

# Algunas aplicaciones de las bases de Gröbner en Inteligencia Artificial<sup>1</sup>

**EUGENIO ROANES LOZANO**

Departamento de Algebra,  
Facultad de Educación & Facultad de CC. Matemáticas,  
Universidad Complutense de Madrid  
eroanes@mat.ucm.es

**I Jornadas de Lógica, Computación e I. A.  
Jornadas homenaje al profesor Luis M. Laita  
Sevilla, 13-14 Noviembre 2008**

---

<sup>1</sup>Esta charla está basada en el artículo:

E. Roanes Lozano, Luis M. Laita, E. Roanes Macías: Cálculos efectivos en lógica proposicional booleana interpretada como un anillo de clases residuales (polinomial) sobre  $\mathbb{Z}_2$ . *Bol. Soc. "Puig Adam" de Profs. de Matemáticas*, 65, 17–42, 2003.

# **1 PREÁMBULO: ÁLGEBRAS DE BOOLE Y ANILLOS BOOLEANOS**

## 1.1 RETÍCULOS

**1.1.1 Definición.-** *Un conjunto en el que hay definidas dos operaciones internas diremos que es un retículo si las dos operaciones son conmutativas, asociativas y cada una es cancelativa (simplificativa) respecto de la otra. Como consecuencia ambas operaciones son idempotentes.*

**1.1.2 Ejemplo.-**  $(\mathcal{P}(E), \cup, \cap)$  *tiene estructura de retículo:*  
 $\forall A, B, C \in \mathcal{P}(E)$ :

- $A \cup B = B \cup A$  ;  $B \cap A = A \cap B$
- $A \cup (B \cup C) = (A \cup B) \cup C$  ;  $A \cap (B \cap C) = (A \cap B) \cap C$
- $A \cup (B \cap A) = A$  ;  $A \cap (B \cup A) = A$

*Como consecuencia:*

- $A \cup A = A$  ;  $A \cap A = A$

*Probemos una de ellas:*

- $A \cup A = A \cup (A \cap (B \cup A)) = A \cup (A \cap D) = A \cup (D \cap A) = A$

## 1.2 RETÍCULO Y ORDEN RETICULAR

**1.2.1 Definición.-** *Denominaremos orden reticular a un orden parcial no estricto tal que, para dos elementos cualesquiera, siempre exista ínfimo y supremo.*

**1.2.2 Proposición.-** *A partir de un retículo se puede definir un orden reticular. Recíprocamente, a partir de un orden reticular, se puede definir un retículo.*

**1.2.3 Ejemplo.-** *Consideremos el retículo de partes de  $(\mathcal{P}(E), \cup, \cap)$ . A partir de las operaciones del retículo se puede definir un orden reticular:*

$$\forall A, B \in \mathcal{P}(E), A \sqsubseteq B \Leftrightarrow A \cup B = B \quad (\Leftrightarrow A \cap B = A)$$

*Es inmediato que la relación así definida es un orden reticular. Observemos que, en este caso,  $\sqsubseteq$  resulta ser  $\subseteq$ .*

**1.2.4 Ejemplo.-** *Recíprocamente, consideremos el conjunto de partes de  $E$ , y el orden reticular  $\subseteq$ , esto es,  $(\mathcal{P}(E), \subseteq)$ .*

*A partir del orden reticular se pueden reconstruir las operaciones del retículo:*

- $\forall A, B \in \mathcal{P}(E), A \sqcup B = \sup_{\subseteq}(A, B)$
- $\forall A, B \in \mathcal{P}(E), A \sqcap B = \inf_{\subseteq}(A, B)$ .

*Es sencillo probar que  $(\mathcal{P}(E), \sqcup, \sqcap)$  es un retículo.*

*Observemos que, en este caso,  $\sqcup$  y  $\sqcap$  resultan ser, respectivamente,  $\cup$  y  $\cap$ .*

## 1.3 ÁLGEBRAS DE BOOLE

### 1.3.1 **Definición.-** *Un retículo que sea*

- *distributivo: e.e., tal que cada una de las dos operaciones es distributiva respecto de la otra*

*y*

- *complementario: e.e.,*
  - *en el que existan ínfimo y supremo (para el orden reticular) del retículo*
  - *en el que haya definida una operación unaria “complemento”, tal que:*
    - \* *al operar con la primera operación del retículo cada elemento con su complemento, se obtenga el supremo del retículo*
    - \* *al operar con la segunda operación del retículo cada elemento con su complemento, se obtenga el ínfimo del retículo*

*se denomina “álgebra de Boole”.*

**1.3.2 Ejemplo.-** *Veamos como  $(\mathcal{P}(E), \cup, \cap, ')$  es un álgebra de Boole.*

- $\cup$  es distributiva respecto de  $\cap$  y viceversa.
- El ínfimo del retículo (para  $\subseteq$ ) es  $\emptyset$  y el supremo del retículo (para  $\subseteq$ ) es  $E$ . Además,  $'$  funciona como complementario:  $\forall A \in \mathcal{P}(E): A \cup A' = E$  ;  $A \cap A' = \emptyset$

**1.3.3 Observación.-** *Los caracteres “distributivo” y “complementario” de un retículo son independientes.*

**1.3.4 Ejemplo.-**

- *El retículo de las variedades lineales del plano vectorial con la suma de variedades lineales y la intersección es un retículo complementario pero no distributivo (si  $R, S, T$  son rectas vectoriales distintas, no se verifica:  $R + (S \cap T) = (R + S) \cap (R + T)$ ).*
- *El retículo  $(\mathbb{N}, \text{mcd}, \text{mcm})$  es distributivo, pero no complementario (el ínfimo es 1 y el supremo 0, pero p.ej. 3 no tiene complementario).*
- *El retículo de los convexos del plano, la unión convexa (menor convexo que contiene a la unión) y la intersección es un retículo, pero no es ni distributivo (p.ej.  $A \cap (B \overset{*}{\cup} C)$ , siendo  $A, B, C$  tres cuadrados alineados disjuntos, el  $A$  en medio) ni complementario (una recta no tiene complementario).*

## 1.4 ÁLGEBRAS DE BOOLE Y ANILLOS BOOLEANOS

**1.4.1 Definición.-** *Un anillo booleano es un anillo (con unidad<sup>2</sup>) tal que la segunda operación es idempotente.*

**1.4.2 Proposición.-** *i) En un anillo booleano todo elemento es su propio simétrico para la primera operación.*

*ii) Además todo anillo booleano es conmutativo.*

**Demostración.-** Sean  $\sqcup$  la primera operación,  $\underline{0}$  el neutro,  $'$  el símbolo de simétrico para  $\sqcup$ ;  $\sqcap$  la segunda operación y  $\underline{1}$  la unidad.

i) Si  $a, b$  son elementos del anillo:

$$(a \sqcup b) = (a \sqcup b) \sqcap (a \sqcup b) = (a \sqcap a) \sqcup (a \sqcap b) \sqcup (b \sqcap a) \sqcup (b \sqcap b) = a \sqcup (a \sqcap b) \sqcup (b \sqcap a) \sqcup b = (a \sqcup b) \sqcup ((a \sqcap b) \sqcup (b \sqcap a))$$

pero  $\sqcup$  es grupo, luego:  $\underline{0} = (a \sqcap b) \sqcup (b \sqcap a)$  (\*).

Por tanto, si fuese  $a = b$ , por idempotencia (de  $\sqcap$ ):  $\underline{0} = a \sqcup a$ .

ii) De (\*), como respecto de  $\sqcup$  es grupo:  $(a \sqcap b)' = (b \sqcap a)$

y como todo elemento es opuesto de sí mismo:  $a \sqcap b = b \sqcap a$ .

---

<sup>2</sup>Para poder obtener de él un algebra de Boole.

**1.4.3 Proposición.-** *A partir de un álgebra de Boole se puede definir un anillo booleano.*

*Recíprocamente, a partir de un anillo booleano se puede definir un álgebra de Boole.*

**1.4.4 Ejemplo.-**  $(\mathcal{P}(E), \cup, \cap, ')$  es un álgebra de Boole (ínfimo:  $\emptyset$  ; supremo:  $E$ ). Definiendo la diferencia simétrica de dos elementos de  $\mathcal{P}(E)$ ,  $A$  y  $B$ :

$$A\Delta B = (A \cap B') \cup (A' \cap B)$$

*tenemos que  $(\mathcal{P}(E), \Delta, \cap)$  es un anillo conmutativo con unidad.*

*En efecto: todas las propiedades son inmediata consecuencia de la correspondiente propiedad del álgebra de Boole o son simplemente una manipulación más o menos larga (como la conmutatividad y asociatividad de  $\Delta$ );*

- $\emptyset$  es el neutro de  $\Delta$  (y el absorbente de  $\cap$ )
- $E$  es el neutro de  $\cap$ .

*y como,  $\forall A \in \mathcal{P}(E)$ ,*

- $A\Delta A = \emptyset$

*todo elemento de  $\mathcal{P}(E)$  es simétrico de sí mismo para  $\Delta$ .*

**1.4.5 Ejemplo.-**  $(\mathcal{P}(E), \Delta, \cap)$  es un anillo (booleano).

Definiendo, en este anillo la siguiente operación:

$$A \sqcup B = (A \Delta B) \Delta (A \cap B)$$

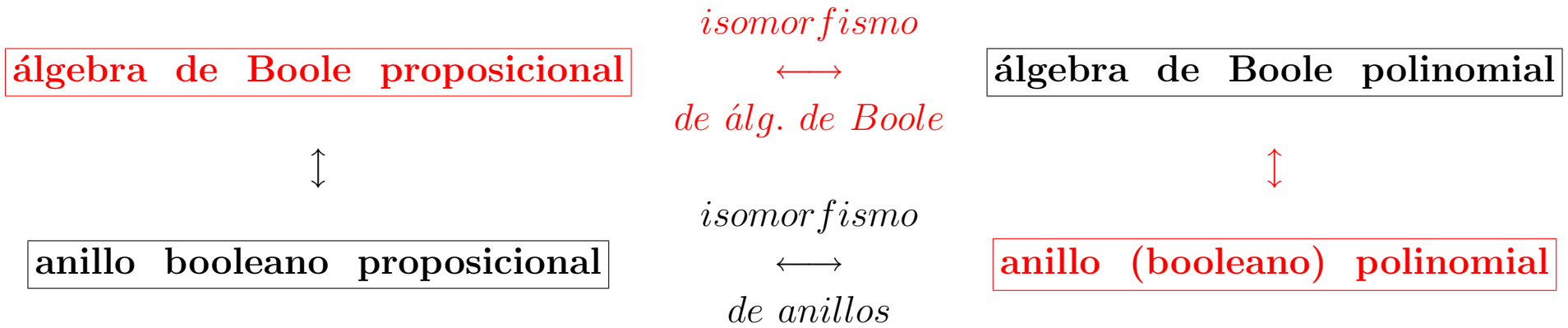
obtenemos un álgebra de Boole (véase el ejemplo siguiente).

**1.4.6 Proposición.-** Si partimos de un álgebra de Boole y obtenemos el correspondiente anillo booleano, y a partir de este obtenemos la correspondiente álgebra de Boole, resulta el álgebra de Boole de partida.

**1.4.7 Ejemplo.-** Prosiguiendo con el ejemplo anterior:

$$A \sqcup B = (A \Delta B) \Delta (A \cap B) = ((A \Delta B) \cap (A \cap B)') \cup ((A \Delta B)' \cap (A \cap B)) = (A \Delta B) \cup (A \cap B) = A \cup B$$

### 1.5 UN MODELO POLINOMIAL PARA EL ÁLGEBRA DE BOOLE PROPOSICIONAL



## **2 CONSTRUYENDO UN ANILLO BOOLEANO POLINOMIAL**

## 2.1 PRIMEROS REQUERIMIENTOS. EL ANILLO $(\mathcal{A}, +, \cdot)$

Tratemos de construir un anillo de polinomios booleano  $(\mathcal{A}, +, \cdot)$ .

- Como se ha visto en 1.4, para todo elemento es simétrico de sí mismo para la primera operación, luego:  $a \in \mathcal{A}$ ,  $a + a = 2 \cdot a = 0$ , y por tanto podemos tomar  $\mathcal{A}$  como un anillo sobre un cuerpo de característica 2.
- Los elementos del anillo booleano son idempotentes para la segunda operación (condición de anillo Booleano).

Estas dos condiciones son verificadas por el anillo de clases residuales (también  $\mathbf{k}$ -álgebra):  $(\mathcal{A}, +, \cdot)$  donde:

$$\mathcal{A} = (\mathbb{Z}/2\mathbb{Z})[x, y, \dots, z] / \langle x^2 - x, y^2 - y, \dots, z^2 - z \rangle .$$

En efecto:

**2.1.1 Proposición.-** *En  $(\mathcal{A}, +, \cdot)$  todo elemento es opuesto de él mismo.*

**2.1.2 Proposición.-** *En  $(\mathcal{A}, +, \cdot)$  todo elemento es idempotente para la operación producto.*

**Demostración.-** Si  $a \in \mathcal{A}$ , se puede escribir en la forma:

$$a = \delta_0 + \delta_x \cdot x + \delta_y \cdot y + \dots + \delta_z \cdot z + \delta_{xy} \cdot x \cdot y + \dots + \delta_{xyz} \cdot x \cdot y \cdot z + \dots$$

donde las  $\delta$  pertenecen a  $\mathbb{Z}/2\mathbb{Z}$  y por tanto son idempotentes. Puesto que hemos pasado al cociente sobre el ideal  $I$ , las variables  $x, y, \dots, z$  deben ser idempotentes también. Además, los dobles productos se anulan, luego

$$a^2 = (\delta_0 + \delta_x \cdot x + \delta_y \cdot y + \dots + \delta_z \cdot z + \delta_{xy} \cdot x \cdot y + \dots + \delta_{xyz} \cdot x \cdot y \cdot z + \dots)^2 = a$$

## 2.2 UN RESULTADO LLAMATIVO

**2.2.1 Proposición.-** *En  $\mathcal{A}$  todo elemento es divisor de cero (el resultado es cierto en cualquier anillo booleano).*

**Demostración.-** Sea  $a \in \mathcal{A}$ . Entonces:  $a \cdot (1 + a) = a + a^2 = a + a = 2 \cdot a = 0$

### **3 CONSTRUYENDO UN ÁLGEBRA DE BOOLE POLINOMIAL**

### 3.1 EL ÁLGEBRA DE BOOLE $(\mathcal{A}, \tilde{+}, \cdot, 1+)$

Probemos a definir un álgebra de Boole a partir de este anillo (como en 1.4):

**3.1.1 Definición.-** Sean  $a, b \in \mathcal{A}$ ; definimos:  $a \tilde{+} b = a + b + a \cdot b$   
(como la suma y el producto son operaciones internas en  $\mathcal{A}$ ,  $\tilde{+}$  también lo es).

**3.1.2 Observación.-** Por supuesto se puede obtener  $+$  a partir de  $\tilde{+}$  y  $\cdot$ :

$$\text{si } a, b \in \mathcal{A}: a + b = (1 + a) \cdot b \tilde{+} a \cdot (1 + b)$$

(realmente así construimos la operación del anillo booleano a partir de las operaciones del álgebra de Boole como se hizo en 1.4).

**3.1.3 Observación.-** Consideraremos  $\cdot$  prioritario frente a  $\tilde{+}$ .

**3.1.4 Proposición.-**  $(\mathcal{A}, \tilde{+}, \cdot, 1+)$  es un algebra de Boole (ínfimo: 0; supremo 1; complemento de  $a \in \mathcal{A}$ :  $1+a$ ). Por tanto se verifican las Leyes de De Morgan.

**Demostración.-**

- i) Las propiedades conmutativas, asociativas, cancelativas y distributivas se comprueban fácilmente.
- ii) Probemos por ejemplo que en  $\mathcal{A}$  todo elemento es idempotente respecto de  $\tilde{+}$ .  
En efecto: para cualquier  $a \in \mathcal{A}$ ,  $a \tilde{+} a = a + a + a \cdot a = a + a + a^2 = 0 + a = a$
- iii) El supremo del retículo es el 1 y el ínfimo el 0.

En efecto: si  $a \in \mathcal{A}$ ,

$$a \tilde{+} 0 = a + 0 + a \cdot 0 = a \quad ; \quad a \cdot 0 = 0$$

$$a \tilde{+} 1 = a + 1 + a \cdot 1 = 1 \quad ; \quad a \cdot 1 = a$$

El complementario del elemento  $a$  es  $1+a$ .

En efecto: si  $a \in \mathcal{A}$ ,

$$a \tilde{+} (1+a) = a + (1+a) + a \cdot (1+a) = a + 1 + a + a + a^2 = 1$$

$$a \cdot (1+a) = a + a^2 = a + a = 2 \cdot a = 0$$

(la existencia de  $1+a$  está asegurada por ser  $(\mathcal{A}, +, \cdot)$  anillo).

- iv) Como es bien conocido, en todo álgebra de Boole se verifican las Leyes de De Morgan. Probemos una de ellas:

$$1 + (a \tilde{+} b) = 1 + (a + b + a \cdot b) = 1 + a + b + a \cdot b$$

$$(1+a) \cdot (1+b) = 1 + a + b + a \cdot b$$

## **4 ORDENACIÓN DEL ÁLGEBRA DE BOOLE POLINOMIAL**

#### 4.1 DEFINICIÓN DE UN ORDEN RETICULAR EN $(\mathcal{A}, \tilde{+}, \cdot, 1+)$

**4.1.1 Definición.-** Sea  $\leq$  un orden reticular definido en el modo usual en el álgebra de Boole  $(\mathcal{A}, \tilde{+}, \cdot, 1+)$ :

$$\forall a, b \in \mathcal{A}: a \leq b \Leftrightarrow a \cdot b = a$$

**4.1.2 Proposición.-** En  $(\mathcal{A}, \tilde{+}, \cdot, 1+)$  son equivalentes:

- (1)  $a \cdot b = a$
- (2)  $a \tilde{+} b = b$
- (3)  $(1 + a) \tilde{+} b = 1$
- (4)  $a \cdot (1 + b) = 0$

*(la demostración es inmediata; de hecho el resultado correspondiente es cierto en cualquier álgebra de Boole).*

**4.1.3 Proposición.-** *El orden así definido en  $\mathcal{A}$  es, precisamente, “ser múltiplo”.*

**Demostración.-**  $\Rightarrow$ )  $a \leq b \Leftrightarrow a \cdot b = a \Rightarrow a$  es múltiplo de  $b$

$\Leftarrow$ )  $a$  es múltiplo de  $b \Leftrightarrow \exists k \in \mathcal{A} : a = b \cdot k \Rightarrow a \cdot b = (b \cdot k) \cdot b = b^2 \cdot k = b \cdot k = a \Leftrightarrow a \leq b$

**4.1.4 Consecuencia.-** *Para cualesquiera  $a, b \in \mathcal{A}$ :  $a, b | (a \cdot b)$  ;  $a \tilde{+} b | a, b$*

**Demostración.-** i) Trivial

ii)  $(a \tilde{+} b) \cdot a = a$  (por la propiedad cancelativa de  $\tilde{+}$  respecto de  $\cdot$ )

- Los resultados siguientes son ciertos en general, pero los particularizaremos para este álgebra de Boole para acostumbrarnos a su extraño funcionamiento.

**4.1.5 Proposición.-** Para cualesquiera  $a, b, c \in \mathcal{A}$ :

$$b|a \Leftrightarrow (1+a)|(1+b)$$

(que corresponde en el álgebra de Boole proposicional con:  $A \rightarrow B \Leftrightarrow \neg B \rightarrow \neg A$ )

**Demostración.-**  $\Rightarrow$ )  $b|a \Leftrightarrow \exists k \in \mathcal{A} : a = k \cdot b$

Por tanto, si llamamos,  $l = 1 + k \cdot b + b$

$$l \cdot (1+a) = (1 + k \cdot b + b) \cdot (1 + k \cdot b) = 1 + k \cdot b + b + k \cdot b + k^2 \cdot b^2 + k \cdot b^2 = 1 + b \Leftrightarrow (1+a)|(1+b)$$

$\Leftarrow$ ) Es consecuencia de la implicación ya probada y de que:  $1+(1+c) = c$

**4.1.6 Proposición.-** Para cualesquiera  $a, b, c \in \mathcal{A}$ :

*i)*  $c|a \Rightarrow c|(a \cdot b)$

*ii)*  $c|a$  **y**  $c|b \Rightarrow c|(a \tilde{+} b)$

**Demostración:** *ii)*  $c|a \Leftrightarrow \exists k \in \mathcal{A} : a = k \cdot c$

$$c|b \Leftrightarrow \exists l \in \mathcal{A} : b = l \cdot c$$

**luego:**  $a \tilde{+} b = a + b + a \cdot b = k \cdot c + l \cdot c + k \cdot l \cdot c^2 = (k + l + k \cdot l) \cdot c \Rightarrow c|(a \tilde{+} b)$

**4.1.7 Proposición.-** Para cualesquiera  $a, b, c \in \mathcal{A}$ :

*i)*  $a|c \Rightarrow (a \tilde{+} b)|c$

*ii)*  $a|c$  **y**  $b|c \Rightarrow (a \cdot b)|c$

**Demostración:** Consecuencia de las Leyes de De Morgan y las dos prop. anteriores.

## 5 EL ISOMORFISMO DE ÁLGEBRAS DE BOOLE $\varphi$

### 5.1 CONSTRUCCIÓN DEL HOMOMORFISMO DE ÁLGEBRAS DE BOOLE $\varphi$

Sea  $(\mathcal{C}, \vee, \wedge, \neg, \rightarrow)$  el álgebra de Boole de las proposiciones generadas por las variables proposicionales  $P, Q, \dots, R$  y denotemos por  $\underline{1}$  a la tautología y por  $\underline{0}$  a la contradicción.

Consideremos el anillo de clases residuales:  $(\mathcal{A}, \tilde{+}, \cdot, 1+, \text{“ser múltiplo”})$  donde

$$\mathcal{A} = (\mathbb{Z}/2\mathbb{Z})[p, q, \dots, r] / \langle p^2 - p, q^2 - q, \dots, r^2 - r \rangle$$

Definiendo

$$\varphi: (\mathcal{C}, \vee, \wedge, \neg, \rightarrow) \longrightarrow (\mathcal{A}, \tilde{+}, \cdot, 1+, \text{“ser múltiplo”})$$

del modo siguiente: para las variables proposicionales

$$\begin{aligned} P &\longrightarrow p \\ Q &\longrightarrow q \\ &\dots\dots\dots \\ R &\longrightarrow r \end{aligned}$$

y para cualesquiera  $A, B \in \mathcal{C}$

$$\begin{aligned} A \vee B &\longrightarrow a \tilde{+} b \\ \neg A &\longrightarrow 1 + a \end{aligned}$$

como consecuencia de las Leyes de De Morgan:  $A \wedge B \longrightarrow a \cdot b$   
y por tanto  $\varphi$  es un homomorfismo.

**5.1.1 Consecuencia.-**  $\varphi(\underline{1}) = 1, \varphi(\underline{0}) = 0$  **y  $\varphi$  conserva la ordenación.**

**Demostración:** Ínfimo y supremo:

$$\underline{0} = P \wedge \neg P \Rightarrow \varphi(\underline{0}) = \varphi(P \wedge \neg P) = \varphi(P) \cdot \varphi(\neg P) = p \cdot (1 + p) = p + p^2 = 0$$

Análogamente se prueba que  $\varphi(\underline{1}) = 1$

**Ordenación:** sean  $A$  y  $B$  dos proposiciones cualesquiera

$$\begin{aligned} A \rightarrow B &\Leftrightarrow A \wedge B \equiv A \Rightarrow \varphi(A \wedge B) = \varphi(A) \Leftrightarrow \varphi(A) \cdot \varphi(B) = \varphi(A) \Leftrightarrow \\ &\Leftrightarrow a \cdot b = a \Rightarrow a \text{ es múltiplo de } b. \end{aligned}$$

**5.1.2 Proposición.-**  $\varphi$  **está bien definida.**

**Demostración:** Es consecuencia de que se preserve la ordenación. Sean  $A$  y  $B$  dos proposiciones cualesquiera:

$$\begin{aligned} A \equiv B &\Rightarrow A \rightarrow B \text{ y } B \rightarrow A \Rightarrow \\ \Rightarrow \varphi(A) &\text{ es múltiplo de } \varphi(B) \text{ y } \varphi(B) \text{ es múltiplo de } \varphi(A) \Leftrightarrow \\ \Leftrightarrow a &\text{ es múltiplo de } b \text{ y } b \text{ es múltiplo de } a \Leftrightarrow a = b \end{aligned}$$

## 5.2 EL ISOMORFISMO DE ÁLGEBRAS DE BOOLE $\varphi$

### 5.2.1 **Proposición.-** $\varphi$ es suprayectiva.

**Demostración:** Todo elemento del anillo  $\mathcal{A}$  (son los mismos que los del álgebra de Boole  $\mathcal{A}$ ) es una combinación lineal algebraica de las variables polinomiales. Como hemos visto que:

$$\begin{aligned}\varphi(P \wedge Q) &= p \cdot q \\ \varphi((\neg P \wedge Q) \vee (P \wedge \neg Q)) &= p + q\end{aligned}\quad (3.1.2)$$

$\varphi$  es suprayectiva.

### 5.2.2 **Proposición.-** $\varphi$ es inyectiva.

**Demostración:** Supongamos  $\varphi(P) = p$  ,  $\varphi(Q) = q$  y  $p = q$  (de donde  $p|q$  y  $q|p$ ). Como  $\varphi$  preserva el orden (se corresponden  $\rightarrow$  y “ser múltiplo”):

$$q|p \Rightarrow P \rightarrow Q \quad ; \quad p|q \Rightarrow Q \rightarrow P$$

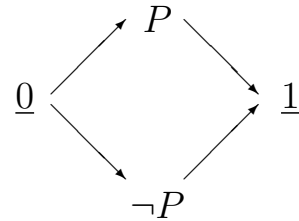
luego  $P \leftrightarrow Q$

**5.2.3 Observación.-** Para ser precisos, realmente consideramos  $\mathcal{C}/\leftrightarrow$  (álgebra de Lindenbaum).

### 5.3 EJEMPLOS

5.3.1 **Ejemplo.-** Sea  $\mathcal{C} = \{\underline{0}, P, \neg P, \underline{1}\}$ .

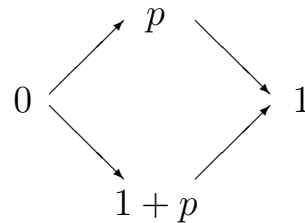
Entonces  $(\mathcal{C}, \rightarrow)$  es el cierre transitivo de:



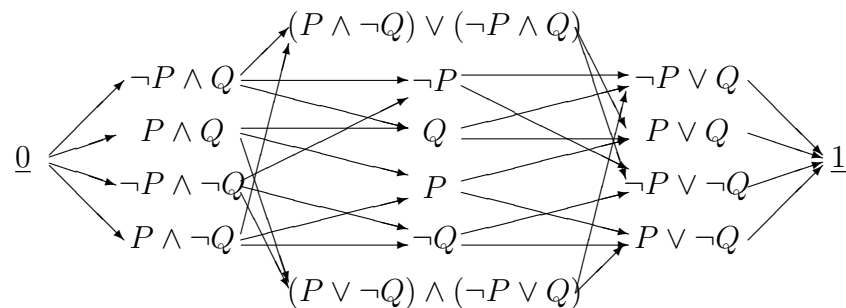
que se corresponderá en  $\varphi$  con  $(\mathcal{A}, \text{“ser múltiplo”})$ , donde

$$\mathcal{A} = (\mathbb{Z}/2\mathbb{Z})[p]/\langle p^2 - p \rangle = \{1, p, 1 + p, 0\}$$

y “ser múltiplo” es el cierre transitivo de:



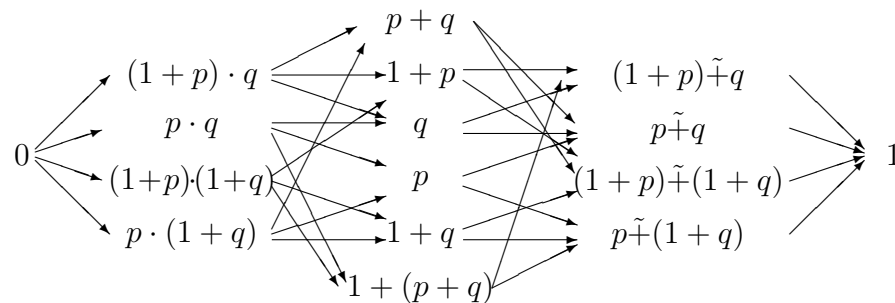
**5.3.2 Ejemplo.-** Sean las variables proposicionales de  $\mathcal{C}$ :  $P$  y  $Q$ . Entonces  $\mathcal{C}$  posee 16 elementos y  $(\mathcal{C}, \rightarrow)$  será el cierre transitivo de:



que se corresponderá en  $\varphi$  con  $(\mathcal{A}, \text{"ser múltiplo"})$ , donde

$$\mathcal{A} = (\mathbb{Z}/2\mathbb{Z})[p, q] / \langle p^2 - p, q^2 - q \rangle$$

“Ser múltiplo” vendrá dada por el cierre transitivo de:



## 5.4 ÁTOMOS Y CO-ÁTOMOS DE UN ÁLGEBRA DE BOOLE

**5.4.1 Definición.-** *Un elemento de un álgebra de Boole que sea minimal (resp. maximal) para la ordenación se dice que es un átomo (resp. co-átomo).*

**5.4.2 Consecuencia.-** *Los co-átomos de  $(\mathcal{A}, \tilde{+}, \cdot, 1+, \text{“ser múltiplo”})$  son los polinomios irreducibles.*

**Demostración:**  $d$  es co-átomo  $\Leftrightarrow d$  es maximal para “ser múltiplo”  $\Leftrightarrow$   
 $\Leftrightarrow$  el único elemento ( $\neq d$ ) del que  $d$  es múltiplo es del supremo (1)  $\Leftrightarrow$   
 $\Leftrightarrow d$  es irreducible.

**5.4.3 Observación.-** *Notemos que una variable proposicional no es irreducible. P.ej. en el caso de que haya dos variables proposicionales,  $P$  y  $Q$  (véase 5.3.2):*

*$(p\tilde{+}q)$  es irreducible*

*$(p\tilde{+}(1+q))$  es irreducible*

*$(p\tilde{+}q) \cdot (p\tilde{+}(1+q)) = p \cdot (q\tilde{+}(1+q)) = p \cdot 1 = p$ , luego  $p$  no es irreducible.*

**5.4.4 Proposición.-** *Para cualquier  $B \in (\mathcal{C}, \vee, \wedge, \neg, \rightarrow)$ :*

*$B$  es un átomo  $\Leftrightarrow \neg B$  es co-átomo.*

*Para cualquier  $b \in (\mathcal{A}, \tilde{+}, \cdot, 1+, \text{“ser múltiplo”})$*

*$b$  es un átomo  $\Leftrightarrow 1+b$  es co-átomo*

**Demostración:** Basta considerar las definiciones de átomo y co-átomo y 4.1.5.

**5.4.5 Proposición.-** *Los átomos de  $(\mathcal{A}, \text{“ser múltiplo”})$ , donde  $\mathcal{A} = (\mathbb{Z}/2\mathbb{Z})[p, q, \dots, r]/\langle p^2 - p, q^2 - q, \dots, r^2 - r \rangle$  son de la forma:*

$$m = [\delta_p \cdot p + (1 - \delta_p) \cdot (1 + p)] \cdot [\delta_q \cdot q + (1 - \delta_q) \cdot (1 + q)] \cdot \dots \cdot [\delta_r \cdot r + (1 - \delta_r) \cdot (1 + r)]$$

donde

$$\delta_i \in (\mathbb{Z}/2\mathbb{Z}) \quad (\text{e.e. : } \delta_i = 0 \quad \text{o} \quad \delta_i = 1).$$

*Por tanto, los átomos son polinomios de  $\mathcal{A}$  de grado total máximo (grado uno en cada variable, grado total el número de variables).*

**Demostración:** i) Veamos que  $m$  es un átomo.

Sea  $a \in \mathcal{A}$ ,  $m|a \Leftrightarrow \exists k \in \mathcal{A} : a = k \cdot m$ . Como  $k \in \mathcal{A}$ , se puede expresar en la forma:

$$k = \alpha_0 + \alpha_p \cdot p + \alpha_q \cdot q + \dots + \alpha_{pq} \cdot p \cdot q + \dots + \alpha_{pqr} \cdot p \cdot q \cdot r + \dots$$

luego  $a = k \cdot m$  será una suma de monomios como p.ej.:  $(\alpha_{pq} \cdot p \cdot q) \cdot m$ .

\* Si  $\alpha_{pq} = 0$ , entonces el monomio se anula.

\* Si  $\alpha_{pq} = 1$ :

– Si  $(1 + p)$  ó  $(1 + q)$  dividen a  $m$ , entonces el monomio se anula.

– En otro caso,  $p$  y  $q$  dividen a  $m$ , y el monomio queda:  $(1 \cdot p \cdot q) \cdot m = m$ .

En cualquier caso,  $a = k \cdot m$  será una suma de monomios iguales a 0 ó a  $m$ , luego:

$$a = m \quad \text{o bien} \quad a = 0$$

y por tanto  $a$  es átomo.

ii) Veamos que si  $c$  es átomo de  $(\mathcal{A}, \text{"ser múltiplo"})$  debe ser de esta forma.

Si  $c$  es átomo, y lo expresamos con las operaciones del álgebra de Boole  $(\mathcal{A}, \tilde{+}, \cdot, 1+)$ , no se debe poder escribir en la forma

$$c = h\tilde{+}g \quad ; \quad h \neq 0 \quad \text{y} \quad g \neq 0$$

pues en tal caso  $h$  y  $g$  serían múltiplos de  $c$ :  $c \cdot h = (h\tilde{+}g) \cdot h = h$  y por tanto  $c$  no sería minimal.

Por tanto, si expandimos  $c$  por distributividad de  $\cdot$  respecto de  $\tilde{+}$  y cancelamos, no pueden aparecer  $\tilde{+}$  en tales expansiones.

Luego  $c$  es de la forma

$$c = \delta_0 + [\delta_p \cdot p + \delta'_p(1 + p)] \cdot [\delta_q \cdot q + \delta'_q(1 + q)] \cdot \dots \cdot [\delta_r \cdot r + \delta'_r(1 + r)]$$

donde  $\delta_0, \delta_i, \delta'_i \in (\mathbb{Z}/2\mathbb{Z})$  y donde no todas las variables polinomiales tienen necesariamente que aparecer (e.e., puede no aparecer p.ej. el factor  $[\delta_q \cdot q + \delta'_q(1 + q)]$ ).

Analicemos las  $\delta$ :

\* si algún  $\delta$  y el correspondiente  $\delta'$ , por ejemplo  $\delta_p$  y  $\delta'_p$ , fueran iguales a 1, entonces  $[\delta_p \cdot p + \delta'_p(1 + p)] = 1$ , es decir, no aparecerían ni el factor  $p$  ni el  $(1 + p)$  en  $c$

\* si algún  $\delta$  y el correspondiente  $\delta'$ , por ejemplo  $\delta_p$  y  $\delta'_p$ , fueran iguales a 0, entonces  $[\delta_p \cdot p + \delta'_p(1 + p)] = 0$ , y quedaría  $c = \delta_0$ . Entonces:

- si  $\delta_0 = 0$ ,  $c$  no sería minimal (sería  $c = 0$ , e.e., el ínfimo)
- si  $\delta_0 = 1$ ,  $c$  no sería minimal (sería  $c = 1$ , e.e., el supremo).

Por tanto

$$c = \delta_0 + [\delta_p \cdot p + (1 - \delta_p) \cdot (1 + p)] \cdot [\delta_q \cdot q + (1 - \delta_q) \cdot (1 + q)] \cdot \dots \cdot [\delta_r \cdot r + (1 - \delta_r) \cdot (1 + r)]$$

donde  $\delta_0, \delta_i \in (\mathbb{Z}/2\mathbb{Z})$  y donde no todas las variables polinomiales tienen necesariamente que aparecer.

Como por las leyes de De Morgan,  $1 + (a \cdot b) = (1 + a) \tilde{+} (1 + b)$ , y hemos visto que  $c$  no se debe poder expresar como  $\tilde{+}$  de elementos no nulos, debe ser  $\delta_0 = 0$ .

En consecuencia:

$$c = [\delta_p \cdot p + (1 - \delta_p) \cdot (1 + p)] \cdot [\delta_q \cdot q + (1 - \delta_q) \cdot (1 + q)] \cdot \dots \cdot [\delta_r \cdot r + (1 - \delta_r) \cdot (1 + r)]$$

donde  $\delta_i \in (\mathbb{Z}/2\mathbb{Z})$  y donde no todas las variables polinomiales tienen necesariamente que aparecer.

Pero si por ejemplo ni  $r$  ni  $(1 + r)$  aparecieran,  $c \cdot r$  sería múltiplo (propio) de  $c$  y  $c$  no sería minimal. Por tanto todas las variables polinomiales tienen necesariamente que aparecer.

**5.4.6 Consecuencia.-** Si en la  $k$ -álgebra  $A$  hay  $n$  variables, en  $(A, \text{"ser múltiplo"})$  hay  $2^n$  átomos (respectivamente co-átomos).

*Lo mismo ocurrirá en  $\mathcal{C}$  si se genera a partir de  $n$  variables proposicionales.*

## **6 IDEALES Y FILTROS**

## 6.1 IDEALES DE ANILLOS

**6.1.1 Definición.-** Sea  $(\mathcal{R}, +, \cdot)$  anillo. Un subconjunto  $I \subseteq \mathcal{R}$  se dice que es un ideal de  $\mathcal{R}$  si se cumple:

$$i) \forall i, i' \in I : i + i' \in I$$

$$ii) \forall i \in I, \forall a \in \mathcal{R} : a \cdot i \in I$$

(e.e.  $I$  es subanillo de  $\mathcal{A}$  tal que el producto de un elemento del anillo por un elemento del ideal pertenece siempre al ideal).

**6.1.2 Definición.-** Sea  $(\mathcal{R}, +, \cdot)$  anillo. Sea  $S \neq \emptyset$ ,  $S \subseteq \mathcal{R}$ . Se llama ideal generado por  $S = \{p_1, \dots, p_m\}$ ,  $\langle p_1, \dots, p_m \rangle$ , al menor ideal que contiene a  $S$ .

En particular, si  $S = \{q\}$ , el ideal generado por  $q$ ,  $\langle q \rangle$ , se dice que es un ideal principal y resulta ser:

$$\langle q \rangle = \{a \in \mathcal{A} : q|a\}$$

## 6.2 IDEALES (Y FILTROS) DE ÁLGEBRAS DE BOOLE

**6.2.1 Definición.-** En  $(\mathcal{C}, \vee, \wedge, \neg, \rightarrow)$  (álgebra de Boole) se define el ideal (principal) generado por  $Q$  como

$$E_Q = \{ X \in \mathcal{C} : X \rightarrow Q \}$$

y el filtro (principal) generado por  $P$  como

$$E^P = \{ X \in \mathcal{C} : P \rightarrow X \}$$

**6.2.2 Observación.-** Los ideales y filtros (principales) del álgebra de Boole  $(A, \tilde{+}, \cdot, 1+, \text{"ser múltiplo"})$  se definen de modo análogo. Por ejemplo, el ideal principal generado por  $q \in A$  será:

$$\{a \in A : a \text{ es múltiplo de } q\}$$

**6.2.3 Proposición.-** Como  $\varphi$  preserva el orden, los ideales y filtros del álgebra de Boole  $(\mathcal{C}, \vee, \wedge, \neg, \rightarrow)$  se corresponden por  $\varphi$  con los ideales y filtros del álgebra de Boole  $(A, \tilde{+}, \cdot, 1+, \text{"ser múltiplo"})$ .

### 6.3 IDEALES DEL ANILLO $\mathcal{A}$ Y DEL ÁLGEBRAS DE BOOLE $\mathcal{A}$

**6.3.1 Proposición.-** *Es obvio que los ideales del álgebra de Boole  $(\mathcal{A}, \tilde{+}, \cdot, \text{"ser múltiplo"})$  son ideales del anillo  $(\mathcal{A}, +, \cdot, \text{"ser múltiplo"})$ .*

**6.3.2 Teorema.-**  *$(\mathcal{A}, +, \cdot)$  es un anillo en que todo ideal es principal.*

**Demostración:** Sean  $s_1, s_2, \dots, s_n \in \mathcal{A}$ . Entonces:  $\langle s_1, s_2, \dots, s_n \rangle = \langle s_1 \tilde{+} s_2 \tilde{+} \dots \tilde{+} s_n \rangle$

En efecto:

i)  $\tilde{+}$  es operación interna en el ideal (por serlo  $+$  y  $\cdot$ ) luego:

$$s_1 \tilde{+} s_2 \tilde{+} \dots \tilde{+} s_n \in \langle s_1, s_2, \dots, s_n \rangle \Rightarrow \langle s_1 \tilde{+} s_2 \tilde{+} \dots \tilde{+} s_n \rangle \subseteq \langle s_1, s_2, \dots, s_n \rangle$$

ii) Por 4.1.7 i):  $s_1 \tilde{+} s_2 \tilde{+} \dots \tilde{+} s_n | s_i ; i = 1, \dots, n \Rightarrow s_i \in \langle s_1 \tilde{+} s_2 \tilde{+} \dots \tilde{+} s_n \rangle ; i = 1, \dots, n \Rightarrow$   
 $\Rightarrow$  el mínimo ideal que contiene a  $\{s_1, s_2, \dots, s_n\} = \langle s_1, s_2, \dots, s_n \rangle \subseteq \langle s_1 \tilde{+} s_2 \tilde{+} \dots \tilde{+} s_n \rangle$

**6.3.3 Observación.-** *De modo similar se prueba que el filtro del álgebra de Boole  $(\mathcal{A}, \tilde{+}, \cdot, \text{"ser múltiplo"})$  generado por  $\{s_1, s_2, \dots, s_n\}$  es también generado por  $s_1 \cdot s_2 \cdot \dots \cdot s_n$*

**6.3.4 Proposición.-** *Los ideales del álgebra de Boole  $(\mathcal{A}, \tilde{+}, \cdot, \text{"ser múltiplo"})$  coinciden con los ideales del anillo  $(\mathcal{A}, +, \cdot, \text{"ser múltiplo"})$ .*

**Demostración:** i) 6.3.1

ii) Los ideales del anillo  $(\mathcal{A}, +, \cdot)$  son ideales del álgebra de Boole  $(\mathcal{A}, \tilde{+}, \cdot, \text{"ser múltiplo"})$ :

En efecto: por 6.3.2, los ideales del anillo son principales, luego los múltiplos del generador deben estar en el ideal, y es obvio que el conjunto de múltiplos constituye un ideal del anillo.

## 6.4 MÁS RESULTADOS SOBRE IDEALES Y FILTROS

**6.4.1 Proposición.-** *Si el ideal de  $\mathcal{A}$  generado por  $p$  corta al filtro generado por su complementario,  $1 + p$ , entonces ambos son todo el anillo, e.e.:*

$$E_p \cap E^{(1+p)} \neq \emptyset \Leftrightarrow E_p = E^{(1+p)} = \mathcal{A}$$

**Demostración:**  $\Leftarrow$ ) Es evidente.

$$\Rightarrow) E_p \cap E^{(1+p)} \neq \emptyset \Rightarrow \exists a \in E_p \cap E^{1+p}$$

y para ese  $a$ , debe verificarse (por definición de ideal y de filtro):

$$p|a \text{ y } a|(1+p) \Rightarrow p|(1+p) \Rightarrow (1+p) \in \langle p \rangle \Rightarrow 1 \in \langle p \rangle \Rightarrow \langle p \rangle = \mathcal{A}$$

$$\text{Para el filtro: } 1 \in \langle p \rangle \Rightarrow p|1 \Rightarrow (1+1)|(1+p) \Rightarrow 0|(1+p) \Rightarrow 0 = (1+p) \Rightarrow E^{1+p} = \mathcal{A}$$

**6.4.2 Teorema.-** *Todo elemento de  $\mathcal{A}$  (distinto de la unidad) es expresable de modo único como producto de irreducibles.*

**Demostración:** i) Todo elemento es producto de co-átomos (irreducibles).

**En efecto:** sea  $a \in \mathcal{A}$ . Como todos son múltiplos de 1, pueden ocurrir dos cosas:

- $b$  es irreducible (y hemos terminado)
- $b$  no es irreducible. Como el anillo es finito, tiene que existir un irreducible  $k$  tal que  $1|k|b$ . Por tanto  $\exists b' : b = k \cdot b'$ . Reiterando el proceso para  $b'$  obtendremos la descomposición de  $b$  como producto de irreducibles (como  $b' \cdot b = b \Leftrightarrow b' \leq b$  y  $b' \neq b$ , y el anillo es finito, el proceso tiene fin).

ii) La expresión de un elemento como producto de irreducibles es única.

Sea  $a$  un elemento cualquiera de  $\mathcal{A}$ . Consideremos el filtro  $E^a$ . Entonces  $a$  es el producto de los co-átomos (irreducibles) de  $E^a$ ,  $\pi_1, \pi_2, \dots, \pi_j$ , y esa es la única forma de expresarlo como producto de elementos irreducibles.

**En efecto:** por 4.1.7 ii

$$\pi_i | a \quad ; \quad i = 1, 2, \dots, j \quad \Rightarrow \quad \pi_1 \cdot \pi_2 \cdot \dots \cdot \pi_j | a$$

Otros irreducibles no pueden dividir a  $a$ , pues pertenecerían a  $E^a$ .

Si algún  $\pi_i$  apareciera más de una vez, simplificaría por idempotencia.

**Por tanto:**  $\pi_1 \cdot \pi_2 \cdot \dots \cdot \pi_j = a$

**6.4.3 Observación.-**  $(\mathcal{A}, +, \cdot)$  *no es un Dominio de Factorización Única pues en 2.2.1 se vio que todo elemento es divisor de cero, luego  $\mathcal{A}$  no es dominio. De hecho la factorización en general no es única:*

$$p \cdot q = p \cdot (p \cdot q) \quad y : \quad q \neq p \cdot q$$

**6.4.4 Proposición.-** *El anillo de clases residuales  $\mathcal{A}$  es finito y por tanto es un anillo noetheriano y artiniano.*

## **7 IMPLEMENTACIÓN EN *CoCoA***

## 7.1 SOBRE *CoCoA*

- *CoCoA* es un lenguaje de Algebra Computacional especializado en cálculos de GB y NF módulo un ideal en anillos de polinomios sobre cuerpos finitos.
- No se puede fijar en *CoCoA* que el anillo sea de clases residuales.
- Lo que haremos es reducir módulo el ideal todo los cálculos (lo que viene a ser lo mismo).
- La tautología y la contradicción se representarán respectivamente como  $T$  ( $T = 1$ ) y  $C$  ( $C = 0$ ).

## 7.2 CÓDIGO EN *WinCoCoA v.4.2*

- Supongamos que las variables proposicionales son  $P_1, P_2, \dots, P_{10}$  y las variables polinomiales correspondientes  $p_1, p_2, \dots, p_{10}$ .
- Consideramos entonces el anillo polinomial:

$$(\mathbb{Z}/2\mathbb{Z})[p_1, p_2, \dots, p_{10}]$$

y reducimos todos los cálculos módulo el ideal:

$$I = \langle p_1^2 - p_1, p_2^2 - p_2, \dots, p_{10}^2 - p_{10} \rangle$$

**Código:**

```
A := Z/(2) [ p[1..10] ] ;
USE A;
MEMORY.I := Ideal (p[1]^2-p[1], p[2]^2-p[2], p[3]^2-p[3], p[4]^2-p[4], p[5]^2-p[5],
                  p[6]^2-p[6], p[7]^2-p[7], p[8]^2-p[8], p[9]^2-p[9], p[10]^2-p[10]);
T:=1;
C:=0;
NEG(M) := NF(1+M, MEMORY.I);
O(M,N) := NF(M+N+M*N, MEMORY.I);
Y(M,N) := NF(M*N, MEMORY.I);
IMP(M,N) := NF(1+M+M*N, MEMORY.I);
```

### 7.3 EJEMPLOS DE USO DE LA IMPLEMENTACIÓN EN WinCoCoA

-- Ejemplo: distributividad

```
0(p[1],Y(p[2],p[3])) - Y(0(p[1],p[2]),0(p[1],p[3]));  
0
```

-- Ejemplo: Ley de De Morgan:

```
NEG(0(p[1],p[2])) - Y(NEG(p[1]),NEG(p[2]));  
0
```

**En los dos casos la respuesta es 0, con lo que queda probada la distributividad de  $\vee$  respecto de  $\wedge$  y una de las leyes de De Morgan.**

## **8 CONCLUSIONES**

- Esta aproximación tiene la ventaja sobre la de Kapur-Narendran [11] o Hsiang [10] de proporcionar una estructura de algebra de Boole (polinomial) isomorfa al algebra proposicional [13], en lugar de sólo una forma de realizar cálculos efectivos.
- Ello es la clave para dar un paso más y obtener un modelo para Sistemas Expertos (S.E.) basados en reglas sobre una lógica booleana, pasando de

$$\mathcal{A} = (\mathbb{Z}/2\mathbb{Z})[x, y, \dots, z] / \langle x^2 - x, y^2 - y, \dots, z^2 - z \rangle$$

a

$$\mathcal{A}/J$$

donde  $J$  es el ideal generado por la negación de los hechos establecidos como ciertos (de entre los hechos potenciales), reglas y restricciones de integridad.

- De este modo, **se pueden estudiar extracción de conocimiento y verificación de S.E.**
- Todo ello se puede generalizar a lógicas modales multivalentes (extendiendo los trabajos de Alonso et al. [3] y Chazarain et al. [5]), también con la ventaja de proporcionar un anillo de clases residuales isomorfo y poder pasar a tratar S.E. basados en reglas sobre lógicas modales multivalentes [17, 14].

- **También** se pueden desarrollar aproximaciones algebraicas similares (basadas en el uso de bases de Gröbner), para la toma de decisiones en ciertos problemas de ingeniería del transporte, como:
  - **enclavamientos ferroviarios** independientes de la topología de la estación (un enclavamiento evita que se pueda autorizar una disposición de colores de semáforos y posiciones de agujas de los desvíos que pueda llevar a una colisión) [18],



Figura 1: Estación de Moreda, dirección norte (Linares).



Figura 2: Estación de Moreda, dirección sur (Granada / Almería).

- sistemas de supervisión de la labor del controlador de rodadura en una terminal aeroportuaria (**A-SMGCS**: Advanced Surface Movement Guide and Control System) [19].

## Referencias

- [1] W.W. Adams, P. Lounstaunau: *An Introduction to Gröbner Bases*. Graduate Studies in Mathematics 3, AMS, 1994.
- [2] A.G. Akritas: *Elements of Computer Algebra with Applications*. Wiley - Interscience, 1989.
- [3] J.A. Alonso, E. Briales: **Lógicas Polivalentes y Bases de Gröbner**, en: M. Vide ed. *Procs. of the V Congress on Natural Languages and Formal Languages*, Barcelona U. Press, 1989, 307-315.
- [4] A. Capani, G. Niesi: *CoCoA User's Manual (v. 3.0b)*. (Depto. de Matemáticas, Universidad de Genova, Genova, 1996).
- [5] J. Chazarain, A. Riscos, J.A. Alonso, E. Briales: **Many-valued Logic and Gröbner Bases with Applications to Modal Logic**. *Journal of Symbolic Computation*, 11, 181-194, 1991.
- [6] D. Cox, J. Little, D. O'Shea: *Ideals, varieties, and algorithms*. Springer-Verlag, 1992.
- [7] P.R. Halmos: *Lectures on Boolean Algebras*. Springer-Verlag, 1974.
- [8] P. Halmos, S. Givant: *Logic as Algebra*. The Mathematical Association of America, 1998.
- [9] H. Hermes: *La teoría de retículos y su aplicación a la lógica matemática*. Conf. Mat. VI. CSIC-Madrid, 1963.
- [10] J. Hsiang: **Refutational Theorem Proving using Term-rewriting Systems**. *Artificial Intelligence*, 25 (1985), 255-300.
- [11] D. Kapur, P. Narendran: **An Equational Approach to Theorem Proving in First-Order Predicate Calculus**, 84CRD296, *General Electric Corporate Research and Development Report* (Schenectady, NY, March 1984, rev Dec 1984). También en: *Proceedings of IJCAI-85*, (1985) 1146-1153.
- [12] M. Kreuzer, L. Robbiano: *Computational Commutative Algebra*. Springer-Verlag, 2000.
- [13] L.M. Laita, L. de Ledesma, E. Roanes Lozano, E. Roanes Macías: **An interpretation of the propositional Boolean algebra as a k-algebra: effective calculus**. En: J. Calmet, J.A. Campbell (editores): *Integrating Symbolic Mathematical Computation and Artificial Intelligence; Selected Papers AISMC-2*). Springer-Verlag LNCS 958, 1995, págs. 255-263.

- [14] L.M. Laita, E. Roanes-Lozano, L. de Ledesma, J.A. Alonso: **A Computer Approach to Verification and Deduction in Many-valued Knowledge Systems.** *Soft Computing*, 3 (1), 7-19, 1999.
- [15] E. Mendelson: *Theory and Problems of Boolean Algebras and Switching Circuits.* Schaum's / MacGraw-Hill, 1970.
- [16] D. Monk: *Handbook of Boolean Algebras.* North-Holland, 1989.
- [17] E. Roanes-Lozano, L.M. Laita, E. Roanes-Macías: **A Polynomial Model for Many-valued Logics with a Touch of Algebraic Geometry and Computer Algebra.** *Mathematics and Computers in Simulation*, 45 (1), 83-99, 1998.
- [18] E. Roanes Lozano, E. Roanes Macías, L.M. Laita: **Railway Interlocking Systems and Groebner Bases.** *Mathematics and Computers in Simulation*, 51/5, 473–481, 2000.
- [19] E. Roanes Lozano, R. Muga, L.M. Laita, E. Roanes Macías: **A terminal area topology-independent GB-based conflict detection system for A-SMGCS.** *RACSAM (Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales, Serie A, Matemáticas)*, 98 (1-2), 229–237, 2005.
- [20] L. Robbiano et al.: *CoCoA 4.2 Online Help* (electronic file accompanying CoCoA v.4.2). 2002.
- [21] M. Stone: **The Theory of Representations for Boolean Algebras.** *Transactions AMS*, 40, 37-111, 1940.
- [22] R. Turner: *Logics for Artificial Intelligence.* Ellis Horwood, 1984.
- [23] F. Winkler: *Polynomial Algorithms in Computer Algebra.* Springer-Verlag, 1996.