6 = \rightarrow$ (implicación) y $f_7 = \leftrightarrow$ (equivalencia); las aridades son $\delta(1) = \delta(2) = \delta(3) = 1$, $\delta(4) = \cdots = \delta(7) = 2$; y las tablas de verdad son las funciones H_i definidas por

a	$H_1(a)$	$H_2(a)$	$H_3(a)$
0	1	0	0
1	0	1	1
2	2	1	0

a	b	$H_4(a,b)$	$H_5(a,b)$	$H_6(a,b)$	$H_7(a,b)$
0	0	0	0	1	1
0	1	1	0	1	0
0	2	2	0	1	2
1	0	1	0	0	0
1	1	1	1	1	1
1	2	1	2	2	2
2	0	2	0	2	2
2	1	1	2	1	2
2	2	2	2	1	1

1.5 Definiciones.

(1) Una **valoración** es una aplicación $v : \{X_1, \ldots, X_n\} \to \mathbf{Z}_p$.

(2) Para cada valoración v se define $\hat{v} : \mathbf{P}(X_1, \ldots, X_n) \to \mathbf{Z}_p$ recursivamente por:

$$\hat{v}(A) = \begin{cases} v(A), & \text{si } A \in \{X_1, \ldots, X_n\}; \\ H_j(\hat{v}(A_1), \ldots, \hat{v}(A_{\delta(j)})), & \text{si } A \text{ es } f_j(A_1, \ldots, A_{\delta(j)}). \end{cases}$$

(3) A es una **tautología**, $\models A$, si para toda valoración v, $\hat{v}(A) = 1$.

(4) A es una **consecuencia tautológica** de $\{B_1, \ldots, B_m\}$, $\{B_1, \ldots, B_m\} \models A$, si para toda valoración v,

$$\hat{v}(B_1) = \cdots = \hat{v}(B_m) = 1 \quad \Longrightarrow \quad \hat{v}(A) = 1.$$

1.6 Ejemplos. En L_3 se tiene:

(1) $\models X \leftrightarrow \neg\neg X$.

(2) $X \vee \neg X$ y $(\Diamond X \wedge (X \rightarrow Y)) \rightarrow \Diamond Y$ no son tautologías.

(3) $\{\Diamond X, X \rightarrow Y\} \models \Diamond Y$.

1.7 Nota. El objetivo del presente trabajo consiste en resolver mediante algoritmos algebraicos los siguientes problemas:

- Problema 1 Dada una proposición A, decidir si $\models A$.
- Problema 2 Dada una proposición A_0 y un conjunto finito de proposiciones $\{A_1, \ldots, A_m\}$, decidir si $\{A_1, \ldots, A_m\} \models A_0$. ∎

2 TAUTOLOGIAS E IDEALES

2.1 Notación. En lo que sigue:

(1) $\mathbf{Z}_p[X_1, \ldots, X_n]$ es el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ y con coeficientes en $\mathbf{Z}_p$.
(2) Usaremos las letras p, q, r (posiblemente con subíndices) como variables para polinomios.
(3) Usaremos las letras F, G (posiblemente con subíndices) como variables para conjuntos de polinomios distintos de cero.

2.2 Definición. Para cada valoración v, $v^* : \mathbf{Z}_p[X_1, \ldots, X_n] \to \mathbf{Z}_p$ es el único homomorfismo tal que $v^*(X_i) = v(X_i)$, para todo $i \in \{1, \ldots, n\}$.

2.3 Definición.

(1) Para cada conectiva f_j se define la aplicación

$$\theta_j : \mathbf{Z}_p[X_1, \ldots, X_n]^{\delta(j)} \to \mathbf{Z}_p[X_1, \ldots, X_n]$$

por

$$\theta_j(q_1, \ldots, q_{\delta(j)}) = \sum_{\substack{0 \le i_1 \le p-1 \\ \cdots\cdots\cdots\cdots \\ 0 \le i_{\delta(j)} \le p-1}} H_j(i_1, \ldots, i_{\delta(j)}) L_{i_1}(q_1) \ldots L_{i_{\delta(j)}}(q_{\delta(j)}),$$

donde $L_0(q) = 1 - q^{p-1}$ y $L_i(q) = L_0(q - i)$ para $i \in \{1, \ldots, p-1\}$.

(2) La aplicación $\theta : \mathbf{P}(X_1, \ldots, X_n) \to \mathbf{Z}_p[X_1, \ldots, X_n]$ está definida por:

$$\theta(A) = \begin{cases} A, & \text{si } A \in \{X_1, \ldots, X_n\}; \\ \theta_j(\theta(A_1), \ldots, \theta(A_{\delta(j)})), & \text{si } A \text{ es } f_j(A_1, \ldots, A_{\delta(j)}). \end{cases}$$

2.4 Ejemplo. En L_3,

$$\begin{aligned}
\theta_1(q) &= 2q + 1, \\
\theta_2(q) &= q^2, \\
\theta_3(q) &= 2q^2 + 2, \\
\theta_4(q_1, q_2) &= 2q_1^2q_2^2 + q_1^2q_2 + q_1q_2^2 + q_1q_2 + q_1 + q_2, \\
\theta_5(q_1, q_2) &= q_1^2q_2^2 + 2q_1^2q_2 + 2q_1q_2^2 + 2q_1q_2, \\
\theta_6(q_1, q_2) &= q_1^2q_2^2 + 2q_1^2q_2 + 2q_1q_2^2 + 2q_1q_2 + 2q_1 + 1, \\
\theta_7(q_1, q_2) &= 2q_1^2q_2^2 + q_1^2q_2 + q_1q_2^2 + q_1q_2 + 2q_1 + 2q_2 + 1.
\end{aligned}$$

2.5 Lema. Para toda valoración v, $\hat{v} = v^* \circ \theta$.

Demostración: Por inducción sobre la longitud de las proposiciones. ∎

2.6 Definición. El **ideal engendrado** por $F = \{q_1, \ldots, q_m\}$ es

$$I(F) = \left\{ \sum_{i=1}^{m} r_i q_i : r_i \in \mathbf{Z}_p[X_1, \ldots, X_n] \right\}$$

Escribiremos $(q_1, \ldots, q_m)$ en lugar de $I(\{q_1, \ldots, q_m\})$.

2.7 Lema. Si $I = (X_1^p - X_1, \ldots, X_n^p - X_n)$, entonces son equivalentes:

(a) $q \in I$.

(b) Para toda valoración v, $v^*(q) = 0$.

Demostración:

(a) $\Longrightarrow$ (b): Por el Primer Teorema de Fermat.

(b) $\Longrightarrow$ (a): Por inducción sobre n. ∎

2.8 Teorema. Sea $A \in \mathbf{P}(X_1, \ldots, X_n)$. Entonces

$$\models A \iff \theta(A) - 1 \in (X_1^p - X_1, \ldots, X_n^p - X_n)$$

Demostración:

$$\begin{array}{lll} \models A & \iff & (\forall v)[\hat{v}(A) = 1] \qquad \text{[por 1.5]} \\ & \iff & (\forall v)[v^*(\theta(A)) = 1] \qquad \text{[por 2.5]} \\ & \iff & (\forall v)[v^*(\theta(A) - 1) = 0] \\ & \iff & \theta(A) - 1 \in (X_1^p - X_1, \ldots, X_n^p - X_n) \qquad \text{[por 2.7]} \ ∎ \end{array}$$

2.9 Lema. Sean $q_0, q_1, \ldots q_m \in \mathbf{Z}_p[X_1, \ldots, X_n]$. Son equivalentes:

(a) Para toda valoración v,

$$v^*(q_1) = \cdots = v^*(q_m) = 0 \implies v^*(q_0) = 0.$$

(b) Para toda valoración v,

$$v^*((q_0 + q_1 + \cdots + q_m)(q_1^{p-1} - 1) \cdots (q_m^{p-1} - 1)) = 0.$$

(c) $(q_0 + q_1 + \cdots + q_m)(q_1^{p-1} - 1) \cdots (q_m^{p-1} - 1) \in (X_1^p - X_1, \ldots, X_n^p - X_n)$.

(d) $q_0 \in (q_1, \ldots, q_m, X_1^p - X_1, \ldots, X_n^p - X_n)$.

Demostración:

(a) $\Longrightarrow$ (b): Por ser v^* homomorfismo y por el Primer Teorema de Fermat.

(b) $\Longrightarrow$ (c): Por el Lema 2.7.

(c) $\Longrightarrow$ (d): Trivial.

(d) $\Longrightarrow$ (a): Por el Primer Teorema de Fermat.

2.10 Teorema. Sean $A_0, A_1, \ldots, A_m \in \mathbf{P}(X_1, \ldots, X_n)$. Son equivalentes:

(a) $\{A_1, \ldots, A_m\} \models A_0$.

(b) $\theta(A_0) - 1 \in (\theta(A_1) - 1, \ldots, \theta(A_m) - 1, X_1^p - X_1, \ldots, X_n^p - X_n)$.

(c) $\displaystyle\sum_{i=0}^{m} (\theta(A_i) - 1) \prod_{j=1}^{m} \sum_{k=1}^{p-1} \theta(A_j)^k \in (X_1^p - X_1, \ldots, X_n^p - X_n)$.

Demostración: (a) $\Longleftrightarrow$ (b): Por 1.5, 2.5 y 2.9, se tiene

$\{A_1, \ldots, A_m\} \models A_0 \iff$

$\iff \quad (\forall v)[\hat{v}(A_1) = \cdots = \hat{v}(A_m) = 1 \implies \hat{v}(A_0) = 1]$

$\iff \quad (\forall v)[v^*(\theta(A_1)) = \cdots = v^*(\theta(A_m)) = 1 \implies v^*(\theta(A_0)) = 1]$

$\iff \quad (\forall v)[v^*(\theta(A_1) - 1) = \cdots = v^*(\theta(A_m) - 1) = 0 \implies v^*(\theta(A_0) - 1) = 0]$

$\iff \quad \theta(A_0) - 1 \in (\theta(A_1) - 1, \ldots, \theta(A_m) - 1, X_1^p - X_1, \ldots, X_n^p - X_n)$

(b) $\Longleftrightarrow$ (c): Por el Lema 2.9. ∎

2.11 Nota. Mediante los Teoremas 2.8 y 2.10, los Problemas de la Nota 1.7 se reducen al siguiente:

- Problema 3 Dado un conjunto finito de polinomios $\{q_1, \ldots, q_m\}$ y un polinomio q_0 , decidir si $q_0 \in (q_1, \ldots, q_m)$.

3 IDEALES Y BASES DE GRÖBNER

3.1 Notación. En lo que sigue:

(1) Usaremos la letra a (posiblemente con subíndices) como variable para **términos** (i.e. polinomios de la forma $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$).
(2) Usaremos la letra u (posiblemente con subíndices) como variable para elementos de $\mathbf{Z}_p$.

3.2 Definición. En el conjunto de los términos de $\mathbf{Z}_p[X_1, \ldots, X_n]$ se define la relación $>_T$ por:
$X_1^{\alpha_1} \ldots X_n^{\alpha_n} >_T X_1^{\beta_1} \ldots X_n^{\beta_n}$ syss
$\alpha_1 + \cdots + \alpha_n > \beta_1 + \cdots + \beta_n$ ó
$\alpha_1 + \cdots + \alpha_n = \beta_1 + \cdots + \beta_n$ y $(\exists i \in \{1, \ldots, n\})[\alpha_i > \beta_i \wedge (\forall j)[1 \leq j < i \rightarrow \alpha_j = \beta_j]]$

3.3 Definición. Sea q un polinomio distinto de cero.

(1) Para cada término a, $\mathrm{coef}(a, q)$, representa el coeficiente de a en q.
(2) El **término líder** de q, $\mathrm{TL}(q)$, es el mayor término a (respecto de $>_T$) tal que $\mathrm{coef}(a, q) \neq 0$.
(3) El **coeficiente líder** de q es $\mathrm{CL}(q) = \mathrm{coef}(\mathrm{TL}(q), q)$.
(4) El **resto** de q es $\mathrm{R}(q) = q - \mathrm{CL}(q)\mathrm{TL}(q)$.

3.4 Definición. Sea q un polinomio distinto de cero, F un conjunto de polinomios distintos de cero y a un término.

(1) $\rho(q, a) : \mathbf{Z}_p[X_1, \ldots, X_n] \rightarrow \mathbf{Z}_p[X_1, \ldots, X_n]$ está definida por:

$$\rho(q, a)(r) = r - \frac{\mathrm{coef}(a\mathrm{TL}(q), r)}{\mathrm{CL}(q)} aq.$$

(2) $r_1 \longrightarrow_{q,a} r_2$ si $r_2 = \rho(q, a)(r_1) \neq r_1$.
(3) $r_1 \longrightarrow_q r_2$ si existe un término a tal que $r_1 \longrightarrow_{q,a} r_2$.
(4) $r_1 \longrightarrow_F r_2$ si existe un $q \in F$ tal que $r_1 \longrightarrow_q r_2$.
(5) $r_1 \xrightarrow{*}_F r_2$ si existen $k \in \mathbf{N}$ y $q_0, \ldots, q_k \in \mathbf{Z}_p[X_1, \ldots, X_n]$ tales que

$$r_1 = q_0 \longrightarrow_F q_1 \longrightarrow_F \cdots \longrightarrow_F q_k = r_2.$$

3.5 Definición. Sea F un conjunto finito de polinomios distintos de cero.

(1) q es **reducible** (respecto de F) si existe un r tal que $q \longrightarrow_F r$; en caso contrario, se dice que q es **irreducible** (respecto de F).

(2) q es una **forma irreducible** (respecto de F) de r si q es irreducible respecto de F y $r \xrightarrow{*}_F q$.

3.6 Nota. Dado un conjunto finito F de polinomios distintos de cero, cada polinomio tiene al menos una forma irreducible respecto de F; pero puede tener más de una (ver ejemplo en 4.1.2).

3.7 Definición. Un conjunto finito F de polinomios distintos de cero es una **base de Gröbner** si cada polinomio tiene una única forma irreducible respecto de F.

3.8 Teorema (Buchberger, 1976). Si F es una base de Gröbner, entonces

$$I(F) = \{q \in \mathbf{Z}_p[X_1, \ldots, X_n] : q \xrightarrow{*}_F 0\}.$$

3.9 Nota. Mediante el Teorema anterior, el Problema 3 de la Nota 2.11 se reduce a los siguientes:

- Problema 4 Dado un conjunto finito F de polinomios distintos de cero y un polinomio q, calcular una forma irreducible de q respecto de F.
- Problema 5 Dado un conjunto finito F de polinomios distintos de cero, calcular una base de Gröbner G tal que $I(G) = I(F)$.

4 ALGORITMOS Y EJEMPLOS

4.1 Algoritmo de forma normal

4.1.1 Algoritmo. (de forma normal para el Problema 4)
Entrada: Un conjunto finito $F = \{q_1, \ldots, q_m\}$ de polinomios distintos de cero y un polinomio $q = u_1 a_1 + \cdots + u_k a_k$
Salida: Una forma irreducible de q respecto de F.
Procedimiento: $FN(q, F)$

$i := 1$
mientras–que $i \leq m$
  $j := 1$
  mientras–que $j \leq k$
    si $\mathrm{TL}(q_i)$ divide a a_j
      entonces $FN\left(q - \dfrac{u_j a_j}{\mathrm{CL}(q_i)\mathrm{TL}(q_i)} q_i, F\right)$
      en–otro–caso $j := j + 1$
  $i := i + 1$
devolver q

4.1.2 Ejemplo. En $\mathbf{Z}_3[X, Y]$ se consideran el conjunto $F = \{q_1 = X^2 - 1, q_2 = X^2Y^2 + 2X^2Y + 2XY^2 + 2XY + 2X, q_3 = X^3 - X, q_4 = Y^3 - Y\}$. Entonces $FN(X^3Y^3, F) = XY$, pero XY no es la única forma irreducible de X^3Y^3 respecto de F (por ejemplo, $XY^2 + Y^2 + 2Y$ es otra). Por tanto, F no es una base de Gröbner.

4.1.3 Nota. Es fácil de comprobar que el algoritmo anterior termina y es correcto.

4.2 Algoritmo de base de Gröbner

4.2.1 Definición. Sean q_1, q_2 dos polinomios distintos de cero. El **S-polinomio** de q_1 y q_2 es

$$S(q_1, q_2) = \frac{r}{a_1 u_1} q_1 - \frac{r}{a_2 u_2} q_2,$$

donde $a_i = \mathrm{CL}(q_i)$, $u_i = \mathrm{TL}(q_i)$ y $r = \mathrm{mcm}(u_1, u_2)$.

4.2.2 Algoritmo. (de base de Gröbner para el Problema 5)
Entrada: Un conjunto finito $F = \{q_1, \ldots, q_m\}$ de polinomios distintos de cero.
Salida: Una base de Gröbner G tal que $I(G) = I(F)$.
Procedimiento: $BG(F)$

$(\forall i \in \{1, \ldots, m\})\left[r_i := \dfrac{q_i}{\mathrm{CL}(q_i)}\right]$
$G := \{r_i : i \in \{1, \ldots, m\}\}$
$G := Reduce(G)$ [Supongamos que $G = \{q'_1, \ldots, q'_k\}$]
$B := \{(q'_i, q'_j) : 1 \leq i < j \leq k\}$
mientras–que $B \neq \emptyset$ **hacer**
(q'_i, q'_j) un elemento de B
$B := B - \{(q'_i, q'_j)\}$
$r := FN(S(q'_i, q'_j), G)$
si $r \neq 0$ **entonces** $BG(G \cup \{r\})$
devolver G

Subalgoritmo. (de reducción)
Entrada: Un conjunto finito $F = \{q_1, \ldots, q_m\}$ de polinomios mónicos distintos de cero.
Salida: Un conjunto G de polinomios mónicos tal que $I(G) = I(F)$ y
$FN(q, G - \{q\}) = q$ para todo $q \in G$.
Procedimiento: $Reduce(F)$

$G := F$
si $(\exists q \in G)[FN(q, G - \{q\}) \neq q]$
entonces $i := \inf\{j \in \{1, \ldots, m\} : FN(q_j, G - \{q_j\}) \neq q_j\ \}$
$G := G - \{q_i\}$
$q := FN(q_i, G)$
si $q = 0$ **entonces** $Reduce(G)$
en–otro–caso $Reduce(G \cup \{q/\mathrm{CL}(q)\})$
en-otro-caso devolver G

4.2.3 Ejemplo. Vamos a aplicar el algoritmo de bases de Gröbner al conjunto F del Ejemplo 4.1.2:

En primer lugar aplicamos el algoritmo de reducción y obtenemos $G = \{q'_1 = X^2 - 1, q'_2 = Y^3 - Y, q'_3 = XY^2 + XY + 2Y^2 + X + Y\}$ y $B = \{(q'_1, q'_2), (q'_1, q'_3), (q'_2, q'_3)\}$. Elegimos $(q'_1, q'_3) \in B$ y calculamos $r = FN(S(q'_1, q'_3), G) = XY + 2X + Y + 2$. Puesto que $r \neq 0$, tenemos que calcular $BG(\{q'_1, q'_2, q'_3, r\})$. Al aplicar el algoritmo de reducción se obtiene $G = \{q'_1 = X^2 - 1, q'_2 = XY + 2X + Y + 2, q'_3 = Y^2 + 2\}$. Puesto que,

$FN(S(q_1', q_2'), G) = 0$, $FN(S(q_1', q_3'), G) = 0$, $FN(S(q_2', q_3'), G) = 0$, se tiene que $BG(F) = \{X^2 - 1, XY + 2X + Y + 2, Y^2 + 2\}$.

4.2.4 Teorema. El algoritmo de la base de Gröbner es correcto.

Demostración (Esquema): La terminación se demuestra a partir del teorema de la base de Hilbert y la corrección parcial a partir del siguiente teorema:

Teorema (Buchberger) G es una base de Gröbner syss para todo $q_1, q_2 \in G$, $S(q_1, q_2) \xrightarrow{*}_G 0$.

4.3 Algoritmos de validez

4.3.1 Algoritmo. (de deducción)
Entrada: Una proposición A_0 y un conjunto finito $\Gamma = \{A_1, \ldots, A_m\}$ de proposiciones.
Salida: "S´", si $\Gamma \models A_0$; "NO", en caso contrario.
Procedimiento:

$G := BG((\{\theta(A_i) - 1 : 1 \leq i \leq m\} \cup \{X_i^p - X_i : 1 \leq i \leq n\}) - \{0\})$
$q := FN(\theta(A_0) - 1, G)$
si $q = 0$ **entonces devolver** "S´"
en–otro–caso devolver "NO"

4.3.2 Teorema. El algoritmo de deducción es correcto.

Demostración: Sean $F = \{\theta(A_1) - 1, \ldots, \theta(A_m) - 1, X_1^p - X_1, \ldots, X_n^p - X_n\}$ y $G = BG(F - \{0\})$.

$$\begin{array}{rcll} \Gamma \models A_0 & \iff & \theta(A_0) - 1 \in I(F) & \text{[por 2.10]} \\ & \iff & \theta(A_0) - 1 \in I(G) & \text{[por 4.2.4]} \\ & \iff & \theta(A_0) - 1 \xrightarrow{*}_G 0 & \text{[por 3.8]} \\ & \iff & FN(\theta(A_0) - 1, G) = 0, & \end{array}$$

ya que $FN(\theta(A_0) - 1, G)$ es la única forma irreducible de $\theta(A_0) - 1$ respecto de G. ∎

4.3.3 Ejemplo. Consideremos, en L_3, la proposición $A_0 = \Diamond Y$ y el conjunto $\Gamma = \{A_1, A_2\}$, siendo $A_1 = \Diamond X$ y $A_2 = X \to Y$. Vamos a usar el algoritmo de deducción para decidir si $\Gamma \models A_0$.

$$\begin{aligned} G &= BG(\{X^2 - 1, X^2Y^2 + 2X^2Y + 2XY^2 + 2XY + 2X, X^3 - X, Y^3 - Y\} \\ &= \{X^2 - 1, XY + 2X + Y + 2, Y^2 + 2\}, \end{aligned}$$

por el Ejemplo 4.2.3. Puesto que, $FN(\theta(A_0) - 1, G) = FN(Y^2 - 1, G) = 0$, resulta que $\Gamma \models A_0$.

4.3.4 Algoritmo. (de validez)
Entrada: Una proposición A.
Salida: "S´", si $\models A$; "NO", en caso contrario.
Procedimiento:

$G := \{X_i^p - X_i : 1 \leq i \leq n\}$
$q := FN(\theta(A) - 1, G)$
si $q = 0$ **entonces devolver** "S´"
en–otro–caso devolver "NO"

4.3.5 Teorema. El algoritmo de validez es correcto.

Demostración: Análoga a la del Teorema 4.3.2, observando que $\{X_i^p - X_i : 1 \leq i \leq n\}$ es una base de Gröbner. ∎

4.3.6 Ejemplo. Vamos a aplicar el algoritmo anterior para estudiar la validez en L_3 de las siguientes proposiciones: $A_1 = X \leftrightarrow \neg\neg X$ (eliminación de la doble negación), $A_2 = X \vee \neg X$ (ley del tercio excluido) y $A_3 = (\Diamond X \wedge (X \rightarrow Y)) \rightarrow \Diamond Y$.

Sea $F = \{X^3 - X\}$. Puesto que, $FN(\theta(A_1) - 1, F) = FN(2X^4 + 2X^3 + X^2 + X, F) = 0$, $FN(\theta(A_2) - 1, F) = FN(2X^4 + 2X^3 + 2X, F) = 2X^2 + X$ y $FN(\theta(A_3) - 1, F) = X^2Y^2 + 2X^2 + 2XY^2 + X + 1$, resulta que A_1 es una tautología de L_3 y A_2, A_3 no lo son.

4.3.7 Algoritmo. (de deducción. Versión 2)
Entrada: Una proposición A_0 y un conjunto finito $\Gamma = \{A_1, \ldots, A_m\}$ de proposiciones.
Salida: "S´", si $\Gamma \models A_0$; "NO", en caso contrario.
Procedimiento:

$G := \{X_i^p - X_i : 1 \leq i \leq n\}$
$q := FN\left(\sum_{i=0}^{m}(\theta(A_i) - 1)\prod_{j=1}^{m}\sum_{k=1}^{p-1}\theta(A_j)^k, G\right)$
si $q = 0$ **entonces devolver** "S´"
en–otro–caso devolver "NO"

4.3.8 Teorema. El algoritmo anterior es correcto.

Demostración: Análoga a la del Teorema 4.3.5. ∎

5 IMPLEMENTACIÓN

Los anteriores algoritmos pueden implementarse directamente en REDUCE. El Apéndice A es un programa en REDUCE de los algoritmos 4.3.4 y 4.3.7 para la lógica trivalente de Lukasiewicz. El Apéndice B es una sesión en REDUCE usando el programa anterior (en la que se ha subrayado los mensajes del sistema).

BIBLIOGRAF´A

Buchberger, B. (1985), "Gröbner Basis: An Algorithmic Method in Polynomial Ideal Theory", en N.K. Bose, ed. *Multidimensional Systems Theory.* Reidel, Dordrecht.

Hsiang, J. (1985), "Refutational Theorem Proving using Term–Rewriting Systems" *Artificial Intelligence*, **25**, pp. 255–300.

Kapur, D. y P. Narendran (1985) "An Equational Approach to Theorem Proving in First Order Predicate Calculus", en 9th IJCAI.

Moisil, G.C. (1969) *The Algebraic Theory of Switching Circuits* Pergamon Press, Oxford.

Rescher, N. (1969) *Many–valued Logic.* McGraw–Hill, New York.

Apéndice A: Lógica trivalente de Lukasiewicz (Programa)

```
% Las conectivas se representan por NN (negacion), MM (posibilidad)
% LL (necesidad), OO (disyuncion), YY (conjuncion), II (implicacion)
% y EE (equivalencia).

% Transformaciones de formulas en polinomios (Ejemplo 2.4)
FOR ALL X LET
    NN(X) = 2*X+1,
    MM(X) = X**2,
    LL(X) = 2*X**2 + 2*X;
FOR ALL X,Y LET
    OO(X,Y) = 2*X**2*Y**2 + X**2*Y + X*Y**2 + X*Y + X + Y,
    YY(X,Y) = X**2*Y**2 + 2*X**2*Y + 2*X*Y**2 + 2*X*Y,
    II(X,Y) = X**2*Y**2 + 2*X**2*Y + 2*X*Y**2 + 2*X*Y + 2*X + 1,
    EE(X,Y) = 2*X**2*Y**2 + X**2*Y + X*Y**2 + X*Y + 2*X + 2*Y + 1;
INFIX OO, YY, II, EE;

% Algoritmo 4.3.4
PROCEDURE PRUEBA A;
BEGIN
  SETMOD 3;
  ON MODULAR;
  FOR ALL X LET X**3 = X;
  IF A - 1 = 0 THEN <<RETURN "SI";>> ELSE <<RETURN "NO";>>;
END;

% Algoritmo 4.3.7
PROCEDURE DEDUCE;
BEGIN
  OFF MODULAR;
  WRITE "ESCRIBE EL NUMERO DE PREMISAS";
  M:=XREAD();
  OPERATOR A;
  FOR I:=1:M DO
      <<WRITE "ESCRIBE LA PREMISA ",I;A(I):=XREAD()>>;
  WRITE "ESCRIBE LA CONCLUSION ";
  A(0):=XREAD();
  FOR ALL X LET X**3 = X;
  AUX:=(FOR I:=0:M SUM A(I)-1) *
       (FOR J:=1:M PRODUCT FOR K:=1:2 SUM A(J)**K);
  OFF MODULAR;
  SETMOD 3;
  ON MODULAR;
  IF AUX = 0 THEN <<RETURN "SI";>> ELSE <<RETURN "NO";>>;
END;

END;
```

Apéndice B: Lógica trivalente de Lukasiewicz (Sección)

```
C> REDUCE
REDUCE .....
1: IN "L3.RED"; % carga el programa del Apendice A
2: PRUEBA (X EE (NN (NN X)));
SI
3: PRUEBA (X OO (NN X));
NO
4: PRUEBA (((MM X) YY (X II Y)) II (MM Y)):
NO
5: DEDUCE ();
ESCRIBE EL NUMERO DE PREMISAS
2;
ESCRIBE LA PREMISA 1
MM X;
ESCRIBE LA PREMISA 2
X II Y;
ESCRIBE LA CONCLUSION
MM Y;
SI
5: QUIT;
```