

R 11189

043

105629

71



**MÉTODOS ALGEBRAICOS**

**DE RAZONAMIENTO AUTOMÁTICO**

UNIVERSIDAD DE SEVILLA  
SECRETARÍA GENERAL

Queda registrada esta Tesis Doctoral  
al folio.....2..... número.....26.....del libro  
correspondiente.  
Sevilla, - 1 JUN. 1988

El Jefe del Negociado de Tesis,

*E. Laffitte*

Memoria presentada por José  
Antonio Alonso Jiménez para  
optar al grado de Doctor en  
Matemáticas por la Universidad  
de Sevilla.

UNIVERSIDAD DE SEVILLA

Depositado en Departamento de Álgebra, Computación, Geometría y Topología  
de la Facultad de Matemáticas  
de esta Universidad desde el día 4 de Junio de 1988  
hasta el día 21 de Junio de 1988

Sevilla, Mayo 1988

Sevilla 27 de Junio de 1988

EL DIRECTOR DEL Departamento

*José L. Vicente*

Director de la Memoria:

Prof. D. Agustín Riscos Fernández



*Agustín Riscos*

VºBº del Director del Departamento

*José L. Vicente*

José Luis Vicente Córdoba

DEPARTAMENTO DE ALGEBRA, COMPUTACIÓN, GEOMETRÍA Y TOPOLOGÍA

Autorizo la cédula  
del presente trabajo

*Agustín Riscos*

Expreso mi agradecimiento a todos los que han hecho posible el presente trabajo. En particular, a los Prof. Luis Laita de la Rica, Alejandro Fernández Margarit y Agustín Riscos Fernández que me pusieron en contacto con la Lógica Matemática; a la Pfra. Delia Balbontín Noval, que me puso en contacto con la Inteligencia Artificial; al Prof. Francisco Castro Jiménez, que me puso en contacto con el Algebra Computacional, y al Prof. Emilio Briales Morales que me ayudó en la implantación de los algoritmos. Finalmente, agradezco al Prof. Agustín Riscos Fernández, director del presente trabajo, por haberme decidido a empezarlo, ayudado a desarrollarlo y animado a terminarlo.

# ÍNDICE

<b>INTRODUCCIÓN.....</b>	<b>I</b>
<b>1.-RELACIONES CANÓNICAS.....</b>	<b>1</b>
<b>2.- ALGORITMOS DE BASES DE GRÖBNER EN <math>Z_p[X_1, \dots, X_n]</math></b>	
2.1.- Notaciones y definiciones.....	16
2.2.- Relación de reducción definida por un conjunto de polinomios.....	20
2.3.- Reducciones e ideales.....	25
2.4.- Base de Gröbner.....	28
2.5.- Bases de Gröbner y pertenencia a un ideal.....	31
2.6.- Pares críticos.....	34
2.7.- Caracterización de bases de Gröbner mediante pares críticos.....	35
2.8.- Algoritmo de cálculo de bases de Gröbner.....	38
2.9.- Mejoras del algoritmo.....	44
2.10.- Bases de Gröbner reducidas.....	50
<b>3.- CÁLCULOS PROPOSICIONALES</b>	
<b><u>3.1.- CÁLCULO PROPOSICIONAL CLÁSICO</u></b>	
3.1.A.- Definiciones.....	53
3.1.B.- Polinomios asociados a proposiciones.....	55
3.1.C.- Caracterización algebraica de las tautologías.....	57
3.1.D.- Caracterización algebraica de la deducción.....	62
3.1.E.- Algoritmos de deducción.....	69
<b><u>3.2.- CÁLCULOS PROPOSICIONALES POLIVALENTES</u></b>	
3.2.A.- Definiciones.....	78
3.2.B.- Polinomios asociados a proposiciones.....	82
3.2.C.- Caracterización algebraica de las tautologías.....	85
3.2.D.- Caracterización algebraica de la deducción.....	91

## **4.- LÓGICA MONÁDICA**

<b>4.1.- Definiciones.....</b>	<b>95</b>
<b>4.2.- Polinomios asociados a proposiciones.....</b>	<b>100</b>
<b>4.3.- Caracterización algebraica de la validez.....</b>	<b>103</b>
<b>4.4.- Caracterización algebraica de la deducción.....</b>	<b>114</b>
<b>APÉNDICE: PROGRAMAS Y SESIONES.....</b>	<b>117</b>
<b>BIBLIOGRAFÍA.....</b>	<b>128</b>

## INTRODUCCIÓN

El objetivo del presente trabajo es la resolución mediante algoritmos algebraicos de problemas del cálculo proposicional clásico, de los cálculos proposicionales polivalentes y de la lógica monádica. En otras palabras, el objetivo es una aplicación del álgebra computacional al razonamiento automático.

El álgebra computacional es la parte de la ciencia de la computación que se ocupa del diseño, análisis, implantación y aplicación de algoritmos algebraicos (LOOS[83] p.1)

En CAVINESS[85] se da como fecha de nacimiento del álgebra computacional el año 1966 por haberse celebrado en dicho año las dos primeras conferencias sobre el tema (SYMSAM 1966 e IFIP 1966).

Dentro del álgebra computacional nuestro interés se centra en los problemas algorítmicos de la teoría de polinomios. El método de las bases de Gröbner soluciona el problema de simplificación de ideales de polinomios y, como consecuencia, soluciona fácilmente muchos otros problemas, en particular, el de pertenencia a un ideal que es el que nos interesa.

El método de las bases de Gröbner fue introducido por BUCHBERGER, implícitamente en 1965 y explícitamente en 1976. La idea básica del método consiste en dado un conjunto finito  $F$  de polinomios transformarlo en una forma canónica

G, llamada base de Gröbner, que engendra el mismo ideal que F y tal que todo polinomio de dicho ideal se reduce a 0 módulo G y todo polinomio del anillo tiene una única forma irreducible respecto de G.

En 1967, KNUTH y BENDIX, usando las dos ideas básicas del método de las bases de Gröbner (i.e. pares críticos y completación) dieron un algoritmo para resolver el problema de las palabras en álgebras universales.

El razonamiento automático es la parte de la ciencia de la computación cuyo objeto es el descubrimiento, formulación e implantación de conceptos y procedimientos que permitan usar los ordenadores como una ayuda para el razonamiento. Uno de sus principales objetivos es el diseño y la implantación de programas (frecuentemente llamados demostradores de teoremas) que automaticen el razonamiento (WOS[85], página 85).

El primer programa de demostración automática de teorema apareció en 1957 y fue realizado por NEWELL, SHAW y SIMON.

En 1965, ROBINSON introdujo el método de resolución para la demostración automática de teoremas. Una parte importante del trabajo realizado desde entonces en este campo ha sido la elaboración de refinamientos, estrategias y extensiones del método de resolución.

Una exposición completa del método de resolución y sus variantes puede encontrarse en CHANG & LEE[83], LOVELAND[78]

y SIEKMANN & WRICHTSON[83]. El último también contiene una historia del desarrollo del razonamiento automático.

En 1983, HSIANG y DERSHOWITZ, basándose en el algoritmo de Knuth y Bendix, propusieron un método alternativo al de resolución de Robinson. La clave de dicho método fue el descubrimiento de un conjunto canónico de reglas para las álgebras de Boole. En KAPUR & NARENDRAN[85], HSIANG[85] y CHAZARAIN[86] aparecen variantes de dicho método.

Nuestro trabajo es una continuación de los anteriormente citados. Usando las bases de Gröbner en lugar del algoritmo de Knuth y Bendix, damos nuevos métodos de razonamiento automático.

A continuación exponemos los problemas que resolvemos en este trabajo.

En la primera parte del Capítulo 3, estudiamos algoritmos algebraicos para resolver problemas del cálculo proposicional clásico

El cálculo proposicional clásico consta de un lenguaje (formado por las variables  $X_1, \dots, X_n$  y las conectivas  $\neg$  (negación),  $\&$  (conjunción),  $\vee$  (disyunción),  $\rightarrow$  (implicación) y  $\leftrightarrow$  (equivalencia)); un conjunto de proposiciones  $P(X_1, \dots, X_n)$ ; un conjunto de valores de verdad,  $Z_2$ ; y una tabla de verdad  $H_k$  para cada conectiva  $k$ . Una valoración de verdad es una aplicación  $v$  de  $\{X_1, \dots, X_n\}$  en  $Z_2$ . Cada valoración  $v$  se

extiende a una aplicación  $V$  de  $P(X_1, \dots, X_n)$  en  $Z_2$  definida por

$$V(P) = \begin{cases} v(X_i), & \text{si } P \text{ es } X_i \\ H_{\neg}(V(Q)), & \text{si } P \text{ es } \neg Q \\ H_k(V(Q), V(R)), & \text{si } P \text{ es } QkR \end{cases}$$

Los problemas del cálculo proposicional clásico que estudiamos son los siguientes:

**Problema CPC1:** Dada una proposición  $P$ , determinar si  $P$  es una tautología (i.e. si para toda valoración  $v$ ,  $V(P) = 1$ )

**Problema CPC2:** Dada una proposición  $P$ , determinar si  $P$  es una contradicción (i.e. si para toda valoración  $v$ ,  $V(P) = 0$ )

**Problema CPC3:** Dada una proposición  $P$ , determinar si  $P$  es contingente (i.e. si  $P$  no es ni tautología ni contradicción) y, en caso afirmativo hallar un modelo y un contra-modelo de  $P$  (i.e. dos valoraciones  $v$  y  $v'$  tales que  $V(P) = 1$  y  $V'(P) = 0$ ).

**Problema CPC4:** Dadas las proposiciones  $P_1, \dots, P_m, Q$  determinar si  $Q$  es consecuencia tautológica de  $P_1, \dots, P_m$  (i.e. si para toda valoración  $v$  tal que  $V(P_1) = \dots = V(P_m) = 1$ ,  $V(Q) = 1$ ).

**Problema CPC5:** Dado un conjunto finito de proposiciones  $AX = \{P_1, \dots, P_m\}$ , determinar si  $AX$  es consistente (i.e. si existe una valoración  $v$  tal que  $V(P_1) = \dots = V(P_m) = 1$ ).

**Problema CPC6:** Dados dos conjuntos finitos de axiomas  $AX$  y  $AX'$ , determinar si  $AX$  y  $AX'$  son equivalentes (i.e. si



todo elemento de AX es consecuencia tautológica de AX' y todo elemento de AX' es consecuencia tautológica de AX).

El Problema CPC1 lo resolvemos mediante el Teorema 3.1.C.7 (*P es una tautología sii  $ST(P) \dashrightarrow_{F^*} 1$* ) donde ST es la aplicación de  $P(X_1, \dots, X_n)$  en el anillo de polinomios  $Z_2[X_1, \dots, X_n]$  definida por

$$ST(P) = \begin{cases} X_i, & \text{si } P \text{ es } X_i \\ ST(Q) + 1, & \text{si } P \text{ es } \neg Q \\ ST(Q) \cdot ST(R), & \text{si } P \text{ es } Q \ \& \ R \\ ST(Q) + ST(R) + ST(Q) \cdot ST(R), & \text{si } P \text{ es } Q \ \vee \ R \\ ST(Q) \cdot ST(R) + ST(Q) + 1, & \text{si } P \text{ es } Q \rightarrow R \\ ST(Q) + ST(R) + 1, & \text{si } P \text{ es } Q \leftrightarrow R \end{cases}$$

$F = \{X_i^2 + X_i : 1 \leq i \leq n\}$  y  $\dashrightarrow_{F^*}$  es la clausura reflexiva-transitiva de la relación  $\dashrightarrow_F$  definida en  $Z_2[X_1, \dots, X_n]$  por  $q \dashrightarrow_F q'$  sii  $q \neq q'$  y existe un  $p \in F$  y un monomio  $a$  tal que  $q'$  es el polinomio obtenido sustituyendo en  $q$  el monomio  $aL(p)$  (donde  $L(p)$  el mayor monomio de  $p$  respecto del orden diagonal) por  $aR(p)$  (donde  $R(p) = p - L(p)$ ).

El Problema CPC2 lo resolvemos mediante el Corolario 3.1.C.8 (*P es una contradicción sii  $ST(P) \dashrightarrow_{F^*} 0$* ).

El Problema CPC3 lo resolvemos mediante el Corolario 3.1.C.11 (*P es contingente sii  $ST(P) \dashrightarrow_{F^*} 1$  y  $ST(P) \dashrightarrow_{F^*} 0$* ) y la Nota 3.1.C.12 (Si  $X_1^{\alpha_1} \dots X_n^{\alpha_n}$  es el menor monomio de  $ST(P)$ , la valoración  $v$  definida por  $v(X_i) = \alpha_i$  es un modelo

de  $P$ . Si  $X_1^{\beta_1} \dots X_n^{\beta_n}$  es el menor monomio de  $ST(P) + 1$ , la valoración  $v$  definida por  $v(X_i) = \beta_i$  es un contramodelo de  $P$ ).

El Problema CPC4 lo reducimos a otro de ideales de polinomios mediante el Teorema 3.1.D.4 (*Q es una consecuencia tautológica de  $P_1, \dots, P_m$  sii  $ST(Q) + 1$  pertenece al ideal de  $Z_2[X_1, \dots, X_n]$  engendrado por  $F = \{ST(P_1) + 1, \dots, ST(P_m) + 1, X_1^2 + X_1, \dots, X_n^2 + X_n\}$ ). Dicho problema se resuelve fácilmente si  $F$  es una base de Gröbner usando el Corolario 2.5.4 (Sea  $F$  una base de Gröbner. Un polinomio  $q$  pertenece al ideal engendrado por  $F$  sii  $q \rightarrow_F^* 0$ ). Si  $F$  no es una base de Gröbner, podemos reducir el problema al caso anterior construyendo, mediante el Algoritmo 2.8.8, una base de Gröbner  $G$  que genere el mismo ideal que  $F$ . El algoritmo 2.8.8 se basa en el Teorema 2.7.2 ( $F$  es una base de Gröbner sii para todo  $p_1, p_2 \in F$ ,*

$$SP(PC(p_1, p_2)) = \text{mcm}(L(p_1), L(p_2))R(p_1)/L(p_1) - \text{mcm}(L(p_1), L(p_2))R(p_2)/L(p_2) \rightarrow_F^* 0$$

Otros algoritmos de construcción de bases de Gröbner que usan criterios de reducción de pares innecesarios son el 2.9.3 y el 2.9.8 que se basan respectivamente en los Teoremas 2.9.2 ( $F$  es una base de Gröbner sii para todo  $p_1, p_2 \in F$  cuyos líderes son primos entre sí,  $SP(PC(p_1, p_2)) \rightarrow_F^* 0$ ) y 2.9.7 (Sea  $A \subseteq Z_2[X_1, \dots, X_n]$ .  $F$  es una base de Gröbner sii para todo  $p_1, p_2 \in F$  tales que  $PC(p_1, p_2)$  no es AF-eliminable,  $SP(PC(p_1, p_2)) \rightarrow_F^* 0$ ).

Una de las ventajas del método anterior usando bases de Gröbner respecto del método de resolución de Robinson es la

"compilación" de axiomas (es decir, dado un conjunto de proposiciones  $AX = \{P_1, \dots, P_m\}$  para determinar si las proposiciones  $Q_1, Q_2, \dots$  se deducen de  $AX$  basta calcular una base de Gröbner  $G$  que genere el mismo ideal que  $F = \{ST(P_1) + 1, \dots, ST(P_m) + 1, X_1^2 + X_1, \dots, X_n^2 + X_n\}$  y comprobar si  $ST(Q_i) + 1 \xrightarrow{G^*} 0$ ; en cambio, con el método de resolución hay que transformar  $AX$  en un conjunto equivalente de cláusulas,  $A$ ; transformar  $\neg Q_i$  en otro conjunto equivalente de cláusulas,  $B_i$ , y comprobar por resolución que el conjunto  $A \cup B_i$  es inconsistente. Cada una de estas comprobaciones es de la misma complejidad que el cálculo de la base de Gröbner  $G$ ).

En la demostración del Teorema 3.1.D.4 nos hemos basado en el Teorema 3.1.D.3 (*La aplicación  $ST'$  del anillo booleano  $B(X_1, \dots, X_n)$  en el cociente de  $Z_2[X_1, \dots, X_n]$  respecto del ideal  $I$  engendrado por  $\{X_i^2 + X_i : 1 \leq i \leq n\}$  definida por  $ST'([P]) = ST(P) + I$  es un isomorfismo de anillos*)

El Problema CPC5 lo resolvemos mediante el Corolario 3.1.D.5 ( *$\{P_1, \dots, P_m\}$  es inconsistente sii 1 pertenece al ideal de  $Z_2[X_1, \dots, X_n]$  generado por  $F = \{ST(P_1) + 1, \dots, ST(P_m) + 1, X_1^2 + X_1, \dots, X_n^2 + X_n\}$ ). Es importante notar que no basta usar los polinomios  $X_i^2 + X_i$  para reducir, sino que es necesario usarlos también para formar pares críticos como demostramos en la Nota 3.1.E.7.*

El Problema CPC6 lo resolvemos mediante el algoritmo 3.1.E.8 que se basa en el Teorema 2.10.2 (*Si  $F$  y  $F'$  son*

bases de Gröbner reducidas y engendran el mismo ideal, entonces son iguales).

En la segunda parte del Capítulo 3, estudiamos algoritmos algebraicos para resolver problemas del cálculo proposicional polivalente.

El cálculo proposicional polivalente consta de un lenguaje (formado por un conjunto de variables,  $\text{VAR} = \{X_1, \dots, X_n\}$ , un conjunto de conectivas,  $\text{CON}$ , y una función de aridad,  $\text{ar} : \text{CON} \rightarrow \mathbb{N}$ ); un conjunto de proposiciones,  $P(\text{VAR}, \text{CON})$ ; un conjunto de valores de verdad,  $Z_r$ ; y una tabla de verdad,  $H_k : Z_r^{\text{ar}(k)} \rightarrow Z_r$ , para cada conectiva  $k$ . Una valoración de verdad es una aplicación  $v$  de  $\{X_1, \dots, X_n\}$  en  $Z_r$ . Cada  $v$  se extiende a una aplicación  $V$  de  $P(\text{VAR}, \text{CON})$  en  $Z_r$  definida por

$$V(P) = \begin{cases} v(X_i), & \text{si } P \text{ es } X_i \\ H_k(V(P_1), \dots, V(P_{\text{ar}(k)})), & \text{si } P \text{ es } k(P_1, \dots, P_{\text{ar}(k)}) \end{cases}$$

En los cálculos proposicionales polivalentes nos planteamos los mismos problemas que en el clásico y designamos por CPPi el problema correspondiente a CPCi. Por el Teorema 3.2.A.3 (Sea  $P$  un cálculo proposicional  $r$ -valente,  $p$  un entero mayor que  $r$  y  $P'$  el cálculo proposicional  $p$ -valente tal que la tabla de verdad de cada conectiva  $k$  está definida por  $H'_k(u_1, \dots, u_{\text{ar}(k)}) = H_k(u'_1, \dots, u'_{\text{ar}(k)})$  donde  $H_k$  es la tabla de verdad de  $k$  en  $P$  y  $u'_i = \min(u_i, r-1)$ . Entonces los conjuntos de tautologías de  $P$  y  $P'$  son iguales), podemos limi-

tarnos sin pérdida de generalidad a los cálculos con un número primo,  $p$ , de valores de verdad.

El Problema CPP1 lo resolvemos mediante el Teorema 3.2.C.6 (*P es una tautología sii  $ST(P) \dashrightarrow_{F^*} 0$* ) donde  $F = \{X_i^p - X_i : 1 \leq i \leq n\}$  y  $ST$  es la aplicación de  $P(\text{VAR}, \text{CON})$  en  $Z_p[X_1, \dots, X_n]$  definida por

$$ST(P) = \begin{cases} X_i, & \text{si } P \text{ es } X_i \\ ST_k(ST(P_1), \dots, ST(P_{ar(k)})), & \text{si } P \text{ es } k(P_1, \dots, P_{ar(k)}) \end{cases}$$

donde, para cada conectiva  $k$ ,  $ST_k$  es la aplicación de  $Z_p[X_1, \dots, X_n]^{ar(k)}$  en  $Z_p[X_1, \dots, X_n]$  definida por

$$ST_k(q_1, \dots, q_r) = \sum_{\substack{0 \leq i_1 \leq p-1 \\ \dots \\ 0 \leq i_r \leq p-1}} H_k(i_1, \dots, i_r) \prod_{m=1}^r \prod_{\substack{j=0 \\ j \neq i_m}}^{p-1} (q_m - j) / (i_m - j),$$

siendo  $r = ar(k)$ .

Los problemas CPP2, CPP4 y CPP5 los resolvemos mediante el Corolario 3.12.C.9, el Teorema 3.2.D.3 y el Corolario 3.2.D.4, respectivamente.

En el capítulo 4 estudiamos algoritmos algebraicos para resolver problemas de la lógica monádica.

Consideremos un lenguaje monádico  $L$  que tiene como signos lógicos las variables  $x, y, z, \dots$ , las conectivas  $\neg$  y  $\&$  y el cuantificador universal  $\forall$  y como signos no-lógicos las constantes  $c_1, \dots, c_r$  y los símbolos de predicado monádicos

$p_1, \dots, p_m$ . Sean  $n = r + 2^m$  y  $L'$  el lenguaje obtenido añadiéndole a  $L$  las nuevas constantes  $c_{r+1}, \dots, c_n$ .

Los problemas de la lógica monádica que estudiamos son los siguientes:

**Problema LM1:** Dada una sentencia  $A$  de  $L$ , determinar si  $A$  es válida (i.e. si para toda  $L$ -estructura  $M$ ,  $M(A) = 1$ ).

**Problema LM2:** Dadas las sentencias  $A_1, \dots, A_s, B$  de  $L$ , determinar si  $B$  es una consecuencia lógica de  $\{A_1, \dots, A_s\}$  (i.e. si para todo modelo  $M$  de  $\{A_1, \dots, A_s\}$ ,  $M(B) = 1$ ).

**Problema LM3:** Dada un conjunto finito de sentencias de  $L$  determinar si es consistente (i.e. si tiene un modelo).

El Problema LM1 lo resolvemos mediante el Teorema 4.3.8 (Una sentencia  $A$  de  $L$  es válida sii  $G(A) \dashrightarrow_F^* 0$ ) donde  $F = \{X_i^2 + X_i : 1 \leq i \leq mn\}$  y  $G$  es la aplicación del conjunto de las sentencias de  $L'$  en  $Z_2[X_1, \dots, X_{mn}]$  definida por

$$G(A) = \begin{cases} X_{(i-1)n+j} & \text{si } A \text{ es } p_i c_j \\ G(B) + 1 & \text{si } A \text{ es } \neg B \\ G(B) \cdot G(C) & \text{si } A \text{ es } B \ \& \ C \\ G(B_x[c_1]) \dots G(B_x[c_n]) & \text{si } A \text{ es } \forall x B \end{cases}$$

El Problema LM2 lo resolvemos mediante el Teorema 4.4.1 (La sentencia  $B$  es consecuencia lógica de las sentencias  $A_1, \dots, A_s$  sii  $G(B) + 1 \dashrightarrow_F^* 0$  donde  $F$  es una base de Gröbner del ideal de  $Z_2[X_1, \dots, X_{mn}]$  engendrado por el conjunto  $\{G(A_1) + 1, \dots, G(A_s) + 1, X_1^2 + X_1, \dots, X_{mn}^2 + X_{mn}\}$ ).

El Problema LM3 lo resolvemos mediante el Corolario 4.4.3 (El conjunto de sentencias  $\{A_1, \dots, A_5\}$  es inconsistente sii 1 pertenece al ideal de  $Z_2[X_1, \dots, X_{mn}]$  engendrado por  $F = \{G(A_1) + 1, \dots, G(A_5) + 1, X_1^2 + X_1, \dots, X_{mn}^2 + X_{mn}\}$ ).

Al comienzo de cada uno de los capítulos se encuentra un resumen del mismo.

Los algoritmos presentados a lo largo de todo el trabajo los hemos programado en Le\_Lisp. En el apéndice se encuentra el programa correspondiente al cálculo proposicional clásico y a las bases de Gröbner en  $Z_2[X_1, \dots, X_n]$  y una sesión realizada con dicho programa en la que se comprueban los ejemplos contenidos en la Tesis.

## **CAPITULO 1**

### **RELACIONES CANÓNICAS**

En este capítulo definimos y caracterizamos las relaciones canónicas. El Teorema 1.30 y el Corolario 1.31 resumen todas las caracterizaciones. En el capítulo siguiente usaremos las relaciones canónicas para estudiar las bases de Gröbner.



**1.1.- Notación**

En lo que sigue E representará un conjunto y  $\text{--->}$  una relación binaria sobre E que llamaremos reducción. Las variables x, y, z representarán elementos de E.

**1.2.- Definición**

Para cualquier relación  $\text{--->}$  sobre E se definen:

(a) La relación de identidad:

$$\text{--->}^0 = \{ \langle x, x \rangle : x \in E \}$$

(b) La n-ésima ( $n > 0$ ) composición de  $\text{--->}$ :

$$\text{--->}^n = \{ \langle x, y \rangle \in E^2 : (\exists z \in E) [x \text{--->} z \ \& \ z \text{--->}^{n-1} y] \}$$

(c) La clausura transitiva de  $\text{--->}$ :

$$\text{--->}^+ = \bigcup_{n > 0} \text{--->}^n$$

(d) La clausura transitiva-reflexiva de  $\text{--->}$ :

$$\text{--->}^* = \bigcup_{n \geq 0} \text{--->}^n$$

(e) La inversa de  $\text{--->}$ :

$$\text{<---} = \{ \langle x, y \rangle : y \text{--->} x \}$$

(f) La clausura simétrica de  $\text{--->}$ :

$$\text{<--->} = \text{--->} \cup \text{<---}$$

**1.3.- Nota**

A la inversa y a la clausura simétrica se le pueden aplicar los apartados (a) - (d) de la anterior definición. En particular podemos obtener la clausura transitiva-reflexiva-simétrica de  $\text{--->}$ ,  $\text{<--->}^*$ , como la clausura transitiva-reflexiva de la clausura simétrica de  $\text{--->}$ .

**1.4.-Nota**

Sean  $\rightarrow_1$  y  $\rightarrow_2$  dos relaciones sobre E. Escribiremos  $x \rightarrow_1 y$  y  $\rightarrow_2 z$  en lugar de  $x \rightarrow_1 y$  e  $y \rightarrow_2 z$ .

**1.5.- Nota**

Las relaciones definidas en 2 pueden describirse como:

(a)  $x \rightarrow^n y$  sii existen  $x_0, x_1, \dots, x_n \in E$  tales que

$$x = x_0 \rightarrow x_1 \rightarrow \dots \rightarrow x_n = y$$

(b)  $x \rightarrow^+ y$  sii existe un  $n > 0$  y  $x_0, \dots, x_n \in E$

tales que

$$x = x_0 \rightarrow x_1 \rightarrow \dots \rightarrow x_n = y$$

(c)  $x \rightarrow^* y$  sii existe  $n \geq 0$  y  $x_0, \dots, x_n \in E$  tales

que

$$x = x_0 \rightarrow x_1 \rightarrow \dots \rightarrow x_n = y$$

(d)  $x \leftarrow^* y$  sii existe  $n \geq 0$  y  $x_0, \dots, x_n \in E$  tales

que

$$x = x_0 \leftarrow x_1 \leftarrow \dots \leftarrow x_n = y$$

**1.6.- Definición**

$x$  es  $\rightarrow$ -irreducible si no existe ningún  $y$  tal que  $x \rightarrow y$  (es decir, si  $x$  es minimal respecto de  $\rightarrow$ ).

**1.7.- Definición**

$y$  es una forma  $\rightarrow$ -irreducible de  $x$  si  $y$  es  $\rightarrow$ -irreducible y  $x \rightarrow^* y$ .

**1.8.- Nota**

Un elemento puede tener varias formas  $\rightarrow$ -irreducibles

o no tener ninguna. Por ejemplo, consideremos las siguientes relaciones en  $Z[X,Y]$ :

$$\text{---}>_1 = \{ \langle p, p.X \rangle : p \in Z[X,Y] \} \quad \text{y}$$

$$\text{---}>_2 = \{ \langle X, 1 \rangle, \langle X, Y \rangle \}$$

entonces  $X$  no tiene ninguna forma  $\text{---}>_1$ -irreducible y tiene dos formas  $\text{---}>_2$ -irreducibles.

### 1.9.- Definición

$\text{---}>$  es noetheriana si no existe ninguna sucesión infinita  $(x_n)$  tal que  $x_1 \text{---}> x_2 \text{---}> \dots$

### 1.10.- Ejemplo

En la nota 1.8, la relación  $\text{---}>_1$  no es noetheriana y la  $\text{---}>_2$  sí lo es.

### 1.11.- Nota

Si  $\text{---}>$  es noetheriana, cada elemento tiene al menos una forma  $\text{---}>$ -irreducible. El recíproco no es cierto.

### 1.12.- Lema (Principio de inducción noetheriana)

Si  $\text{---}>$  es noetheriana y  $A \subseteq E$  es tal que

$$(\forall x \in E) [\{y : x \text{---}>^+ y\} \subseteq A \implies x \in A],$$

entonces  $A = E$ .

### Demostración

Supongamos que  $A \neq E$ . Existe un  $x_0 \in E - A$ . Vamos a demostrar que para todo  $n$ , existen  $x_1, \dots, x_n \in E - A$  tales que  $x_0 \text{---}>^+ x_1 \text{---}>^+ \dots \text{---}>^+ x_n$  y, por lo tanto, que  $\text{---}>$  no es noetheriana. Lo haremos por inducción sobre  $n$ .

Para  $n = 1$  :  $\{y: x_0 \dashrightarrow^+ y\} \not\subseteq A$  (en caso contrario,  $x_0$  pertenecería a  $A$ ). Existe un  $x_1 \in \{y: x_0 \dashrightarrow^+ y\} - A$ . Luego,  $x_1 \in E - A$  y  $x_0 \dashrightarrow^+ x_1$ .

Para  $n = m+1$ : Supongamos que existen  $x_1, \dots, x_m$  pertenecientes a  $E - A$  tales que  $x_0 \dashrightarrow^+ x_1 \dashrightarrow^+ \dots \dashrightarrow^+ x_m$ . Como antes, existe un  $x_{m+1} \in E - A$  tal que  $x_m \dashrightarrow^+ x_{m+1}$ . Por tanto,  $x_0 \dashrightarrow^+ x_1 \dashrightarrow^+ \dots \dashrightarrow^+ x_m \dashrightarrow^+ x_{m+1}$ .

### 1.13.- Definición

(a)  $x$  e  $y$  tienen un inmediato común sucesor ( $x \downarrow y$ ) si existe un  $z$  tal que  $x \dashrightarrow z \dashleftarrow y$ .

(b)  $x$  e  $y$  tienen un común sucesor ( $x \downarrow^* y$ ) si existe  $z$  tal que  $x \dashrightarrow^* z \dashleftarrow^* y$ .

(c)  $x$  e  $y$  tienen un inmediato común antecesor ( $x \uparrow y$ ) si existe un  $z$  tal que  $x \dashleftarrow z \dashrightarrow y$ .

(d)  $x$  e  $y$  tienen un común antecesor ( $x \uparrow^* y$ ) si existe  $z$  tal que  $x \dashleftarrow^* z \dashrightarrow^* y$ .

### 1.14.- Definición

$\dashrightarrow$  es confluente si para todo  $x, y$  :

$$x \uparrow^* y \implies x \downarrow^* y.$$

### 1.15.- Ejemplo

En la nota 1.8, la relación  $\dashrightarrow_1$  es confluente y  $\dashrightarrow_2$  no lo es.

**1.16.- Nota**

Si  $\dashrightarrow$  es confluente, cada elemento tiene como máximo una forma  $\dashrightarrow$ -irreducible. El recíproco no es cierto.

**1.17.- Definición**

$\dashrightarrow$  es canónica si es noetheriana y confluente.

**1.18.- Ejemplo**

En el conjunto de los números racionales positivos, la relación  $a/b \dashrightarrow a'/b'$  sii  $a/b = a'/b'$  y  $\text{m.c.d.}(a,b) > \text{m.c.d.}(a',b')$  es canónica; pero no lo es en  $\mathbb{Q}$ .

**1.19.- Nota**

Si  $\dashrightarrow$  es canónica, cada elemento tiene una única forma  $\dashrightarrow$ -irreducible. El recíproco no es cierto (por ejemplo, la relación  $\dashrightarrow$  definida en  $\mathbb{N}$  por

$$\dashrightarrow = \{(n,0) : n \in \mathbb{N} - \{0\}\} \cup \{(n,n+1) : n \in \mathbb{N} - \{0\}\},$$

gráficamente

$$\begin{array}{ccccccc} 1 & \dashrightarrow & 2 & \dashrightarrow & 3 & \dashrightarrow & \dots \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 & & 0 & & 0 & & \end{array}$$

no es canónica aunque cada elemento tiene una única forma  $\dashrightarrow$ -irreducible).

**1.20.- Lema**

Si  $\rightarrow$  es noetheriana, son equivalentes:

(a)  $\rightarrow$  es canónica;

(b) cada elemento tiene una única forma  $\rightarrow$ -irreducible.

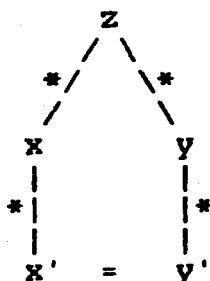
**Demostración**

(a)  $\implies$  (b): es la nota anterior.

(b)  $\implies$  (a): Hay que probar que  $\rightarrow$  es confluente.

Sean  $x, y \in E$  tales que  $x \uparrow^* y$ . Existe un  $z \in E$  tal que  $x \leftarrow^* z \rightarrow^* y$ . Sean  $x'$  e  $y'$  las formas  $\rightarrow$ -irreducibles de  $x$  e  $y$ , respectivamente. Ambas son formas  $\rightarrow$ -irreducibles de  $z$ . Por tanto, son iguales. Luego,  $x \downarrow^* y$ .

Gráficamente:

**1.21.- Definición**

Si  $\rightarrow$  es canónica, la forma  $\rightarrow$ -irreducible de cada elemento  $x$  se llama la forma  $\rightarrow$ -normal y se representa por  $FN(x)$ .

**1.22.- Definición**

$\rightarrow$  tiene la propiedad de Church - Rösser si para todo  $x, y$ :  $x \leftarrow^* y \implies x \downarrow^* y$ .

**1.23.- Lemma**

Las siguientes condiciones son equivalentes:

(a)  $\text{---}\rightarrow$  es confluente.

(b)  $\text{---}\rightarrow$  tiene la propiedad de Church - Rösser.

**Demostración**

(a)  $\implies$  (b): Puesto que  $\text{---}\rightarrow^* = \bigcup_{n \geq 0} \text{---}\rightarrow^n$ , basta

probar que para todo  $n \geq 0$ ,  $x \text{---}\rightarrow^n y \implies x \downarrow^* y$ . Lo haremos por inducción sobre  $n$ .

Base ( $n = 0$ ): Si  $x \text{---}\rightarrow^0 y$ , entonces  $x = y$ .

$x \text{---}\rightarrow^* x \text{---}\rightarrow^* y$ ,  $x \downarrow^* y$ .

Inducción: Supongamos que para todo  $z, y$ :

$z \text{---}\rightarrow^n y \implies z \downarrow^* y$ . Sean  $x, y \in E$  tales que  $x \text{---}\rightarrow^{n+1} y$ .

Existe  $z \in E$  tal que  $x \text{---}\rightarrow z \text{---}\rightarrow^n y$ . Por la hipótesis de inducción, existe  $u \in E$  tal que  $z \text{---}\rightarrow^* u \text{---}\rightarrow^* y$ . Puesto que

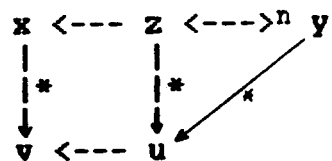
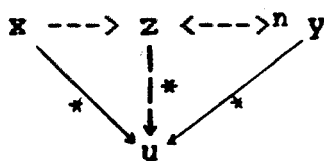
$x \text{---}\rightarrow z$ , se tiene que  $x \text{---}\rightarrow z$  ó  $x \text{---}\rightarrow z$ . En el primer

caso,  $x \text{---}\rightarrow^* u \text{---}\rightarrow^* y$  y  $x \downarrow^* y$ . En el segundo caso, se

tiene que  $x \text{---}\rightarrow z \text{---}\rightarrow^* u$  y, por (a), existe  $v \in E$  tal que

$x \text{---}\rightarrow^* v \text{---}\rightarrow^* u$ ; luego,  $x \text{---}\rightarrow^* v \text{---}\rightarrow^* y$  y  $x \downarrow^* y$ .

[Nota: gráficamente,



(b)  $\implies$  (a): Sean  $x, y \in E$  tales que  $x \downarrow^* y$ . Entonces existe  $z \in E$  tal que  $x \text{---}\rightarrow^* z \text{---}\rightarrow^* y$  y  $x \text{---}\rightarrow^* y$ . Por tanto,  $x \downarrow^* y$ .

**1.24.- Definición**

---> es localmente confluyente si para todo  $x, y$ :

$$x \uparrow y \implies x \downarrow^* y.$$

**1.25.- Nota**

Si ---> es confluyente, también es localmente confluyente. El recíproco no es cierto (por ejemplo, la relación ---> definida en  $E = \{0, 1, 2, 3\}$  por

$$2 \leftarrow 0 \leftarrow 1 \rightarrow 3$$

es localmente confluyente, pero no es confluyente).

**1.26.- Lema**

Si ---> es noetheriana, son equivalentes

- (a) ---> es confluyente
- (b) ---> es localmente confluyente

**Demostración**

(a)  $\implies$  (b): es la nota anterior

(b)  $\implies$  (a): tenemos que probar que

$$(\forall z) [(\forall x, y) [x \leftarrow^* z \rightarrow^* y \implies x \downarrow^* y]] \quad [1]$$

Sea  $A = \{z: (\forall x, y) [x \leftarrow^* z \rightarrow^* y \implies x \downarrow^* y]\}$ . [1] es equivalente a  $A = E$  que por el Lema 12 (Principio de Inducción Noetheriana), es equivalente a

$$(\forall z) [\{u: z \rightarrow^+ u\} \subseteq A \implies z \in A] \quad [2]$$

Sea  $z \in E$  tal que  $\{u: z \rightarrow^+ u\} \subseteq A$ . Sean  $x, y \in E$  tales que

$$x \leftarrow^* z \rightarrow^* y.$$

Veamos que  $x \downarrow^* y$ , lo que prueba que  $z \in A$ .

Pueden darse tres casos:



Caso 1:  $x = z$ . Entonces  $x \dashrightarrow^* y \dashleftarrow^* y \quad y \quad x \downarrow^* y$ .

Caso 2:  $y = z$ . Entonces  $x \dashrightarrow^* x \dashleftarrow^* y \quad y \quad x \downarrow^* y$ .

Caso 3:  $x \neq z$  e  $y \neq z$ . Entonces existen  $u, v \in E$

tales que

$$x \dashleftarrow^* u \dashleftarrow z \dashrightarrow v \dashrightarrow^* y.$$

Por ser  $\dashrightarrow$  localmente confluente, existe  $w \in E$  tal que

$$u \dashrightarrow^* w \dashleftarrow^* v.$$

Por la definición de  $z$ , los elementos  $u$  y  $v$  están en  $A$ .

Puesto que  $u \in A$  y  $x \dashleftarrow^* u \dashrightarrow^* w$ , existe  $u' \in E$  tal que

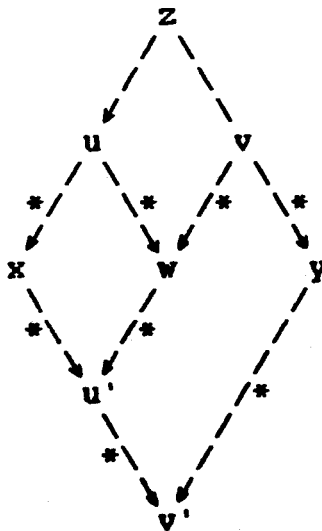
$$x \dashrightarrow^* u' \dashleftarrow^* w.$$

Puesto que  $v \in A$  y  $u' \dashleftarrow^* w \dashleftarrow^* v \dashrightarrow^* y$ , existe  $v' \in E$  tal que

$$u' \dashrightarrow^* v' \dashleftarrow^* y.$$

Por tanto,  $x \dashrightarrow^* u' \dashrightarrow^* v' \dashleftarrow^* y \quad y \quad x \downarrow^* y$ .

Gráficamente:



**1.27.- Teorema**

Si  $\rightarrow$  es noetheriana, las siguientes condiciones son equivalentes:

- (a)  $\rightarrow$  es canónica
- (b)  $\rightarrow$  es confluyente
- (c)  $\rightarrow$  tiene la propiedad de Church - Rösser
- (d)  $\rightarrow$  es localmente confluyente
- (e) cada elemento tiene una única forma  $\rightarrow$ -irreducible.

**Demostración**

- (e) y (a) son equivalentes por el Lema 1.20.
- (a) y (b) son equivalentes por la Definición 1.17.
- (b) y (c) son equivalentes por el Lema 1.23.
- (c) y (d) son equivalentes por el Lema 1.26.

**1.28.- Definición**

Una relación binaria definida en E es un orden noetheriano en E si es transitiva y noetheriana.

**1.29.- Definición**

Sea  $>$  un orden noetheriano en E.  $x$  e  $y$  están conectados bajo  $z$ ,  $x \leftarrow^* y (< z)$ , si existen  $x_0, \dots, x_n \in E$ ,  $n \geq 0$ , tales que  $x = x_0 \leftarrow x_1 \leftarrow \dots \leftarrow x_n = y$  y  $x_i < z$  para todo  $i \in \{0, \dots, n\}$ .

**1.30.- Teorema (Lema de Newman generalizado)**

Si  $\succ$  es un orden noetheriano y  $\text{---} \subseteq \succ$ , son equivalentes:

(a)  $\text{---}$  es confluente

(b) Para todo  $x, y, z \in E$ :

$$x \text{---} z \text{---} y \implies x \text{---}^* y (< z)$$

**Demostración**

(a)  $\implies$  (b): Sean  $x, y, z \in E$  tales que

$$x \text{---} z \text{---} y.$$

Existe un  $u \in E$  tal que

$$x \text{---}^* u \text{---}^* y.$$

Existen  $x_0, \dots, x_n, y_0, \dots, y_m$  ( $n, m \geq 0$ ) tales que

$$x = x_0 \text{---} \dots \text{---} x_n = u = y_m \text{---} \dots \text{---} y_0 = y.$$

Puesto que  $\text{---} \subseteq \succ$ ,  $x \text{---}^* y (< z)$ .

(b)  $\implies$  (a): Como en el Lema 1.26, sea

$$A = \{z: (\forall x, y \in E) [x \text{---}^* z \text{---}^* y \implies x \downarrow^* y]\}.$$

Tenemos que probar que  $A = E$ . Por el principio de inducción noetheriana (sobre  $\succ$ ), basta probar que

$$(\forall z) [\{u: z \succ^+ u\} \subseteq A \implies z \in A]$$

Sea  $z \in E$  tal que  $\{u: z \succ^+ u\} \subseteq A$ . Sean  $x, y \in E$  tales que

$$x \text{---}^* z \text{---}^* y.$$

Veamos que  $x \downarrow^* y$ . Y, por tanto,  $z \in A$ . Si  $z = x$  ó  $z = y$ ,  $x \downarrow^* y$ . Supongamos que  $z \neq x$  y  $z \neq y$ . Existen  $u, v \in E$  tales que

$$x \text{---}^* u \text{---} z \text{---} v \text{---}^* y.$$

Por (b),  $u \text{---}^* v (< z)$ . Existen  $u_0, \dots, u_n$  ( $n \geq 0$ ) tales que

$$u = u_0 \text{---} \dots \text{---} u_n = v$$

y  $u_i < z$  para  $i \in \{0, \dots, n\}$ . Existe  $w \in E$  tal que

$$u \text{ ----}^* w \text{ <----}^* v$$

(se demuestra por inducción sobre  $n$ :

Base: para  $n = 0$ ,  $w = u$ .

Inducción: Supongamos que  $u \downarrow^* u_{n-1}$ . Entonces existe  $w' \in E$  tal que

$$u \text{ ----}^* w' \text{ <----}^* u_{n-1}.$$

Puesto que  $u_{n-1} \text{ <----} u_n$  pueden darse dos casos:

Caso 1 :  $u_{n-1} \text{ <----} u_n$ . Entonces

$$u \text{ ----}^* w' \text{ <----}^* u_n$$

y  $u_0 \downarrow^* u_n$ .

Caso 2 :  $u_{n-1} \text{ ----} u_n$ . Entonces

$$u \text{ ----}^* w' \text{ <----}^* u_{n-1} \text{ ----} u_n.$$

$u_{n-1} \in A$  (ya que  $u_{n-1} \in \{u : z >^+ u\} \subseteq A$ ).  $w' \downarrow^* u_n$ . Existe  $w \in E$  tal que

$$w' \text{ ----}^* w \text{ <----}^* u_n.$$

Por tanto,

$$u \text{ ----}^* w \text{ <----}^* u_n.)$$

$u \in A$  (ya que  $z \text{ ----} u$ ,  $\text{----} \subseteq >$  y  $\{u : z >^+ u\} \subseteq A$ ).

$$x \text{ <----}^* u \text{ ----}^* w.$$

Existe  $u' \in E$  tal que

$$x \text{ ----}^* u' \text{ <----}^* w.$$

$v \in A$  (Análogamente a  $u \in A$ ).

$$u' \text{ <----}^* w \text{ <----}^* v \text{ ----}^* y.$$

Existe  $v' \in E$  tal que

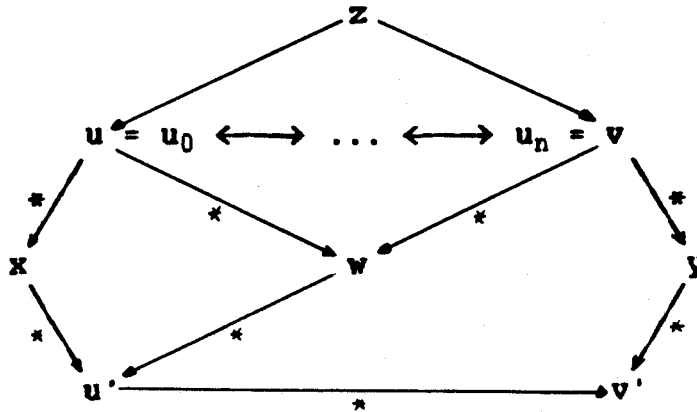
$$u' \text{ ----}^* v' \text{ <----}^* y.$$

Por tanto,

$$x \text{ ----}^* u' \text{ ----}^* v' \text{ <----}^* y$$

$y \times \downarrow^* y$ .

Gráficamente:



### 1.31.- Corolario

Si  $>$  es un orden noetheriano y  $----> \subseteq >$ , son equivalentes:

(a)  $---->$  es canónica.

(b) Para todo  $x, y, z \in E$ :

$$x <---- z <----> y \implies x <---->^* y \ (\langle z \rangle)$$

## CAPITULO 2

### ALGORITMOS DE BASE DE GRÖBNER EN $Z_p[X_1, \dots, X_n]$

En este capítulo estudiamos las bases de Gröbner en  $Z_p[X_1, \dots, X_n]$  y damos algoritmos para construirlas.

En la sección 2.1 introducimos la notación; definimos los órdenes que usaremos entre los términos, los monomios y los polinomios y demostramos algunas de sus propiedades.

En la sección 2.2 definimos la relación de reducción,  $\text{---}\rightarrow_F$ , determinada por un conjunto de polinomios,  $F$ , y estudiamos sus propiedades fundamentales en el Lema 2.2.17.

En la sección 2.3 demostramos la igualdad de la relación de equivalencia definida por el ideal engendrado por  $F$  y la clausura reflexiva-simétrica-transitiva de  $\text{---}\rightarrow_F$ .

En la sección 2.4 definimos las bases de Gröbner y en el Teorema 2.4.3 damos otras condiciones equivalentes que usaremos en la demostración de los algoritmos para construirlas.

En la sección 2.5 vemos cómo las bases de Gröbner sirven para decidir el problema de la pertenencia a un ideal.

En la sección 2.6 definimos los pares críticos que usamos en la 2.7 para caracterizar las bases de Gröbner.

En la sección 2.8, basándonos en la caracterización anterior, damos un algoritmo para calcular bases de Gröbner.

En la sección 2.9 damos dos criterios para detectar reducciones innecesarias en la construcción de bases de Gröbner.

En la sección 2.10 demostramos la unicidad de las bases de Gröbner reducidas.

**2.1.- NOTACIONES Y DEFINICIONES****2.1.1 Notaciones**

En lo que sigue,

$p$ , representa un número primo;

$n$ , representa un entero mayor o igual que 1;

$\alpha = (\alpha_1, \dots, \alpha_n)$ ,  $\beta = (\beta_1, \dots, \beta_n)$ , representan elementos de  $\mathbb{N}^n$ ;

$Z_p[X_1, \dots, X_n]$  es el anillo de polinomios en  $X_1, \dots, X_n$  con coeficientes en  $Z_p$ ;

$u, v$  representan elementos de  $Z_p$ ;

$X^\alpha = X_1^{\alpha_1} \dots X_n^{\alpha_n}$  es un término de  $Z_p[X_1, \dots, X_n]$ ;

$a, b, c, d$  representan términos de  $Z_p[X_1, \dots, X_n]$ ;

$uX^\alpha$  es un monomio de  $Z_p[X_1, \dots, X_n]$ ;

$m$  representa monomios de  $Z_p[X_1, \dots, X_n]$ ;

$p = m_1 + \dots + m_k$  es un polinomio de  $Z_p[X_1, \dots, X_n]$ ;

$p, q, r, s, h$  representan polinomios de  $Z_p[X_1, \dots, X_n]$ .

**2.1.2.- Definición**

$X^\alpha >_T X^\beta$  si

(a) el grado de  $X^\alpha$  es mayor que el grado de  $X^\beta$  (es decir,  $\alpha_1 + \dots + \alpha_n > \beta_1 + \dots + \beta_n$ ), o

(b)  $X^\alpha$  y  $X^\beta$  tienen igual grado y existe un  $k \in \{1, \dots, n\}$  tal que  $\alpha_k > \beta_k$  y  $\alpha_i = \beta_i$  para  $1 \leq i < k$ .

**2.1.3.- Definición**

$ua <_M vb$  si  $a <_T b$  ó  $(a = b \text{ y } u < v)$ .

**2.1.4.- Nota**

Los monomios de  $Z_3[X,Y]$  están ordenados por  $<_M$  de la siguiente forma:

$$1 <_M 2 <_M Y <_M 2Y <_M X <_M 2X <_M Y^2 <_M 2Y^2 <_M XY <_M 2XY <_M X^2$$

**2.1.5.- Lema**

(a)  $<_T$  es un orden total y noetheriano en el conjunto de los términos de  $Z_p[X_1, \dots, X_n]$ .

(b) Para todo  $a \neq 1$ ,  $1 <_T a$ .

(c) Si  $a <_T b$ , entonces  $ac <_T bc$ .

**2.1.6.- Lema**

(a)  $>_M$  es un orden total y noetheriano en el conjunto de los monomios de  $Z_p[X_1, \dots, X_n]$ .

(b) Si  $m_1 <_M m_2$ , entonces  $am_1 <_M am_2$

**2.1.7.- Lema**

En general, las implicaciones siguientes no son válidas

(a)  $m_1 <_M m_2 \implies m_1 m_3 <_M m_2 m_3$

(b)  $m_1 <_M m_3, m_2 <_M m_4 \implies m_1 m_2 <_M m_3 m_4$

**Demostración**

(a) En  $Z_5[X]$ ,  $2X <_M 3X$ , pero  $(2X)^2 >_M (3X)^2$

(b) En  $Z_5[X]$ ,  $2X <_M 3X$  y  $X <_M 2X$ , pero  $(2X)X >_M (3X)(2X)$

**2.1.8.- Nota**

Supondremos que todos los polinomios no nulos siempre están escritos como sumas de monomios decrecientes; es decir,  $p = m_1 + \dots + m_k$  con  $m_1 >_M \dots >_M m_k$ . Representaremos el líder del polinomio  $p$  por  $L(p) = m_1$  y el resto por



$$R(p) = m_2 + \dots + m_k.$$

### 2.1.9.- Definición

$p > q$  si (a)  $p \neq 0$  y  $q = 0$ , ó

(b)  $p \neq 0$ ,  $q \neq 0$  y  $L(p) >_M L(q)$ , ó

(c)  $p \neq 0$ ,  $q \neq 0$ ,  $L(p) = L(q)$  y  $R(p) > R(q)$ .

### 2.1.10.- Lema

(a)  $>$  es un orden total y noetheriano en  $Z_p[X_1, \dots, X_n]$ .

(b) Si  $p < q$ , entonces  $ap < aq$

### 2.1.11.- Nota

En general, las implicaciones siguientes no son válidas

(a)  $p > q \implies p + r > q + r$

(b)  $p > p'$ ,  $q > q' \implies p + q > p' + q'$

(c)  $p > q \implies pr > qr$

(d)  $p > p'$ ,  $q > q' \implies pq > p'q'$

### Demostración

En  $Z_2[X_1, \dots, X_4]$

(a) Sean  $p = X_1 + X_2$ ,  $q = X_2$  y  $r = X_1$ . Entonces  $p > q$

pero

$$p + r = X_2 < X_1 + X_2 = q + r.$$

(b) Sean  $p = X_1 + X_2 + X_3$ ,  $p' = X_2$ ,  $q = X_1 + X_2 + X_4$  y  $q' = X_4$ . Entonces  $p > p'$  y  $q > q'$ , pero

$$p + q = X_3 + X_4 < X_2 + X_4 = p' + q'.$$

(c) Sean  $p = X_1 + 1$ ,  $q = X_1$  y  $r = X_1 + 1$ . Entonces  $p > q$ . Sin embargo,

$$pr = X_1^2 + 1 < X_1^2 + X_1 = qr.$$

(d) Sean  $p = X_1X_2 + X_2 + 1$ ,  $p' = X_1X_2 + X_2$ ,  $q = X_1 + 1$  y  $q' = X_1$ . Entonces  $p > p'$  y  $q > q'$ , pero

$$pq = X_1^2 X_2 + X_1 + X_2 + 1 < X_1^2 X_2 + X_1X_2 = p'q'.$$

## 2.2.- RELACION DE REDUCCION DEFINIDA POR UN CONJUNTO DE POLINOMIOS

### 2.2.1.- Definición

El coeficiente del término  $a$  en el polinomio  $p$ ,  $\text{coef}(a,p)$ , es  $u$ , si  $ua$  es un monomio de  $p$ , y  $0$ , si no existe ningún  $u$  tal que  $ua$  sea un monomio de  $p$ .

### 2.2.2.- Nota

En la definición anterior hay que tener presente la nota 2.1.8. Así, en  $Z_3[X,Y]$ ,  $\text{coef}(X, X + Y + X) = 2$ .

### 2.2.3.- Definición

Para cada polinomio mónico  $p$  y cada término  $a$  se define la aplicación  $\rho(p,a): Z_p[X_1, \dots, X_n] \rightarrow Z_p[X_1, \dots, X_n]$  por

$$\rho(p,a)(q) = q - \text{coef}(aL(p),q)ap$$

Al escribir  $\rho(p,a)$ , supondremos que  $p$  es mónico.

### 2.2.4.- Nota

$\rho(p,a)(q)$  es  $q$  si  $aL(p)$  no es un término de  $q$  y el polinomio que se obtiene sustituyendo en  $q$  el término  $aL(p)$  por  $-aR(p)$ , en caso contrario.

### 2.2.5.- Ejemplos

En  $Z_2[X_1, X_2, X_3]$ :

$$\rho(X_1 + 1, X_2)(X_1X_2X_3 + X_1X_2) = X_1X_2X_3 + X_2$$

$$\rho(X_1 + 1, X_2X_3)(X_1X_2X_3 + X_1X_2) = X_2X_3 + X_1X_2$$

$$\rho(X_1 + 1, X_3) (X_1 X_2 X_3 + X_1 X_2) = X_1 X_2 X_3 + X_1 X_2$$

### 2.2.6.-Lema

Sea  $\rho = \rho(p, a)$ . Entonces  $\rho(q_1 + q_2) = \rho(q_1) + \rho(q_2)$ . y  
 $\rho(q_1 - q_2) = \rho(q_1) - \rho(q_2)$ .

#### Demostración

Sean  $b = L(p)$ ,  $u_1 = \text{coef}(ab, q_1)$  y  $u_2 = \text{coef}(ab, q_2)$ .

Entonces

$$\begin{aligned} \rho(q_1 + q_2) &= (q_1 + q_2) - \text{coef}(ab, q_1 + q_2)ap = \\ &= (q_1 + q_2) - (u_1 + u_2)ap = \\ &= (q_1 - u_1ap) + (q_2 - u_2ap) = \\ &= \rho(q_1) + \rho(q_2) \end{aligned}$$

$$\begin{aligned} \rho(q_1 - q_2) &= (q_1 - q_2) - \text{coef}(ab, q_1 - q_2)ap = \\ &= (q_1 - q_2) - (u_1 - u_2)ap = \\ &= (q_1 - u_1ap) - (q_2 - u_2ap) = \\ &= \rho(q_1) - \rho(q_2) \end{aligned}$$

### 2.2.7.-Lema

$$\rho(p, ba)(ubq) = ub\rho(p, a)(q)$$

#### Demostración

$$\begin{aligned} \rho(p, ba)(ubq) &= ubq - \text{coef}(baL(p), ubq)ba p = \\ &= ubq - \text{coef}(aL(p), q)ubap = \\ &= ub(q - \text{coef}(aL(p), q)ap) = \\ &= ub\rho(p, a)(q). \end{aligned}$$

**2.2.8.-Definición**

El polinomio  $q$  se reduce a  $q'$  mediante el polinomio mónico  $p$  y el término  $a$  (en símbolos  $q \rightarrow_{p,a} q'$ ) si  $q \neq q'$  y  $q' = \rho(p,a)(q)$ . Al escribir  $q \rightarrow_{p,a} q'$ , supondremos que  $p$  es mónico.

**2.2.9.-Lema**

$\rightarrow_{p,a}$  está contenida en  $>$  y, por tanto, es noetheriana.

**Demostración**

Consecuencia de 2.2.8, 2.1.8, 2.1.9, y 2.1.10.

**2.2.10.-Lema**

(a) Si  $q_1 \rightarrow_{p,a} q'_1$  y  $q_2 \rightarrow_{p,a} q'_2$ , entonces

$$q_1 + q_2 \rightarrow_{p,a} q'_1 + q'_2$$

$$q_1 - q_2 \rightarrow_{p,a} q'_1 - q'_2$$

(b) Si  $q \rightarrow_{p,a} q'$ , entonces  $ubq \rightarrow_{p,ba} ubq'$ .

**2.2.11.-Definición**

El polinomio  $q$  se reduce a  $q'$  mediante el polinomio mónico  $p$  (en símbolos:  $q \rightarrow_p q'$ ) si existe un término  $a$  tal que  $q \rightarrow_{p,a} q'$ . Al escribir  $q \rightarrow_p q'$ , supondremos que  $p$  es mónico.

**2.2.12.- Ejemplos**

En  $Z_2[X_1, X_2, X_3]$ :  $X_1X_2X_3 + X_1X_2 \rightarrow_{X_1+1} X_1X_2X_3 + X_2$  y  
 $X_1X_2X_3 + X_1X_2 \rightarrow_{X_1+1} X_2X_3 + X_1X_2$

**2.2.13.-Lemas**

- (a)  $\rightarrow_p = U\{\rightarrow_{p,a} : a \text{ es un término}\}$
- (b)  $\rightarrow_p \subseteq \succ$
- (c)  $\rightarrow_p$  es noetheriana.
- (d) Si  $q \rightarrow_p q'$ , entonces  $uaq \rightarrow_p uaq'$ .
- (e) Si  $q \rightarrow_p^* q'$ , entonces  $uaq \rightarrow_p^* uaq'$ .

**Demostración**

Consecuencia de 2.2.11, 2.2.9, y 2.2.10.

**2.2.14.-Nota**

Las siguientes implicaciones no son válidas:

- (a)  $q_1 \rightarrow_p q_1' , q_2 \rightarrow_p q_2' \implies q_1 + q_2 \rightarrow_p q_1' + q_2'$
- (b)  $q \rightarrow_p q' \implies rq \rightarrow_p rq'$

**Demostración**

En  $Z_2[X_1, \dots, X_4]$ :

- (a) Sean  $q_1 = X_1X_2 + X_4$ ,  $q_2 = X_1X_3 + X_4$ ,  $p = X_1 + 1$ ,  
 $q_1' = X_2 + X_4$  y  $q_2' = X_3 + X_4$ . Entonces  
 $q_1 \not\rightarrow_p q_1'$ ,  $q_2 \not\rightarrow_p q_2'$  pero  $q_1 + q_2 \rightarrow_p q_1' + q_2'$ .
- (b) Sean  $q = X_1 + X_3$ ,  $p = X_1 + X_2$ ,  $q' = X_2 + X_3$  y  
 $r = X_1 + 1$ . Entonces  $q \rightarrow_p q'$  pero  $rq \not\rightarrow_p rq'$ .

**2.2.15.- Definición**

Sea  $F$  un conjunto finito de polinomios mónicos. Se dice que el polinomio  $q$  se reduce a  $q'$  mediante  $F$  (y se escribe  $q \rightarrow_F q'$ ) si existe  $p \in F$  tal que  $q \rightarrow_p q'$ .

**2.2.16.- Notación**

En lo que sigue  $F$  es un conjunto finito de polinomios mónicos. Escribiremos  $\dashrightarrow$  en lugar de  $\dashrightarrow_F$ .

**2.2.17.- Lema**

- (a)  $\dashrightarrow = U\{\dashrightarrow_p : p \in F\}$
- (b)  $\dashrightarrow \subseteq \succ$
- (c)  $\dashrightarrow$  es noetheriana
- (d) Si  $q \dashrightarrow q'$ , entonces  $uaq \dashrightarrow uaq'$ .
- (e) Si  $q \dashrightarrow^* q'$ , entonces  $uaq \dashrightarrow^* uaq'$ .

**Demostración**

Consecuencia de 2.2.15 y 2.2.13.

**2.2.18.- Nota**

Las siguientes implicaciones no son válidas:

- (a)  $q_1 \dashrightarrow q_1', q_2 \dashrightarrow q_2' \implies q_1 + q_2 \dashrightarrow q_1' + q_2'$ .
- (b)  $q \dashrightarrow q' \implies rq \dashrightarrow rq'$ .

**Demostración**

Consideremos en  $Z_2[X_1, X_2, X_3]$  el conjunto  $F$  formado por los polinomios  $X_1 + X_2$  y  $X_1 + X_3$ .

- (a) Sean  $q_1 = X_1 + X_2$ ,  $q_2 = X_1 + X_3$ ,  $q_1' = q_2' = 0$ .

Entonces  $q_1 \dashrightarrow q_1'$ ,  $q_2 \dashrightarrow q_2'$ ; pero

$$q_1 + q_2 = X_2 + X_3 \not\rightarrow 0 = q_1' + q_2'.$$

- (b) Sean  $q = X_1 + X_2$ ,  $q' = 0$  y  $r = X_1 + 1$ . Entonces

$q \dashrightarrow q'$ ; pero

$$rq = X_1^2 + X_1X_2 + X_1 + X_2 \not\rightarrow 0 = rq'.$$

## 2.3.- REDUCCIONES E IDEALES

### 2.3.1.- Notación

Representaremos por  $I(F)$  el ideal engendrado por  $F$  y por  $\equiv_F$  (ó  $\equiv$ ) la relación de equivalencia definida por  $F$  (es decir,  $q \equiv_F q'$  sii  $q - q' \in I(F)$ ).

### 2.3.2.- Lema

Para todo  $n \in \mathbb{N}$ ,  $\langle \dashrightarrow \rangle^n \subseteq \equiv$

#### Demostración

Por inducción sobre  $n$ .

Para  $n=0$ :  $q \langle \dashrightarrow \rangle^0 q' \implies q = q'$

$$\implies q - q' \in I(F)$$

$$\implies q \equiv q'.$$

Para  $n=1$ : Supongamos que  $q \langle \dashrightarrow \rangle q'$ . Entonces  $q \dashrightarrow q'$  o  $q' \dashrightarrow q$ . Si  $q \dashrightarrow q'$ , existe  $p \in F$ , un  $u \in \mathbb{Z}_p$  y un término  $a$  tales que  $q' = q - uap$ ; luego,  $q - q' = uap \in I(F)$  y  $q \equiv q'$ . Análogamente, si  $q' \dashrightarrow q$ ,  $q \equiv q'$ . Por tanto,  $q \equiv q'$ .

Para  $n = k + 1$ ,  $k > 0$ : Supongamos que  $q \langle \dashrightarrow \rangle^{k+1} q'$  y  $\langle \dashrightarrow \rangle^k \subseteq \equiv$ . Entonces existe  $r$  tal que  $q \langle \dashrightarrow \rangle r \langle \dashrightarrow \rangle^k q'$ . Por el caso  $n = 1$ ,  $q \equiv r$ . Luego, por la hipótesis de inducción,  $r \equiv q'$ . Por tanto,  $q \equiv q'$ .

### 2.3.3.- Lema

$$(a) \langle \dashrightarrow \rangle^* \subseteq \equiv$$

$$(b) \dashrightarrow^* \subseteq \equiv$$

#### Demostración

(a) Consecuencia de 2.3.2 puesto que  $\langle \dashrightarrow \rangle^* = \bigcup_{n \geq 0} \langle \dashrightarrow \rangle^n$ .



$$(b) \text{---}^* \subseteq \text{----}^* \subseteq \equiv.$$

#### 2.3.4.- Nota

En general,  $\text{----}^* \neq \equiv$ .

#### Demostración

En  $Z_2[X_1, X_2, X_3]$ , sea  $F = \{X_1 + X_2, X_1 + X_3\}$ . Entonces  $X_2 + X_3 = 0$ , pero no  $X_2 + X_3 \text{----}^* 0$ .

#### 2.3.5.-Lema

Si  $q \text{----} q'$ , entonces  $q + r \downarrow^* q' + r$ .

#### Demostración

Supongamos que  $q \text{----} q'$ . Existen  $p \in F$  y  $a$  tales que  $q \text{----}_{p,a} q'$ . Sea  $u = \text{coef}(aL(p), q)$ . Entonces,  $q' = q - uap$  y  $\text{coef}(aL(p), q') = 0$ . Sea  $v = \text{coef}(aL(p), r)$ .

$$\begin{aligned} \rho(a,p)(q+r) &= (q+r) - \text{coef}(aL(p), q+r)ap = \\ &= (q+r) - (u+v)ap = \\ &= q - uap + r - vap = \\ &= q' + r - vap. \end{aligned}$$

$$\begin{aligned} \rho(a,p)(q'+r) &= (q'+r) - \text{coef}(aL(p), q'+r)ap = \\ &= (q'+r) - vap. \end{aligned}$$

Por tanto,  $q+r \text{----}^* q'+r - vap \text{----}^* q'+r$  y  $q+r \downarrow^* q'+r$ .

#### 2.3.6.- Lema

Si  $\{p_1, \dots, p_n\} \subseteq F$  y  $\{u_1, \dots, u_n\} \subseteq Z_p - \{0\}$ .

$$q + u_1 a_1 p_1 + \dots + u_n a_n p_n \text{----}^* q.$$

#### Demostración

Por inducción sobre  $n$ :

Para  $m = 1$ :

$$\begin{aligned} u_1 a_1 p_1 \text{ ----} > 0 & \implies q + u_1 a_1 p_1 \downarrow^* q & \text{ [por 2.3.5]} \\ & \implies q + u_1 a_1 p_1 \text{ <----}^* q. \end{aligned}$$

Para  $m > 1$ : Por el caso anterior,

$$q + u_1 a_1 p_1 + \dots + u_m a_m p_m \text{ <----}^* q + u_1 a_1 p_1 + \dots + u_{m-1} a_{m-1} p_{m-1}.$$

Por la hipótesis de inducción,

$$q + u_1 a_1 p_1 + \dots + u_{m-1} a_{m-1} p_{m-1} \text{ <----}^* q.$$

Luego,

$$q + u_1 a_1 p_1 + \dots + u_m a_m p_m \text{ <----}^* q.$$

### 2.3.7.- Lema

$$\equiv \subseteq \text{ <----}^*.$$

#### Demostración

Sean  $q$  y  $q'$  tales que  $q \equiv q'$ . Si  $q = q'$ ,  $q \text{ <----}^* q'$ .

Supongamos que  $q \neq q'$ . Existen  $\{p_1, \dots, p_m\} \subseteq F$ ,  $\{u_1, \dots, u_m\} \subseteq \mathbb{Z}_p - \{0\}$  y términos  $a_1, \dots, a_m$  tales que  $q - q' = u_1 a_1 p_1 + \dots + u_m a_m p_m$ . Por 2.3.6,

$$q = q' + u_1 a_1 p_1 + \dots + u_m a_m p_m \text{ <----}^* q'.$$

### 2.3.8.- Corolario

$$\equiv = \text{ <----}^*.$$

#### Demostración

Consecuencia de 2.3.3 y 2.3.7.

**2.4.-BASES DE GRÖBNER****2.4.1.-Definición**

$F$  es una base de Gröbner si  $\rightarrow$  es canónica.

**2.4.2.- Ejemplo**

En  $\mathbb{Z}_2[X_1, X_2, X_3]$ ,  $F = \{X_1 + X_2, X_1 + X_3\}$  no es una base de Gröbner.

**2.4.3.- Teorema**

Las condiciones siguientes son equivalentes:

- (a)  $F$  es una base de Gröbner.
- (b)  $\rightarrow$  es confluyente.
- (c)  $\rightarrow$  tiene la propiedad de Church-Rösser.
- (d)  $\rightarrow$  es localmente confluyente.
- (e) Cada elemento de  $\mathbb{Z}_p[X_1, \dots, X_n]$  tiene una única forma

$\rightarrow$ -irreducible.

**Demostración**

Consecuencia de 2.4.1, 1.26 y 2.2.17.

**2.4.4.- Lema**

Si  $q_1 - q_2 \rightarrow^* 0$ , entonces  $q_1 \downarrow^* q_2$ .

**Demostración**

Por hipótesis, existen polinomios  $p_1, \dots, p_n$  de  $F$ , términos  $a_1, \dots, a_n$  y aplicaciones  $\rho_1 = \rho(p_1, a_1), \dots, \rho_n = \rho(p_n, a_n)$ , tales que  $\rho^*(q_1 - q_2) = 0$ , donde  $\rho^* = \rho_n \circ \dots \circ \rho_1$ . Puesto que,

$$\begin{aligned}
\varrho^*(q_1 - q_2) = 0 &\implies \varrho^*(q_1) - \varrho^*(q_2) = 0 && \text{[por 2.2.6]} \\
&\implies \varrho^*(q_1) = \varrho^*(q_2) \\
&\implies q_1 \text{ ----}^* \varrho^*(q_1) = \varrho^*(q_2) \text{ <----}^* q_2 \\
&\implies q_1 \downarrow^* q_2
\end{aligned}$$

resulta que  $q_1 \downarrow^* q_2$ .

### 2.4.5.- Lema

Sea  $F$  una base de Gröbner.

(a) Si para todo  $i \in \{1, \dots, m\}$ ,  $q_i \text{ ----}^* 0$ , entonces  $q_1 + \dots + q_m \text{ ----}^* 0$ .

(b) Si  $q \text{ ----}^* 0$ , entonces  $rq \text{ ----}^* 0$ .

### Demostración

(a) Por inducción sobre  $m$ :

Para  $m = 2$ : Existen polinomios  $p_1, \dots, p_k \in F$ , términos  $a_1, \dots, a_k$  y aplicaciones  $\varrho_1 = \varrho(p_1, a_1), \dots, \varrho_k = \varrho(p_k, a_k)$ , tales que  $\varrho^*(q_1) = 0$ , donde  $\varrho^* = \varrho_k \circ \dots \circ \varrho_1$ . Entonces

$$\begin{aligned}
\varrho^*(q_1 + q_2) &= \varrho^*(q_1) + \varrho^*(q_2) = && \text{[por 2.6]} \\
&= \varrho^*(q_2)
\end{aligned}$$

Puesto que  $\varrho^*(q_2) \text{ <----}^* q_2 \text{ ----}^* 0$  y  $\text{----}$  es canónica,

$\varrho^*(q_2) \downarrow^* 0$ ; luego, existen  $s_1, \dots, s_l \in F$ ,  $b_1, \dots, b_l$ ,

$\tau_1 = \varrho(s_1, b_1), \dots, \tau_l = \varrho(s_l, b_l)$ ,  $\tau^* = \tau_l \circ \dots \circ \tau_1$  tales que

$\tau^*(\varrho^*(q_2)) = 0$ . Por tanto,  $(\tau^* \circ \varrho^*)(q_1 + q_2) = 0$  y

$q_1 + q_2 \text{ ----}^* 0$ .

Para  $m = k+1 > 2$ :

$$q_1 + \dots + q_{k+1} = (q_1 + \dots + q_k) + q_{k+1} \text{ ----}^* 0$$

(por hipótesis de inducción y el caso  $m = 2$ ).

(b) Sea  $r = u_1 a_1 + \dots + u_m a_m$ . Para todo  $i \in \{1, \dots, m\}$ ,  $u_i a_i q \text{ ----}^* 0$  (por 2.2.17). Luego,

$$rq = u_1 a_1 q + \dots + u_n a_n q \text{ ----}^* 0 \quad [\text{por (a)}]$$

### 2.4.6.- Nota

Las siguientes implicaciones no son válidas:

$$(a) q_1 \text{ ----}^* 0, q_2 \text{ ----}^* 0 \implies q_1 + q_2 \text{ ----}^* 0$$

$$(b) q \text{ ----}^* 0 \implies rq \text{ ----}^* 0$$

### Demostración

En  $Z_2[X_1, X_2, X_3]$ :

(a) Sean  $F = \{X_1 + X_2, X_1 + X_3\}$ ,  $q_1 = X_1 + X_2$  y  $q_2 = X_1 + X_3$ . Entonces  $q_1 \text{ ----}^* 0$ ,  $q_2 \text{ ----}^* 0$ , pero

$$q_1 + q_2 = X_2 + X_3 \not\text{----}^* 0.$$

(b) Sean  $p_1 = X_1 X_2 + X_3$ ,  $p_2 = X_2 + X_3$ ,  $F = \{p_1, p_2\}$ ,  $q = X_1 X_2 + X_2$  y  $r = X_1 + 1$ . Entonces

$$q = X_1 X_2 + X_2 \text{ ----}^*_{p_1} X_3 + X_2 \text{ ----}^*_{p_2} 0$$

Luego,  $q \text{ ----}^* 0$ , pero

$$\begin{array}{l}
 rq = X_1^2 X_2 + X_2 \begin{cases} \xrightarrow{p_1} X_1 X_3 + X_2 \xrightarrow{p_2} X_1 X_3 + X_3 \\ \xrightarrow{p_2} X_1^2 X_3 + X_2 \xrightarrow{p_2} X_1^2 X_3 + X_3 \\ \xrightarrow{p_2} X_1^2 X_2 + X_3 \begin{cases} \xrightarrow{p_1} X_1 X_3 + X_3 \\ \xrightarrow{p_2} X_1^2 X_3 + X_3 \end{cases} \end{cases}
 \end{array}$$

Las formas ---->-irreducibles de  $rq$  son  $X_1 X_3 + X_3$  y  $X_1^2 X_3 + X_3$

Por tanto,  $rq \not\text{----}^* 0$ .

**2.5.- BASES DE GRÖBNER Y PERTENENCIA A UN IDEAL****2.5.1.- Lema**

Si  $q \dashrightarrow^* 0$ , entonces  $q \in I(F)$ .

**Demostración**

$q \dashrightarrow^* 0 \implies q \equiv 0$  [por 2.3.3.b]

$\implies q \in I(F)$  [por 2.3.1]

**2.5.2.- Lema**

El recíproco del Lema anterior no es válido.

**Demostración**

En  $Z_2[X_1, X_2, X_3]$ , sean  $F = \{X_1 + X_2, X_1 + X_3\}$  y  $q = X_2 + X_3$ .

Entonces  $q \in I(F)$  pero  $q \not\rightarrow^* 0$ .

**2.5.3.- Teorema**

Las siguientes condiciones son equivalentes:

(a)  $F$  es una base de Gröbner.

(b) Para todo  $q$ ,  $q \in I(F) \implies q \dashrightarrow^* 0$ .

**Demostración**

(a)  $\implies$  (b):

$q \in I(F) \implies q \equiv 0$

$\implies q \dashleftarrow^* 0$  [por 2.3.7]

$\implies q \downarrow^* 0$  [por (a) y 2.4.3.c]

$\implies q \dashrightarrow^* 0$ .

(b)  $\implies$  (a): Por 2.4.3, basta probar que  $\dashrightarrow$  tiene la propiedad de Church-Rösser. (i.e.  $q_1 \dashleftarrow^* q_2 \implies q_1 \downarrow^* q_2$ ).

$$\begin{aligned}
 q_1 \text{ <--->}^* q_2 & \implies q_1 \equiv q_2 & \text{[por 2.3.a]} \\
 & \implies q_1 - q_2 \in I(F) & \text{[por 2.3.1]} \\
 & \implies q_1 - q_2 \text{ <--->}^* 0 & \text{[por (b)]} \\
 & \implies q_1 \downarrow^* q_2 & \text{[por 2.4.4]}
 \end{aligned}$$

#### 2.5.4.- Corolario

Sea  $F$  una base de Gröbner. Para todo  $q$ ,

$$q \in I(F) \iff q \text{ <--->}^* 0.$$

#### Demostración

Consecuencia de 2.5.1 y 2.5.3.

#### 2.5.6.- Lema

Sea  $F$  una base de Gröbner

$$(a) \text{ FN}(q_1 + \dots + q_m) = \text{FN}(q_1) + \dots + \text{FN}(q_m)$$

$$(b) \text{ FN}(rq) = \text{FN}(r\text{FN}(q))$$

$$(c) \text{ FN}(q_1 - q_2) = \text{FN}(q_1) - \text{FN}(q_2)$$

#### Demostración

(a) Por la definición de la forma normal,  $q_i \text{ <--->}^* \text{FN}(q_i)$  para todo  $i \in \{1, \dots, m\}$ ; luego,  $q_i \equiv \text{FN}(q_i)$ . Por tanto,

$$q_1 + \dots + q_m \equiv \text{FN}(q_1) + \dots + \text{FN}(q_m)$$

$$q_1 + \dots + q_m \text{ <--->}^* \text{FN}(q_1) + \dots + \text{FN}(q_m)$$

$$\text{FN}(q_1 + \dots + q_m) \equiv \text{FN}(q_1) + \dots + \text{FN}(q_m)$$

(b) Por la definición de  $\text{FN}$ ,  $q \text{ <--->}^* \text{FN}(q)$ . Además

$$q \text{ <--->}^* \text{FN}(q) \implies q \equiv \text{FN}(q) \quad \text{[por 2.3.3.b]}$$

$$\implies rq \equiv r.\text{FN}(q)$$

$$\implies rq \text{ <--->}^* r.\text{FN}(q) \quad \text{[por 2.5.5]}$$

$$\implies rq \downarrow^* r.\text{FN}(q) \quad \text{[por 2.4.3]}$$

$$\implies \text{FN}(rq) = \text{FN}(r.\text{FN}(q))$$

Luego,  $FN(rq) = FN(r.FN(q))$ .

$$\begin{aligned} \text{(c) } FN(q_1 - q_2) &= FN(q_1 + (-q_2)) = \\ &= FN(q_1) + FN(-q_2) = \\ &= FN(q_1) - FN(q_2) \end{aligned}$$

### 2.5.7.- Teorema

Las siguientes condiciones son equivalentes:

(a)  $F$  es una base de Gröbner

(b) Para todo  $q, q_1, q_2$ :

$$q_1 \langle \text{----}^* q \text{----} \rangle^* q_2 \implies q_1 - q_2 \text{----}^* 0.$$

#### Demostración

(a)  $\implies$  (b): Supongamos que  $q_1 \langle \text{----}^* q \text{----} \rangle^* q_2$ . Por 2.4.3,  $q_1 \downarrow^* q_2$ . Luego,  $FN(q_1) = FN(q_2)$ . Por 2.5.6.c,  $FN(q_1 - q_2) = FN(q_1) - FN(q_2) = 0$ . Por tanto,  $q_1 - q_2 \text{----}^* 0$ .

(b)  $\implies$  (a) Por 2.4.3, basta probar que  $\text{--}$  es confluente. Sean  $q, q_1, q_2$  tales que  $q_1 \langle \text{----}^* q \text{----} \rangle^* q_2$ . Por hipótesis,  $q_1 - q_2 \text{----}^* 0$ . Luego, por 2.4.4,  $q_1 \downarrow^* q_2$ .



**2.6.- PARES CRITICOS****2.6.1.- Definición**

El par crítico de  $q_1$  y  $q_2$  es

$$PC(q_1, q_2) = (m.c.m(L(q_1), L(q_2)) \cdot R(q_1) / L(q_1), \\ m.c.m(L(q_1), L(q_2)) \cdot R(q_2) / L(q_2))$$

**2.6.2.- Definición**

El S-polinomio del par  $\langle q_1, q_2 \rangle$  es  $SP(q_1, q_2) = q_1 - q_2$ .

**2.6.3.-Lema**

Si  $q_1, q_2 \in I(F)$ ,  $SP(PC(q_1, q_2)) \in I(F)$ .

**Demostración**

Sean  $a = m.c.m(L(q_1), L(q_2))$  y  $b_i = a/L(q_i)$  para  $i = 1, 2$

Entonces:

$$\begin{aligned} SP(PC(q_1, q_2)) &= b_1 R(q_1) - b_2 R(q_2) = \\ &= b_1 (q_1 - L(q_1)) - b_2 (q_2 - L(q_2)) = \\ &= b_1 q_1 - a - b_2 q_2 + a = \\ &= b_1 q_1 - b_2 q_2 \in \\ &\in I(F). \end{aligned}$$

## 2.7.-CARACTERIZACION DE BASES DE GRÖBNER MEDIANTE PARES CRITICOS.

### 2.7.1.-Lema

Sean  $p_1, p_2 \in F$  y  $q, q_1, q_2 \in Z_p[X_1, \dots, X_n]$  tales que  
 $q \dashrightarrow_{p_1, a_1} q_1$  y  $q \dashrightarrow_{p_2, a_2} q_2$ .

(a) Si  $a_1 L(p_1) \neq a_2 L(p_2)$ , entonces  $q_1 \downarrow^* q_2$ .

(b) Si  $SP(PC(p_1, p_2)) \dashrightarrow^* 0$ , entonces  $q_1 \downarrow^* q_2$ .

### Demostración

(a) Para  $i \in \{1, 2\}$ , sea  $\rho_i = \rho(p_i, a_i)$ . Puesto que  
 $q \dashrightarrow_{p_i, a_i} q_i$ ,

$$\text{coef}(a_i L(p_i), q) = u_i \neq 0. \quad [1.i]$$

Podemos suponer, sin pérdida de generalidad, que

$$a_1 L(p_1) > a_2 L(p_2),$$

con lo que

$$\text{coef}(a_1 L(p_1), a_2 R(p_2)) = 0. \quad [2]$$

Sea

$$r = q - u_1 a_1 L(p_1) - u_2 a_2 L(p_2). \quad [3]$$

Entonces

$$\text{coef}(a_i L(p_i), r) = 0 \quad [4.i]$$

(ya que  $a_1 L(p_1) \neq a_2 L(p_2)$ ).

$$\begin{aligned} q_1 &= q - u_1 a_1 p_1 = \\ &= q - u_1 a_1 L(p_1) - u_1 a_1 R(p_1) = \\ &= r + u_2 a_2 L(p_2) - u_1 a_1 R(p_1) \end{aligned} \quad [5.1]$$

Análogamente,

$$q_2 = r + u_1 a_1 L(p_1) - u_2 a_2 R(p_2). \quad [5.2]$$

Por [4.1] y [2],

$$\text{coef}(a_1L(p_1), q_2) = u_1;$$

$$\rho_1(q_2) = q_2 - a_1u_1p_1.$$

Por [5.2],

$$\rho_1(q_2) = r - u_1a_1R(p_1) - u_2a_2R(p_2) \quad [6]$$

Distinguimos dos casos:

Caso 1:  $\text{coef}(a_2L(p_2), a_1R(p_1)) = 0$ . Entonces, por

[5.1] y [4.2]

$$\text{coef}(a_2L(p_2), q_1) = u_2;$$

$$\begin{aligned} \rho_2(q_1) &= q_1 - u_2a_2p_2 = \\ &= r - u_2a_2R(p_2) - u_1a_1R(p_1) = \\ &= \rho_1(q_2). \end{aligned}$$

Luego,  $q_1 \downarrow^* q_2$ .

Caso 2:  $\text{coef}(a_2L(p_2), a_1R(p_1)) = u_2' \neq 0$ . Entonces por

[6] y [4.2],

$$\begin{aligned} \text{coef}(a_2L(p_2), \rho_1(q_2)) &= -u_1u_2'; \\ \rho_2(\rho_1(q_2)) &= r - u_1a_1R(p_1) - u_2a_2R(p_2) + u_1u_2'a_2p_2 \end{aligned}$$

Por [5.1] y [4.2],

$$\begin{aligned} \text{coef}(a_2L(p_2), q_1) &= u_2 - u_1u_2'; \\ \rho_2(q_1) &= r + u_2a_2L(p_2) - u_1a_1R(p_1) - (u_2 - u_1u_2')a_2p_2 = \\ &= r - u_2a_2R(p_2) - u_1a_1R(p_1) + u_1u_2'a_2p_2 = \\ &= \rho_2(\rho_1(q_2)). \end{aligned}$$

Luego,  $q_1 \downarrow^* q_2$ .

(b) Si  $a_1L(p_1) \neq a_2L(p_2)$ , entonces  $q_1 \downarrow^* q_2$  por (a). Supongamos que

$$a_1L(p_1) = a_2L(p_2). \quad [1]$$

Sean

$$u = \text{coef}(a_1L(p_1), q) = \text{coef}(a_2L(p_2), q),$$

$$b = \text{m.c.m.}(L(p_1), L(p_2)). \quad [2]$$

$$c_i = b/L(p_i) \quad (i \in \{1,2\}) \quad [3.i]$$

Por [1],  $a_1L(p_1)$  es un múltiplo común de  $L(p_1)$  y  $L(p_2)$ , y por [2],  $a_1L(p_1)$  es un múltiplo de  $b$ . Sea

$$d = a_1L(p_1)/b. \quad [4.1]$$

Por [1],

$$d = a_2L(p_2)/b. \quad [4.2]$$

Por [3.i] y [4.i],

$$dc_i = a_i. \quad [5.i]$$

$$q_1 - q_2 = (q - ua_1p_1) - (q - ua_2p_2).$$

Por [1],

$$q_1 - q_2 = -ua_1R(p_1) + ua_2R(p_2).$$

Por [5.1] y [5.2],

$$\begin{aligned} q_1 - q_2 &= udc_1R(p_1) + udc_2R(p_2) = \\ &= ud(c_1R(p_1) - c_2R(p_2)). \end{aligned}$$

Por [3] y 6.1,

$$q_1 - q_2 = -udSP(PC(p_1, p_2)).$$

Por 2.2.17.e,

$$q_1 - q_2 \text{ ---}>^* 0.$$

Por 2.4.4,

$$q_1 \downarrow^* q_2 .$$

### 2.7.2 Teorema

Las siguientes condiciones son equivalentes:

(a)  $F$  es una base de Gröbner

(b) Para todo  $p_1, p_2 \in F$  :  $SP(PC(p_1, p_2)) \text{ ---}>^*_F 0$ .

### Demostración

(a)  $\implies$  (b): Por 2.6.4 y 2.5.3.

(b)  $\implies$  (a): Por 2.4.3 y 2.7.1.

**2.8.- ALGORITMO DE CALCULO DE BASES DE GRÖBNER****2.8.1.- Notación**

En lo que sigue, representaremos por  $A$  el conjunto de los conjuntos finitos de polinomios mónicos de  $Z_p[X_1, \dots, X_n]$ .

**2.8.2.- Definición**

Una función de selección es una función computable

$$\text{Sel}: Z_p[X_1, \dots, X_n] \times A \dashrightarrow Z_p[X_1, \dots, X_n]$$

tal que para todo  $F \in A$  y todo  $p \in Z_p[X_1, \dots, X_n]$  que no sea  $\dashrightarrow_F$ -irreducible,  $p \dashrightarrow_F \text{Sel}(p, F)$ .

**2.8.3.- Lema**

La función

$$\text{selector}: Z_p[X_1, \dots, X_n] \times A \dashrightarrow Z_p[X_1, \dots, X_n]$$

que a cada  $p = u_1 a_1 + \dots + u_k a_k$  y  $F = \{q_1, \dots, q_m\} \in A$  le asocia  $\text{selector}(p, F)$ , definida por:

- (i) si  $p$  es  $\dashrightarrow_F$ -irreducible,  $\text{selector}(p, F) = p$ ;
- (ii) si  $p$  es  $\dashrightarrow_F$ -reducible,  $\text{selector}(p, F) = \varrho(q, a)(p)$ ,

donde

$$j = \inf\{i \in \{1, \dots, m\}: (\exists a) [\text{coef}(aL(q_i), p) \neq 0]\},$$

$$q = q_j,$$

$$j' = \inf\{i \in \{1, \dots, k\}: (\exists a) [aL(q) = u_i a_i]\},$$

$$a = a_{j'} / L(q);$$

es una función de selección.

2.8.4.- Definición

Una función computable

$$S: Z_p[X_1, \dots, X_n] \times A \dashrightarrow Z_p[X_1, \dots, X_n]$$

es un algoritmo de forma normal si para todo  $F \in A$  y todo  $p \in Z_p[X_1, \dots, X_n]$ ,  $S(p, F)$  es una forma  $\dashrightarrow_F$ -irreducible de  $p$ .

2.8.5.- Lema

La función

$$FN : Z_p[X_1, \dots, X_n] \times A \dashrightarrow Z_p[X_1, \dots, X_n]$$

definida por

$$FN(p, F) = \begin{cases} p, & \text{si } p \text{ es } \dashrightarrow_F\text{-irreducible;} \\ FN(\text{selector}(p, F), F), & \text{en caso contrario;} \end{cases}$$

es un algoritmo de forma normal.

Demostración

El cálculo de  $FN(p, F)$  termina porque  $\dashrightarrow_F$  es noetheriana (2.2.17) y  $p \dashrightarrow^* FN(p, F)$  por 2.8.3.

2.8.6.-Lema

Si  $p \dashrightarrow^*_F q$  y  $p \in I(F)$ , entonces  $q \in I(F)$ .

Demostración

$$\begin{aligned} p \dashrightarrow^*_F q &\implies p \dashleftarrow^*_F q \\ &\implies p \equiv q && \text{[por 2.3.6]} \\ &\implies p - q \in I(F) \\ &\implies q = p - (p - q) \in I(F). \end{aligned}$$

2.8.7.- Lema

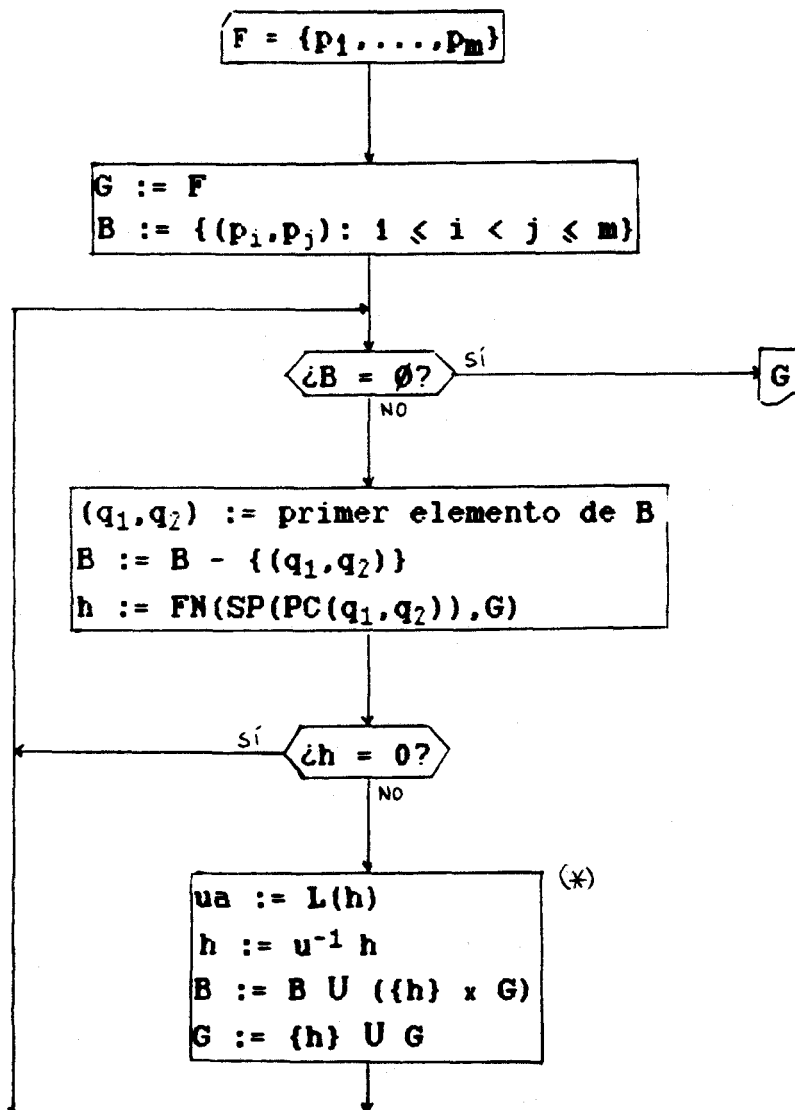
Si  $p \in F$ , entonces  $FN(p, F) \in I(F)$ .

Demostración

Por 2.8.5 y 2.8.4,  $p \rightarrow^*_{\mathcal{F}} \text{FN}(p, \mathcal{F})$ . Por hipótesis y 2.8.6,  $\text{FN}(p, \mathcal{F}) \in I(\mathcal{F})$ .

2.8.8.- Algoritmo (para calcular bases de Gröbner)

Dado  $\mathcal{F} = \{p_1, \dots, p_m\}$ , el siguiente procedimiento



termina construyendo un  $G$  tal que  $I(\mathcal{F}) = I(G)$  y  $G$  es una base de Gröbner.

Demostración

(a) El procedimiento termina:

Para cada  $i \geq 1$ , sea  $G_i$  el valor de  $G$  tras la  $i$ -ésima ejecución del bloque (\*) y  $P_i = \{L(q) : q \in G_i\}$ . Entonces para todo  $i$ ,

$G_i \subset G_{i+1}$ ,  $P_i \subseteq P_{i+1}$ ,  $I(P_i) \subseteq I(P_{i+1})$  e  $I(P_i) \neq I(P_{i+1})$ , ya que en caso contrario  $L(h) \in I(P_i)$  y  $h$  sería  $\rightarrow_{G_i}$ -reducible, en contradicción con la definición de  $h$ . Por lo tanto, si el procedimiento no termina, se forma una cadena infinita ascendente de ideales de  $Z_p[X_1, \dots, X_n]$ ,  $I(P_i)$ , en contradicción con el teorema de la base de Hilbert.

(b) Veamos que  $I(F) = I(G)$ :

Sea  $k$  el número de veces que se ejecuta el bloque (\*). Si  $k = 0$ , entonces  $G = F$  e  $I(G) = I(F)$ . Supongamos que  $k > 0$ . Para cada  $i \in \{1, \dots, k\}$  sea  $h_i$  el valor de  $h$  en la  $i$ -ésima ejecución del bloque (\*) y  $G_i$  el valor de  $G$  tras la  $i$ -ésima ejecución dicho bloque. Sea  $G_0 = F$ . Veamos, por inducción sobre  $i$ , que para todo  $i \in \{0, \dots, k\}$ ,  $I(G_i) = I(F)$ .

$$I(G_0) = I(F).$$

Sea  $j \in \{1, \dots, k-1\}$ . Supongamos que  $I(G_j) = I(F)$ . Entonces  $h_{j+1}$  es un múltiplo de  $FN(SP(PC(q_1, q_2)), G_j)$  y  $q_1, q_2 \in G_j$ . Por 2.6.4,  $SP(PC(q_1, q_2)) \in I(G_j)$ . Por 2.8.7,  $h_{j+1} \in I(G_j)$ . Por tanto,  $h_{j+1} \in I(F)$  y  $I(G_{j+1}) = I(G_j \cup \{h_{j+1}\}) = I(F)$ .

$$\text{Por consiguiente, } I(G) = I(G_k) = I(F).$$

(c)  $G$  es una base de Gröbner:

Por 2.7.2, basta probar que para todo  $q_1, q_2 \in G$ ,  
 $SP(PC(q_1, q_2)) \rightarrow_G^* 0$ .



Sean  $G_0, B_0$  los valores iniciales de  $G$  y  $B$ ,  $k$  el número de veces que se ejecuta el bloque (\*),  $G_i$  y  $B_i$  los valores de  $G$  y  $B$  tras la  $i$ -ésima ( $1 \leq i \leq k$ ) ejecución dicho bloque.

Sean  $q_1, q_2 \in G$ . Tenemos que demostrar que  
 $SP(PC(q_1, q_2)) \dashrightarrow_G^* 0$ . Sean

$$i_1 = \inf\{i: q_1 \in G_i\},$$

$$i_2 = \inf\{i: q_2 \in G_i\},$$

$$i' = \max\{i_1, i_2\}.$$

Supongamos que  $i' = i_1$ .  $\langle q_1, q_2 \rangle \in B_{i'}$  [dem: si  $i' = 0$ ,  $B_0 = B_{i'}$  y  $\langle q_1, q_2 \rangle \in B_{i'}$ ; si  $i' > 0$ ,  $B_{i'} = B_{i'-1} \cup (\{q_1\} \times G_{i'-1})$  y  $\langle q_1, q_2 \rangle \in B_{i'}$ ].  $h := FN(SP(PC(q_1, q_2)), G_j)$  se ejecuta para algún  $j \in \{i', \dots, k\}$ . Si  $h = 0$ ,  $SP(PC(q_1, q_2)) \dashrightarrow_{G_j}^* 0$  y  $SP(PC(q_1, q_2)) \dashrightarrow_G^* 0$ . Si  $h \neq 0$ ,  $h \in G_{j+1}$ .  
 $SP(PC(q_1, q_2)) \dashrightarrow_{G_j}^* h \dashrightarrow_{G_{j+1}} 0$ , y  $SP(PC(q_1, q_2)) \dashrightarrow_G^* 0$ .  
 Por tanto,  $SP(PC(q_1, q_2)) \dashrightarrow_G^* 0$ .

### 2.8.9.- Ejemplo

Vamos a aplicar el Algoritmo anterior para calcular una base de Gröbner del ideal de  $Z_2[a, b, c, d]$  engendrado por el conjunto  $F = \{p_1 = bd + b + d + 1, p_2 = cd + d, p_3 = ab + b\}$ .

#### Solución

$$G = F$$

$$FN(SP(PC(p_1, p_2)), G) = bc + b + c + 1$$

$$p_4 = bc + b + c + 1$$

$$G = G \cup \{p_4\}$$

$$FN(SP(PC(p_1, p_3)), G) = ad + a + d + 1$$

$$p_5 = ad + a + d + 1$$

$$G = G \cup \{p_5\}$$

$$\text{FN}(\text{SP}(\text{PC}(p_2, p_3)), G) = 0$$

$$\text{FN}(\text{SP}(\text{PC}(p_1, p_4)), G) = 0$$

$$\text{FN}(\text{SP}(\text{PC}(p_2, p_4)), G) = 0$$

$$\text{FN}(\text{SP}(\text{PC}(p_3, p_4)), G) = ac + a + c + 1$$

$$p_6 = ac + a + c + 1$$

$$G = G \cup \{p_6\}$$

Los restantes también son iguales a 0. Por tanto una base de Gröbner de  $I(F)$  es  $G = \{bd + b + d + 1, cd + d, ab + b, bc + b + c + 1, ad + a + d + 1, ac + a + c + 1\}$ .

#### 2.8.10.- Nota

En el ejemplo anterior hemos tenido que estudiar 15 pares y sólo 3 han dado lugar a nuevos polinomios. En el próximo párrafo trataremos de establecer criterios para eliminar pares que no producen nuevos polinomios.

**2.9.- MEJORAS DEL ALGORITMO****2.9.1.-Lema**

Sean  $p_1, p_2 \in F$ . Si  $L(p_1)$  y  $L(p_2)$  son primos entre sí, entonces  $SP(PC(p_1, p_2)) \xrightarrow{*}_F 0$ .

**Demostración**

Sea  $q = SP(PC(p_1, p_2))$ . Entonces, por 2.6.1 y 2.2.3.

$$\begin{aligned} q &= L(q_2)R(q_1) - L(q_1)R(q_2) \\ &\xrightarrow{*} o(R(q_1), L(q_2))(q) \\ &= -L(q_1)R(q_2) \\ &\xrightarrow{*} \rho(R(q_2), L(q_1))(-L(q_1)R(q_2)) \\ &= 0. \end{aligned}$$

**2.9.2.- Teorema**

$F$  es una base de Gröbner sii para todo  $p_1, p_2 \in F$  cuyos líderes no son primos entre sí,  $SP(PC(p_1, p_2)) \xrightarrow{*}_F 0$ .

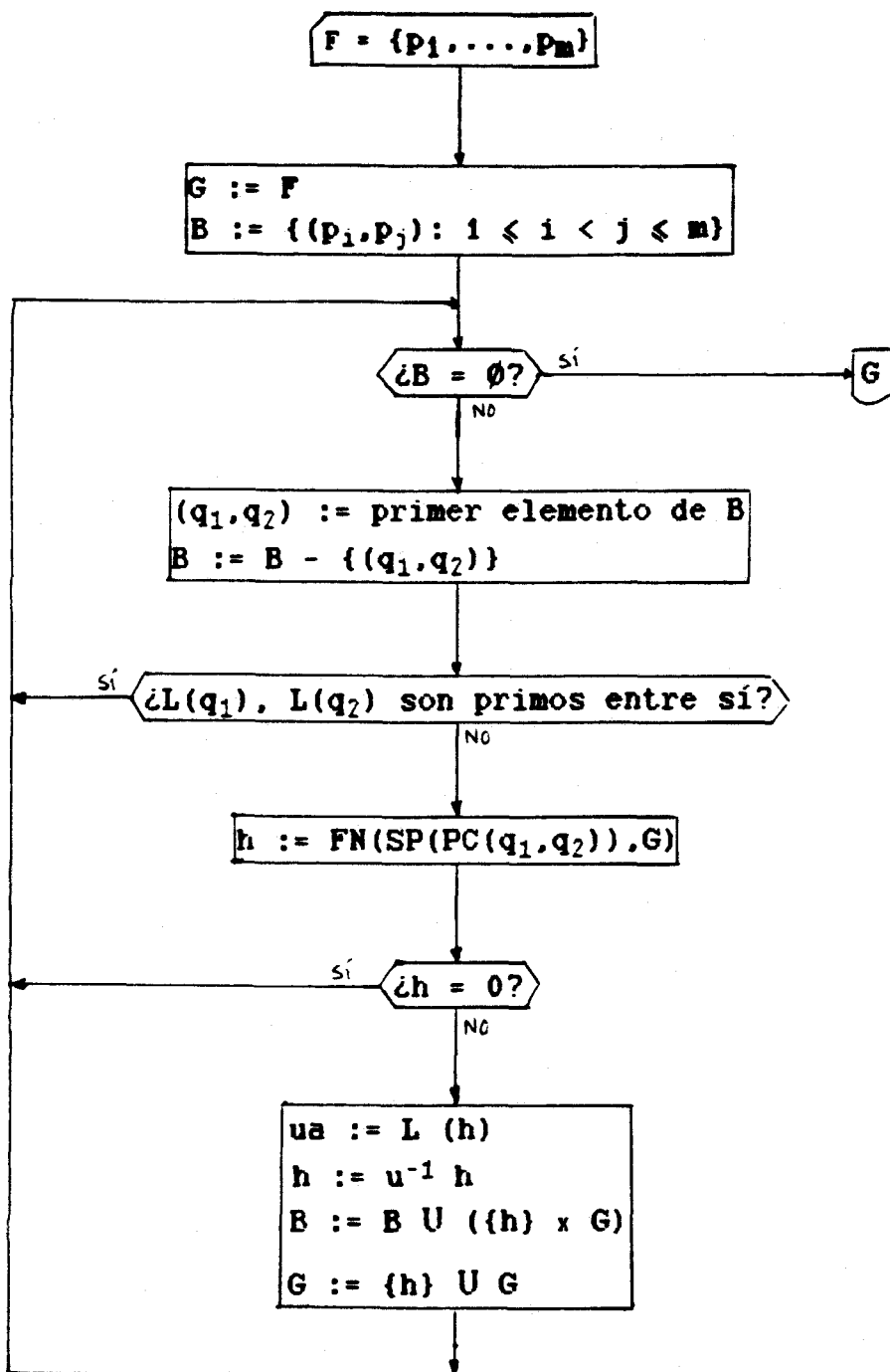
**Demostración**

( $\implies$ ) por 2.7.2.

( $\impliedby$ ) Sean  $p_1, p_2 \in F$ . Si  $L(p_1)$  y  $L(p_2)$  son primos entre sí, entonces  $SP(PC(p_1, p_2)) \xrightarrow{*}_F 0$ , por 2.9.1. Si  $L(p_1)$  y  $L(p_2)$  no son primos entre sí, entonces  $SP(PC(p_1, p_1)) \xrightarrow{*}_F 0$  por hipótesis. Luego,  $SP(PC(p_1, p_2)) \xrightarrow{*}_F 0$ . Por 2.7.2  $F$  es una base de Gröbner.

**2.9.3.- Algoritmo (2º para calcular bases de Gröbner)**

Dado  $F = \{p_1, \dots, p_n\}$ , el siguiente procedimiento



termina construyendo un  $G$  tal que  $I(F) = I(G)$  y  $G$  es una base de Gröbner.

### Demostración

Igual que la de 2.8.8, excepto que en la parte (c) se sustituye "sean  $q_1, q_2 \in G$ " por "sean  $q_1, q_2 \in G$  tales que sus líderes no son primos entre sí" y "2.7.2" por "2.9.2".

2.9.4.-Ejemplo

En el ejemplo 2.8.9, se evitan 3 reducciones: la de los pares  $(p_2, p_3)$ ,  $(p_4, p_5)$  y  $(p_1, p_6)$ .

2.9.5.- Definición

Sea  $A \subseteq Z_p[X_1, \dots, X_n]$ . El par  $(q_1, q_2)$  es AF-eliminable si se verifican las siguientes condiciones:

(a)  $q_1, q_2 \in A$

(b) Existe  $p \in F - A$  tal que  $m.c.m(L(q_1), L(q_2))$  es divisible por  $L(p)$ .

2.9.6.- Lema

Si  $q_1 \leftarrow q \rightarrow q_2$  y  $q_1 \downarrow^* q_2$ , entonces  $q_1 \leftarrow q_2$  ( $< q$ ).

Demostración

Es una consecuencia inmediata de 2.2.7.

2.9.7.-Teorema

Sea  $A \subseteq Z_p[X_1, \dots, X_n]$ .  $F$  es una base de Gröbner sii para todo  $p_1, p_2 \in F$  tales que  $PC(p_1, p_2)$  no es AF-eliminable,  $SP(PC(p_1, p_2)) \rightarrow^* 0$ .

Demostración

( $\implies$ ) Según 2.7.2.

( $\impliedby$ ) Por 2.4.3, 2.2.7 y 1.30, basta probar que para todo  $q, q_1, q_2$ :

$$q_1 \leftarrow q \rightarrow q_2 \implies q_1 \leftarrow^* q_2 \text{ (} < q \text{)}$$

Supongamos que  $q_1 \leftarrow q \rightarrow q_2$ . Existen  $p_1, p_2 \in F$ ,

$u_1, u_2 \in \mathbb{Z}_p - \{0\}$  y monomios  $a_1, a_2$  tales que  $q_1 = \rho(p_1, a_1)(q)$  y  $u_i = \text{coef}(a_i L(p_i), q)$ . Distinguimos los siguientes casos:

Caso 1:  $a_1 L(p_1) \neq a_2 L(p_2)$ :

Según 2.7.1(a) y 2.9.6,  $q_1 \langle \text{---} \rangle^* q_2 (< q)$ .

Caso 2:  $a_1 L(p_1) = a_2 L(p_2)$ :

Caso 2.1:  $(p_1, p_2)$  no es AF-eliminable:

Según 2.7.1(b) y 2.9.6,  $q_1 \langle \text{---} \rangle^* q_2 (< q)$ .

Caso 2.2:  $(p_1, p_2)$  es AF-eliminable:

Existe  $p \in F - A$  tal que  $\text{m.c.m.}(L(q_1), L(q_2))$  es divisible por  $L(p)$ . Puesto que  $a_1 L(p_1)$  es múltiplo de  $L(p_1)$  y de  $L(p_2)$ , también lo es de  $L(p)$ . Sea  $d = a_1 L(p_1)/L(p)$ . Entonces

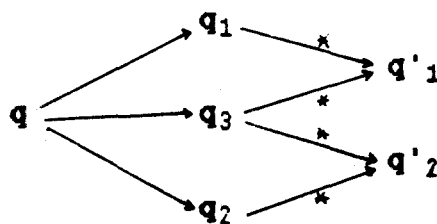
$$dL(p) = a_1 L(p_1) = a_2 L(p_2)$$

y  $\text{coef}(dL(p), q) = u_1 \neq 0$ ;

luego  $q \text{ ---} \rightarrow q_3 = \rho(p, d)(q)$ .

Para  $i \in \{1, 2\}$  tenemos:  $(p_i, p)$  no es AF-eliminable (porque  $p \in A$ ),  $q_i = \rho(p_i, a_i)(q) \langle \text{---} \rangle q \text{ ---} \rightarrow \rho(p, d)(q) = q_3$  y  $a_i L(p_i) = dL(p)$ . Aplicando el Caso 2.1, tenemos que  $q_i \downarrow^* q_3$ .

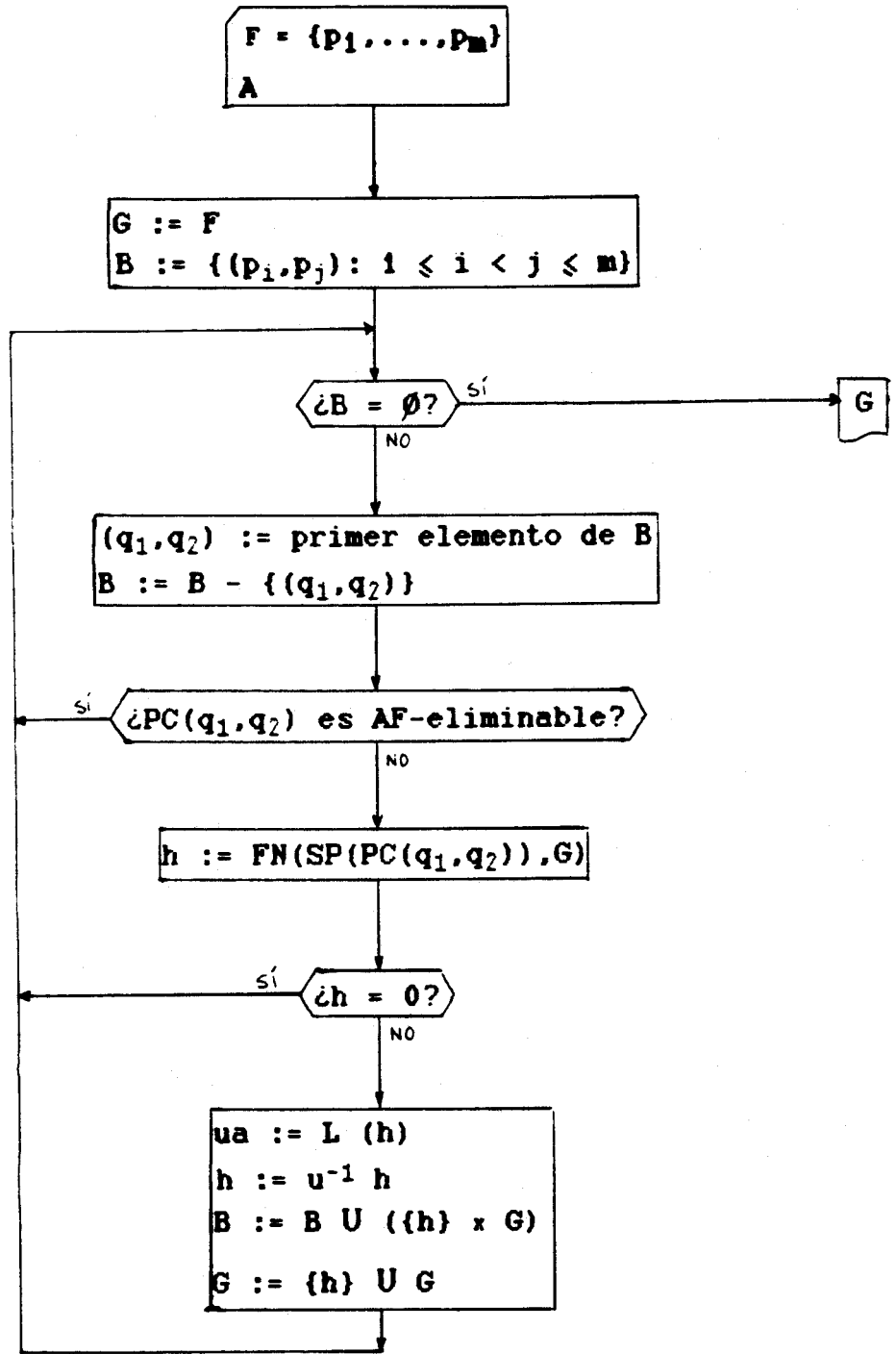
Por tanto, existen  $q'_1, q'_2$  tales que



Luego,  $q_1 \langle \text{---} \rangle^* q_2 (< q)$ .

### 2.9.8.- Algoritmo (3º para calcular bases de Gröbner)

Dados  $F = \{p_1, \dots, p_n\}$  y  $A$ , un conjunto recursivo de polinomios, el siguiente procedimiento



termina construyendo un  $G$  tal que  $I(F) = I(G)$  y  $G$  es una base de Gröbner.

**Demostración**

Igual que la de 2.8.8, excepto que en la parte (c) se sustituye "sean  $q_1, q_2 \in G$ " por "sean  $q_1, q_2 \in G$  tales que  $PC(q_1, q_2)$  no es AF-eliminable" y "2.7.2" por "2.9.7".

**2.9.9.- Ejemplo**

En el ejemplo 2.8.9, considerando el conjunto A de los polinomios distintos de  $p_1$  se evitan 4 reducciones: la de los pares  $(p_2, p_3)$ ,  $(p_2, p_4)$ ,  $(p_3, p_5)$  y  $(p_4, p_5)$ .



**2.10.- BASES DE GRÖBNER REDUCIDAS****2.10.1.- Definición**

Una base de Gröbner  $F$  es reducida si para todo  $p \in F$ ,  
 $FN(p, F - \{p\}) \neq p \neq 0$ .

**2.10.2.- Teorema**

Sean  $F$  y  $F'$  bases de Gröbner reducidas. Si  $I(F) = I(F')$   
entonces  $F = F'$ .

**Demostración**

Supongamos que  $F \neq F'$ . Sean  $F = \{p_1, \dots, p_m\}$  y  $F' = \{p'_1, \dots, p'_m\}$  donde  $p_1 < \dots < p_m$  y  $p'_1 < \dots < p'_m$ . Sea  $A = \{j \in \{1, \dots, m\} : p_j \neq p'_j\}$ .  $A \neq \emptyset$  (en caso contrario,  $FN(p'_{m+1}, F' - \{p'_{m+1}\}) = 0$ ). Sea  $i$  el menor elemento de  $A$ . Distinguimos dos casos

Caso 1:  $L(p_i) \neq L(p'_i)$

Supongamos que  $L(p_i) < L(p'_i)$ . Puesto que  $p_i \in I(F')$  y  $F'$  es una base de Gröbner,  $FN(p_i, F') = 0$ . Los únicos polinomios de  $F'$  que se pueden usar en la reducción de  $p_i$  son  $p'_1, \dots, p'_{i-1}$ . Por tanto,  $p_i$  es reducible por  $\{p_1, \dots, p_{i-1}\} = \{p'_1, \dots, p'_{i-1}\}$ . Contradicción con el ser  $F$  reducida.

Caso 2:  $L(p_i) = L(p'_i)$

$R(p_i) \neq R(p'_i)$ . Sea  $p = R(p_i) - R(p'_i)$ .  $p \in I(F)$  (porque  $p = p_i - p'_i$ ).  $FN(p, F) = 0$ . Existe un  $j < i$  y un monomio  $b$  tales que  $\text{coef}(bL(p_j), p) \neq 0$ . Pero  $\text{coef}(bL(p_j), R(p_i)) = 0$  (por ser  $F$  reducida),  $p_j = p'_j$  (por la definición de  $i$ ) y  $\text{coef}(bL(p_j), R(p'_i)) = \text{coef}(bL(p'_j), R(p'_i)) = 0$  (por ser  $F'$  reducida). Contradicción.

## CAPITULO 3

### CÁLCULOS PROPOSICIONALES

En este capítulo usamos las bases de Gröbner para resolver algorítmicamente problemas de los cálculos proposicionales.

En la primera parte estudiamos el cálculo proposicional clásico.

La sección 3.1.A contiene las definiciones del cálculo proposicional clásico que usaremos en las restantes.

En la sección 3.1.B definimos la aplicación ST que asocia un polinomio de  $Z_2[X_1, \dots, X_n]$  a cada proposición.

En la sección 3.1.C caracterizamos las tautologías (3.1.C.7), las contradicciones (3.1.C.9) e indicamos cómo obtener un modelo y un contramodelo para las contingentes (3.1.C.12).

En la sección 3.1.D construimos un isomorfismo entre el anillo booleano correspondiente al álgebra de Lindenbaum-Tarski y  $Z_2[X_1, \dots, X_n]/I$  (donde  $I$  es el ideal engendrado por  $\{X_i^2 + X_i : 1 \leq i \leq n\}$ ), damos condiciones equivalentes a  $\{P_1, \dots, P_n\} \models Q$  (3.1.D.4) y a  $\{P_1, \dots, P_n\}$  es inconsistente (3.1.D.5).

En la sección 3.1.E damos algoritmos para los problemas de deducción (3.1.E.1), inconsistencia (3.1.E.4 y 3.1.E.6) y equivalencia (3.1.E.8).

En la segunda parte estudiamos el cálculo proposicional polivalente.

La sección 3.2.A contiene las definiciones del cálculo proposicional polivalente que usaremos en las restantes, ejemplos de cálculos polivalentes y el Teorema 3.2.A.3 que permite limitarnos a cálculos con un número primo,  $p$ , de valores de verdad.

En la sección 3.2.B definimos la aplicación  $ST$  que asocia un polinomio de  $Z_p[X_1, \dots, X_n]$  a cada proposición.

En la sección 3.2.C caracterizamos las tautologías (3.2.C.6) y las contradicciones (3.2.C.8).

En la sección 3.2.D damos condiciones equivalentes a  $\{P_1, \dots, P_m\} \models Q$  (3.2.D.3) y a  $\{P_1, \dots, P_m\}$  es inconsistente (3.2.D.4) que nos permiten aplicar a los cálculos polivalentes los algoritmos de la sección 3.1.E para el cálculo clásico.

3.1.- CÁLCULO PROPOSICIONAL CLÁSICO3.1.A.- DEFINICIONES3.1.A.1.- Definición

El conjunto de las proposiciones en  $X_1, \dots, X_n$  (que lo representaremos por  $P(X_1, \dots, X_n)$ ) se define recursivamente por:

- (a) para todo  $i \in \{1, \dots, n\}$ ,  $X_i \in P(X_1, \dots, X_n)$ ;
- (b) si  $P \in P(X_1, \dots, X_n)$ , entonces  $\neg P \in P(X_1, \dots, X_n)$ ;
- (c) si  $P, Q \in P(X_1, \dots, X_n)$  y  $k \in \{v, \&, \rightarrow, \leftrightarrow\}$ , entonces  $P k Q \in P(X_1, \dots, X_n)$ .

3.1.A.2.- Notación

Usaremos las variables  $P, Q, R, \dots$  para representar los elementos de  $P(X_1, \dots, X_n)$ .

3.1.A.3.- Definición

- (a)  $H_{\neg} : Z_2 \rightarrow Z_2$  está definida por

a	$H_{\neg}(a)$
0	1
1	0

- (b) Para cada conectiva  $k \in \{v, \&, \rightarrow, \leftrightarrow\}$  la aplicación  $H_k : Z_2^2 \rightarrow Z_2$  está definida por

a	b	$H_v(a,b)$	$H_{\&}(a,b)$	$H_{\rightarrow}(a,b)$	$H_{\leftrightarrow}(a,b)$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	1	1	1	1

**3.1.A.4.- Definición**

Una valoración es una aplicación

$$v : \{X_1, \dots, X_n\} \rightarrow Z_2.$$

Para cada valoración  $v$ , la aplicación

$$V : P(X_1, \dots, X_n) \rightarrow Z_2$$

está definida por:

$$V(P) = \begin{cases} v(X_i), & \text{si } P \text{ es } X_i \text{ e } i \in \{1, \dots, n\}; \\ \neg(V(Q)), & \text{si } P \text{ es } \neg Q; \\ H_k(V(Q), V(R)), & \text{si } P \text{ es } QkR \text{ y } k \in \{v, \&, \rightarrow, \leftrightarrow\} \end{cases}$$

**3.1.A.5.- Definición**

Una proposición  $P$  es una tautología si para toda valoración  $v$ ,  $V(P) = 1$ . Por  $\models P$  indicaremos que  $P$  es una tautología.

**3.1.A.6.- Definición**

Una proposición  $Q$  es consecuencia tautológica de un conjunto de proposiciones  $\{P_1, \dots, P_m\}$  si para toda valoración  $v$

$$V(P_1) = \dots = V(P_m) = 1 \implies V(Q) = 1.$$

Por  $\{P_1, \dots, P_m\} \models Q$  indicaremos que  $Q$  es consecuencia tautológica de  $\{P_1, \dots, P_m\}$ .

**3.1.B.- POLINOMIOS ASOCIADOS A PROPOSICIONES****3.1.B.1.- Definición**

La aplicación

$$ST : P(X_1, \dots, X_n) \dashrightarrow Z_2[X_1, \dots, X_n]$$

está definida por:

$$ST(P) = \begin{cases} X_i & \text{, si } P \text{ es } X_i \text{ e } i \in \{1, \dots, n\}; \\ ST(Q)+1 & \text{, si } P \text{ es } \neg Q; \\ ST(Q) \cdot ST(R) & \text{, si } P \text{ es } Q \& R; \\ ST(Q)+ST(R)+ST(Q) \cdot ST(R) & \text{, si } P \text{ es } Q \vee R; \\ ST(Q) \cdot ST(R)+ST(Q)+1 & \text{, si } P \text{ es } Q \rightarrow R; \\ ST(Q)+ST(R)+1 & \text{, si } P \text{ es } Q \leftrightarrow R \end{cases}$$

**3.1.B.2.- Notación**

Los polinomios transformados de las proposiciones P, Q, R, ... mediante la aplicación ST los representaremos por p, q, r, ..., respectivamente.

**3.1.B.3.- Definición**

Para cada valoración v, la aplicación

$$V^* : Z_2[X_1, \dots, X_n] \dashrightarrow Z_2$$

es el homomorfismo definido por:

$$V^*(p) = \begin{cases} 1 & \text{, si } p \text{ es } 1; \\ v(X_i) & \text{, si } p \text{ es } X_i \text{ e } i \in \{1, \dots, n\}; \\ V^*(q)+V^*(r) & \text{, si } p \text{ es } Q+r; \\ V^*(q) \cdot V^*(r) & \text{, si } p \text{ es } q \cdot r. \end{cases}$$

**3.1.B.4.- Lema**

Para toda valoración  $v$ ,  $V = V^* \circ ST$ .

**Demostración**

Por inducción sobre la longitud de las proposiciones.

(a) Si  $P$  es  $X_i$  para algún  $i \in \{1, \dots, n\}$ ,

$$\begin{aligned}
 (V^* \circ ST)(P) &= V^*(ST(X_i)) = \\
 &= V^*(X_i) = && \text{[por 3.1.B.1]} \\
 &= v(X_i) = && \text{[por 3.1.B.3]} \\
 &= V(X_i) = && \text{[por 3.1.A.4]} \\
 &= V(P).
 \end{aligned}$$

(b) Si  $P$  es  $Q \ \& \ R$ ,

$$\begin{aligned}
 (V^* \circ ST)(P) &= V^*(ST(Q \ \& \ R)) = \\
 &= V^*(ST(Q) \ . \ ST(R)) = && \text{[por 3.1.B.1]} \\
 &= V^*(ST(Q)) \ . \ V^*(ST(R)) = && \text{[por 3.1.B.3]} \\
 &= V(Q) \ . \ V(R) = && \text{[por hip. ind.]} \\
 &= V(Q \ \& \ R) = && \text{[por 3.1.A.4]} \\
 &= V(P).
 \end{aligned}$$

(c) Análogamente se demuestran los restantes casos.

**3.1.C.- CARACTERIZACIÓN ALGEBRAICA DE LAS TAUTOLOGÍAS****3.1.C.1.- Notación**

En lo que sigue, usaremos las siguientes notaciones:

- .  $F = \{X_1^2 + X_1, \dots, X_n^2 + X_n\}$ ;
- .  $I = I(F)$  es el ideal generado por  $F$ ;
- .  $\text{---}\rightarrow$  es la relación de reducción definida por  $F$ .

**3.1.C.2.- Lema**

$F$  es una base de Gröbner.

**Demostración**

Por 2.9.2, ya que los líderes de los elementos de  $F$  son primos entre sí.

**3.1.C.3.- Lema**

Para toda valoración  $v$ ,

$$p \in I \implies V^*(p) = 0.$$

**Demostración**

Sea  $p \in I$ . Existen polinomios  $q_1, \dots, q_n$  tales que  $p = q_1(X_1^2 + X_1) + \dots + q_n(X_n^2 + X_n)$ . Puesto que  $V^*$  es un homomorfismo,  $V^*(p) = 0$ .

**3.1.C.4.- Lema**

Para toda valoración  $v$ ,

$$p \text{ ---}\rightarrow^* q \implies V^*(p) = V^*(q).$$

**Demostración**

$$\begin{aligned} p \text{ ---}\rightarrow^* q &\implies p = q && \text{[por 2.3.3]} \\ &\implies p - q \in I \end{aligned}$$



$$\implies V^*(p - q) = 0 \quad [\text{por 3.1.C.3}]$$

$$\implies V^*(p) = V^*(q)$$

### 3.1.C.5.- Lema

Si  $p$  es  $\implies$ -irreducible y  $p \neq 0$ , existe una valoración  $v$  tal que  $V^*(p) = 1$ .

#### Demostración

Sea  $X_1^{\alpha_1} \dots X_n^{\alpha_n}$  el menor monomio de  $p$  y  $v$  la valoración definida por  $v(X_i) = \alpha_i$  ( $1 \leq i \leq n$ ). Entonces  $V^*(p) = 1$ .

### 3.1.C.6.- Lema

$p \in I \iff$  para toda valoración  $v$ ,  $V^*(p) = 0$ .

#### Demostración

( $\implies$ ) Lema 3.1.C.3.

( $\impliedby$ ) Sea  $q = \text{FN}(p)$ . Por 2.5.1, para demostrar que  $p \in I$  basta probar que  $q = 0$ . Supongamos que  $q \neq 0$ . Por 3.1.C.5, existe una valoración  $v$  tal que  $V^*(q) = 1$ . Por 3.1.C.4,  $V^*(p) = V^*(q) = 1$ .

### 3.1.C.7. Teorema

$P$  es una tautología  $\iff \text{ST}(P) \implies^* 1$ .

#### Demostración

( $\implies$ ) Sea  $q = \text{FN}(\text{ST}(P))$ . Tenemos que probar que  $q = 1$ . Supongamos que  $q \neq 1$ . Entonces  $q + 1 \neq 0$ . Por 3.1.C.5, existe una valoración  $v$  tal que  $V^*(q + 1) = 1$ .

$$V(P) = V^*(\text{ST}(P)) = \quad [\text{por 3.1.B.4}]$$

$$= V^*(q) = \quad [\text{por 3.1.C.4}]$$

$$= V^*(q + 1) + 1 = \quad [\text{por 3.1.B.3}]$$

$$= 0.$$

Por tanto, P no es una tautología.

(<==) Sea v una valoración,

$$V(P) = V^*(ST(P)) = \quad [\text{por 3.1.B.4}]$$

$$= V^*(FN(ST(P))) = \quad [\text{por 3.1.C.4}]$$

$$= V^*(1) =$$

$$= 1.$$

Por tanto, P es una tautología.

### 3.1.C.8.- Ejemplo

Demostrar que la proposición

$$(X_1 \rightarrow X_2) \vee (X_2 \rightarrow X_1)$$

es una tautología.

#### Demostración

$$ST((X_1 \rightarrow X_2) \vee (X_2 \rightarrow X_1)) =$$

$$= ST(X_1 \rightarrow X_2) + ST(X_2 \rightarrow X_1) + ST(X_1 \rightarrow X_2)ST(X_2 \rightarrow X_1) =$$

$$= (X_1X_2 + X_1 + X_2 + 1) + (X_2X_1 + X_2 + X_1 + 1) +$$

$$(X_1X_2 + X_1 + X_2 + 1)(X_2X_1 + X_2 + X_1 + 1) =$$

$$= X_1^2 X_2^2 + X_1^2 + X_2^2 + 1 \text{ ----}>^*$$

$$\text{----}>^* 1.$$

### 3.1.C.9.- Corolario

P es una contradicción <==> ST(P) ---->^\* 0.

#### Demostración

P es una contradicción

<==>  $\neg P$  es una tautología

<==>  $FN(ST(\neg P)) = 1$  [por 3.1.C.7]

$$\langle === \rangle \text{FN}(\text{ST}(P) + 1) = 1 \quad [\text{por } 3.1.B.1]$$

$$\langle === \rangle \text{FN}(\text{ST}(P)) = 0 \quad [\text{por } 2.5.6]$$

### 3.1.C.10.- Ejemplo

Demostrar que la proposición

$$(X_1 \leftrightarrow X_2) \ \& \ (X_1 \leftrightarrow \neg X_2)$$

es una contradicción.

#### Demostración

$$\begin{aligned} & \text{ST}((X_1 \leftrightarrow X_2) \ \& \ (X_1 \leftrightarrow \neg X_2)) = \\ & = \text{ST}(X_1 \leftrightarrow X_2) \cdot \text{ST}(X_1 \leftrightarrow \neg X_2) = \\ & = (\text{ST}(X_1) + \text{ST}(X_2) + 1)(\text{ST}(X_1) + \text{ST}(\neg X_2) + 1) = \\ & = (X_1 + X_2 + 1)(X_1 + X_2 + 1 + 1) = \\ & = X_1^2 + X_2^2 + X_1 + X_2 \text{ ----}^* \\ & \text{----}^* 0. \end{aligned}$$

### 3.1.C.11.- Corolario

P es contingente  $\langle === \rangle \text{ST}(P) \not\rightarrow^* 1$  y  $\text{ST}(P) \not\rightarrow^* 0$ .

### 3.1.C.12.- Nota

Sea P una proposición contingente.

(a) Si  $X_1^{\alpha_1} \dots X_n^{\alpha_n}$  es el menor monomio de  $\text{ST}(P)$  y  $v$  es la valoración definida por  $v(X_i) = \alpha_i$  ( $1 \leq i \leq n$ ),  $V(P) = 1$ .

(b) Si  $X_1^{\beta_1} \dots X_n^{\beta_n}$  es el menor monomio de  $\text{ST}(P) + 1$  y  $v'$  es la valoración definida por  $v'(X_i) = \beta_i$  ( $1 \leq i \leq n$ ),  $V'(P) = 0$ .

### 3.1.C.13.- Ejemplo

Demostrar que la proposición

$$(X_1 \leftrightarrow X_2) \ \& \ (X_1 \leftrightarrow X_3)$$

es contingente.

Demostración

$$\begin{aligned}
 & ST((X_1 \leftrightarrow X_2) \ \& \ (X_1 \leftrightarrow X_3)) = \\
 & = ST(X_1 \leftrightarrow X_2) \cdot ST(X_1 \leftrightarrow X_3) = \\
 & = (X_1 + X_2 + 1)(X_1 + X_3 + 1) = \\
 & = X_1^2 + X_1X_2 + X_1X_3 + X_2^2 + X_2X_3 + X_3^2 + 1 \text{ ----}>^* \\
 & \text{----}>^* X_1X_2 + X_1X_3 + X_2X_3 + X_1 + X_2 + X_3 + 1.
 \end{aligned}$$

Además,

(a) si  $v$  es la valoración definida por  $v(X_1) = v(X_2) = v(X_3) = 0$ ,  $V((X_1 \leftrightarrow X_2) \ \& \ (X_1 \leftrightarrow X_3)) = 1$ ;

(b) si  $v'$  es la valoración definida por  $v'(X_1) = v'(X_2) = 0$  y  $v'(X_3) = 1$ ,  $V'((X_1 \leftrightarrow X_2) \ \& \ (X_1 \leftrightarrow X_3)) = 0$ .

**3.1.D.- CARACTERIZACIÓN ALGEBRAICA DE LA DEDUCCIÓN****3.1.D.1.- Definición**

En  $P(X_1, \dots, X_n)$  se define la relación

$P E Q$  sii para toda valoración  $v$ ,  $V(P) = V(Q)$ .

$E$  es una relación de equivalencia en  $P(X_1, \dots, X_n)$ . El conjunto cociente  $P^*(X_1, \dots, X_n) = P(X_1, \dots, X_n)/E$  con las operaciones  $+$  y  $\cdot$  definidas por:

$$[P] + [Q] = [\neg(P \leftrightarrow Q)]$$

$$[P] \cdot [Q] = [P \& Q]$$

y los elementos 0 y 1 definidos por:

$$0 = [\neg(X_1 \leftrightarrow X_1)]$$

$$1 = [X_1 \leftrightarrow X_1]$$

es un anillo booleano. Escribiremos  $B(X_1, \dots, X_n)$  en lugar de  $(P^*(X_1, \dots, X_n), +, \cdot, 0, 1)$ .

**3.1.D.2.- Lema**

Sean  $p, q \in Z_2[X_1, \dots, X_n]$ . Son equivalentes:

(a)  $p + I = q + I$ ;

(b) para toda valoración  $v$ ,  $V^*(p) = V^*(q)$ .

**Demostración**

$$p + I = q + I \iff$$

$$\iff p - q \in I$$

$$\iff \text{para toda } v, V^*(p - q) = 0 \quad \text{[por 3.1.C.6]}$$

$$\iff \text{para toda } v, V^*(p) = V^*(q). \quad \text{[por 3.1.B.3]}$$

3.1.D.3.- Teorema

La aplicación

$$ST': B(X_1, \dots, X_n) \longrightarrow Z_2[X_1, \dots, X_n]/I$$

definida por

$$ST'([P]) = ST(P) + I$$

es un isomorfismo de anillos.

Demostración

(a)  $ST'$  es una aplicación inyectiva:

$$[P] = [Q] \iff$$

$$\iff \text{para toda } v, V(P) = V(Q) \quad [\text{por 3.1.D.1}]$$

$$\iff \text{para toda } v, V^*(ST(P)) = V^*(ST(Q)) \quad [\text{por 3.1.B.4}]$$

$$\iff ST(P) + I = ST(Q) + I \quad [\text{por 3.1.D.2}]$$

(b)  $ST'$  es suprayectiva:

Basta comprobar que si definimos

$$ST'': Z_2[X_1, \dots, X_n] \longrightarrow P(X_1, \dots, X_n)$$

por:

$$ST''(p) = \begin{cases} X_i & , \text{si } p \text{ es } X_i \text{ e } i \in \{1, \dots, n\}; \\ X_1 \leftrightarrow X_1 & , \text{si } p \text{ es } 1; \\ \neg(ST''(q) \leftrightarrow ST''(r)) & , \text{si } p \text{ es } q + r; \\ ST''(q) \& ST''(r) & , \text{si } p \text{ es } q.r; \end{cases}$$

se tiene  $ST(ST''(p)) + I = p + I$  para todo  $p \in Z_2[X_1, \dots, X_n]$ ,

lo que garantiza la suprayectividad de  $ST'$ . Lo comprobaremos

por inducción sobre la formación de los polinomios:

(b.1) Si  $p$  es 1,

$$ST(ST''(p)) + I =$$

$$= ST(ST''(1)) + I =$$

$$= ST(X_1 \leftrightarrow X_1) + I =$$

$$= (X_1 + X_1 + 1) + I = \quad [\text{por 3.1.B.1}]$$

$$= 1 + I =$$

$$= p + I.$$

(b.2) Si  $p$  es  $X_i$  para algún  $i \in \{1, \dots, n\}$ .

$$ST(ST''(p)) + I =$$

$$= ST(ST''(X_i)) + I =$$

$$= ST(X_i) + I =$$

$$= X_i + I =$$

[por 3.1.B.1]

$$= p + I.$$

(b.3) Si  $p$  es  $q + r$ .

$$ST(ST'(p)) + I =$$

$$= ST(ST''(q + r)) + I =$$

$$= ST(\neg(ST''(q) \leftrightarrow ST''(r))) + I =$$

$$= (ST(ST''(q)) + ST(ST''(r))) + I = \text{ [por 3.1.B.1]}$$

$$= (ST(ST''(q)) + I) + (ST(ST''(r)) + I) =$$

$$= (q + I) + (r + I) =$$

[por hip. ind.]

$$= (q + r) + I =$$

$$= p + I.$$

(b.4) Si  $p$  es  $q.r$ .

$$ST(ST''(p)) + I =$$

$$= ST(ST''(q.r)) + I =$$

$$= ST(ST''(q) \& ST''(r)) + I =$$

$$= (ST(ST''(q)) \cdot ST(ST''(r))) + I = \text{ [por 3.1.B.1]}$$

$$= (ST(ST''(q)) + I) \cdot (ST(ST''(r)) + I) =$$

$$= (q + I) \cdot (r + I) =$$

[por hip. ind.]

$$= (q.r) + I =$$

$$= p + I.$$

(c)  $ST'$  es un homomorfismo de anillos:

$$\begin{aligned}
 ST'([P] + [Q]) &= \\
 &= ST'([\neg(P \leftrightarrow Q)]) = && \text{[por 3.1.D.1]} \\
 &= ST(\neg(P \leftrightarrow Q)) + I = \\
 &= (ST(P \leftrightarrow Q) + 1) + I = && \text{[por 3.1.B.1]} \\
 &= (ST(P) + ST(Q) + 1 + 1) + I = && \text{[por 3.1.B.1]} \\
 &= (ST(P) + I) + (ST(Q) + I) = \\
 &= ST'([P]) + ST'([Q]).
 \end{aligned}$$

$$\begin{aligned}
 ST'([P] \cdot [Q]) &= \\
 &= ST'([P \& Q]) = && \text{[por 3.1.D.1]} \\
 &= ST(P \& Q) + I = \\
 &= (ST(P) \cdot ST(Q)) + I = && \text{[por 3.1.B.1]} \\
 &= (ST(P) + I) \cdot (ST(Q) + I) = \\
 &= ST'([P]) \cdot ST'([Q]).
 \end{aligned}$$

$$\begin{aligned}
 ST'(1) &= \\
 &= ST'([X_1 \leftrightarrow X_1]) = && \text{[por 3.1.D.1]} \\
 &= ST(X_1 \leftrightarrow X_1) + I = \\
 &= (X_1 + X_1 + 1) + I = && \text{[por 3.1.B.1]} \\
 &= 1 + I.
 \end{aligned}$$

#### 3.1.D.4.- Teorema

Las siguientes condiciones son equivalentes:

(a)  $\{P_1, \dots, P_m\} \models Q$ .

(b)  $ST(Q)+1 \in (ST(P_1)+1, \dots, ST(P_m)+1, X_1^2 + X_1, \dots, X_n^2 + X_n)$ .

#### Demostración

El Teorema es una consecuencia de los siguientes Lemas.



Lema I  $((p_1 \dots p_n + 1) + I) = ((p_1+1) + I, \dots, (p_n+1) + I)$   
 [ideales de  $Z_2[X_1, \dots, X_n]/I$  engendrados respectivamente por  
 $(p_1 \dots p_n + 1) + I$  y  $((p_1+1) + I, \dots, (p_n+1) + I)$ ].

Lema II Son equivalentes:

(a)  $p_1 \dots p_n(q + 1) + I = I$

(b)  $(q + 1) + I \in ((p_1 \dots p_n + 1) + I)$  [ideal de  
 $Z_2[X_1, \dots, X_n]/I$  engendrado por  $(p_1 \dots p_n + 1) + I$ ].

Lema III

$ST'([P_1 \ \& \ \dots \ \& \ P_n \ \rightarrow \ Q]) = (p_1 \dots p_n q + p_1 \dots p_n + 1) + I$ .  
 [siendo  $p_i = ST(P_i)$  y  $q = ST(Q)$ ].

Demostración del Teorema

$\{P_1, \dots, P_n\} \models Q \iff$

$\iff P_1 \ \& \ \dots \ \& \ P_n \ \rightarrow \ Q$  es una tautología

$\iff [P_1 \ \& \ \dots \ \& \ P_n \ \rightarrow \ Q] = 1$

$\iff ST'([P_1 \ \& \ \dots \ \& \ P_n \ \rightarrow \ Q]) = ST'(1)$

$\iff (p_1 \dots p_n q + p_1 \dots p_n + 1) + I = 1 + I$  [por Lema III]

$\iff p_1 \dots p_n(q + 1) + I = I$

$\iff (q + 1) + I \in ((p_1 \dots p_n + 1) + I)$  [por Lema II]

$\iff (q + 1) + I \in (p_1 + 1 + I, \dots, p_n + 1 + I)$  [por Lema I]

$\iff$  existen  $r_1 + I, \dots, r_n + I$  tales que

$$(q+1)+I = (r_1+I)((p_1+1)+I) + \dots + (r_n+I)((p_n+1)+I)$$

$\iff$  existen  $r_1, \dots, r_n, s_1, \dots, s_n$  tales que

$$q+1 = r_1(p_1+1) + \dots + r_n(p_n+1) + s_1(X_1^2+X_1) + \dots + s_n(X_n^2+X_n)$$

$\iff q + 1 \in (p_1 + 1, \dots, p_n + 1, X_1^2 + X_1, \dots, X_n^2 + X_n)$

$\iff ST(Q)+1 \in (ST(P_1)+1, \dots, ST(P_n)+1, X_1^2+X_1, \dots, X_n^2+X_n)$ .

Demostración del Lema I

Para todo  $i \in \{1, \dots, m\}$ ,

$$\begin{aligned} (p_i + 1) + I &= ((p_i + 1) + I)((p_1 \dots p_m + 1) + I) \\ &\in ((p_1 \dots p_m + 1) + I). \end{aligned}$$

Luego,  $((p_1 + 1) + I, \dots, (p_m + 1) + I) \subseteq ((p_1 \dots p_m + 1) + I)$ .

Demostremos la otra inclusión por inducción sobre  $m$ :

Para  $k = 1$ : evidentemente  $((p_1 + 1) + I) \subseteq ((p_1 + 1) + I)$ .

Para  $k = m$ :

$$\begin{aligned} (p_1 \dots p_m + 1) + I &= \\ &= ((p_m + 1) + I)((p_1 \dots p_{m-1} + 1) + I) + ((p_m + 1) + I) \in \\ &\in ((p_1 \dots p_{m-1} + 1) + I, (p_m + 1) + I) \subseteq \\ &\subseteq ((p_1 + 1) + I, \dots, (p_m + 1) + I) \quad [\text{por hip. ind.}] \end{aligned}$$

Demostración del Lema II

( $\implies$ ) Si  $p_1 \dots p_m(q + 1) + I = I$ , entonces

$$\begin{aligned} (q + 1) + I &= ((q + 1) + I)((p_1 \dots p_m + 1) + I) \\ &\in ((p_1 \dots p_m + 1) + I). \end{aligned}$$

( $\impliedby$ ) Si  $(q + 1) + I \in ((p_1 \dots p_m + 1) + I)$ , existe un  $r$  tal que  $(q + 1) + I = r((p_1 \dots p_m + 1) + I)$ . Por tanto,

$$p_1 \dots p_m(q + 1) + I = I.$$

Demostración del Lema III

Por inducción sobre  $m$ .

3.1.D.5.- Corolario

Las siguientes condiciones son equivalentes:

(a)  $\{P_1, \dots, P_m\}$  es inconsistente;

(b)  $1 \in (\text{ST}(P_1) + 1, \dots, \text{ST}(P_m) + 1, X_1^2 + X_1, \dots, X_n^2 + X_n)$ .

Demostración

$\{P_1, \dots, P_m\}$  es inconsistente  $\iff$

$\iff \{P_1, \dots, P_m\} \models X_1 \leftrightarrow \neg X_1$

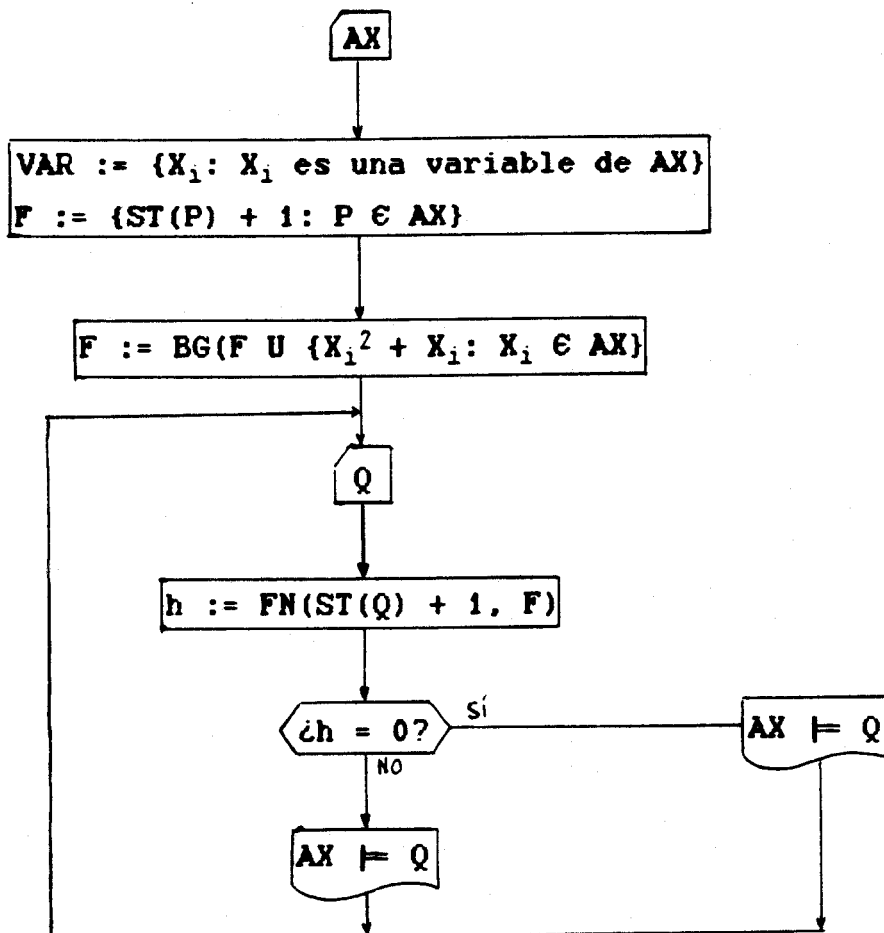
$\iff \text{ST}(X_1 \leftrightarrow \neg X_1) + 1 \in (\text{ST}(P_1) + 1, \dots, \text{ST}(P_m) + 1,$

$X_1^2 + X_1, \dots, X_n^2 + X_n)$  [por 3.1.D.4]

$\iff 1 \in (\text{ST}(P_1) + 1, \dots, \text{ST}(P_m) + 1, X_1^2 + X_1, \dots, X_n^2 + X_n)$

**3.1.E.- ALGORITMOS DE DEDUCCIÓN****3.1.E.1.- Algoritmo**

Dado el conjunto de proposiciones  $AX = \{P_1, \dots, P_n\}$ , para cada proposición  $Q$ , el siguiente procedimiento



termina determinando si  $Q$  es consecuencia lógica de  $AX$  o no lo es.

**Demostración**

Es consecuencia inmediata del Teorema 3.1.D.4 y del Corolario 2.5.4.

**3.1.E.2.- Ejemplo**

Dado el conjunto de axiomas

$$AX = \{a \rightarrow b, b \rightarrow e, c \vee d, \neg(c \& d)\},$$

determinar si las proposiciones

$$\neg e \rightarrow \neg a \& \neg b \quad y$$

$$a \rightarrow (b \leftrightarrow c)$$

son consecuencias de AX.

### Demostración

Los polinomios correspondientes a los elementos de AX son:

$$p_1 = ST(a \rightarrow b) = ab + a + 1$$

$$p_2 = ST(b \rightarrow e) = be + b + 1$$

$$p_3 = ST(c \vee d) = cd + c + d$$

$$p_4 = ST(\neg(c \& d)) = cd + 1$$

La base de Gröbner reducida del ideal engendrado por

$$\{p_1 + 1, p_2 + 1, p_3 + 1, p_4 + 1,$$

$$a^2 + a, b^2 + b, c^2 + c, d^2 + d, e^2 + e\}$$

es

$$F = \{ae + a, be + b, ab + a, c + d + 1,$$

$$a^2 + a, b^2 + b, d^2 + d, e^2 + e\}$$

El polinomio correspondiente a la primera fórmula es

$$q_1 = ST(\neg e \rightarrow \neg a \& \neg b)$$

$$= abe + ab + ae + be + a + b + 1.$$

Puesto que la forma normal de  $q_1 + 1$  respecto de F es 0,

$\neg e \rightarrow \neg a \& \neg b$  es consecuencia de AX.

El polinomio correspondiente a la segunda fórmula es

$$q_2 = ST(a \rightarrow (b \leftrightarrow c)) =$$

$$= ab + ac + 1.$$

Puesto que la forma normal de  $q_2 + 1$  respecto de F es ad,

$a \rightarrow (b \leftrightarrow c)$  no es consecuencia de AX.

**3.1.E.3.- Notas**

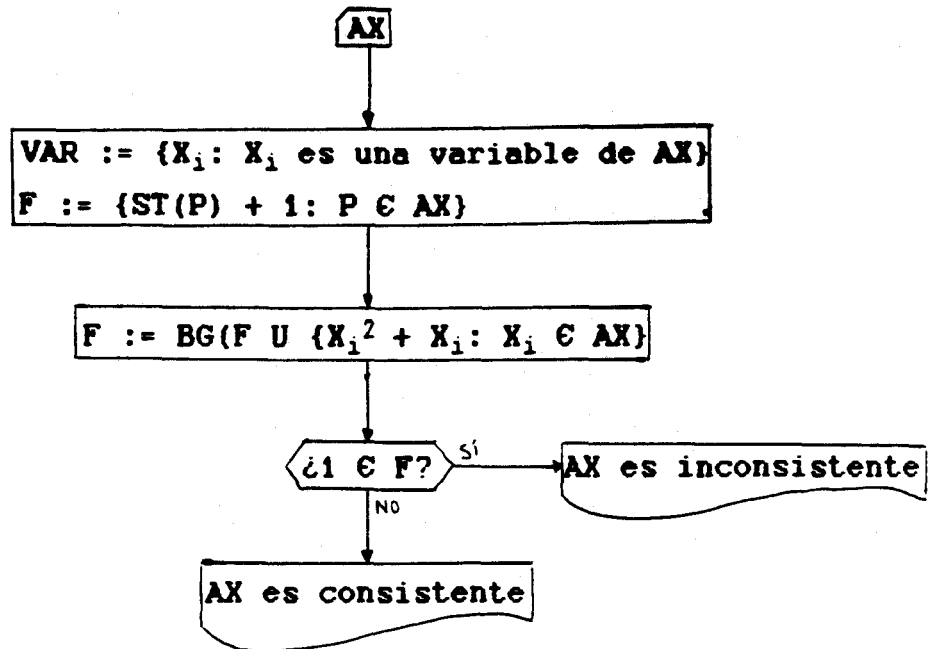
De las diferencias existentes entre la deducción mediante el procedimiento anterior y el método de resolución de Robinson, señalamos las siguientes:

(a) mientras que en el método de resolución las fórmulas tienen que estar en forma de cláusulas, en el procedimiento anterior pueden estar en la forma usual.

(b) El procedimiento de resolución es igual de complejo que el cálculo de una base de Gröbner. El algoritmo anterior, al calcular la base de Gröbner "compila" los axiomas; así, el cambio de la proposición  $Q$  no obliga a rehacer los cálculos; mientras que el método de resolución tiene que rehacer todo el proceso cada vez que se cambia la fórmula  $Q$ .

**3.1.E.4.- Algoritmo (de inconsistencia)**

Dado el conjunto de proposiciones  $AX = \{P_1, \dots, P_n\}$ , el siguiente procedimiento:



termina determinando si AX es consistente o no.

### Demostración

Es consecuencia inmediata del Corolario 3.1.D.5 y del Corolario 2.5.4.

### 3.1.E.5.- Ejemplo

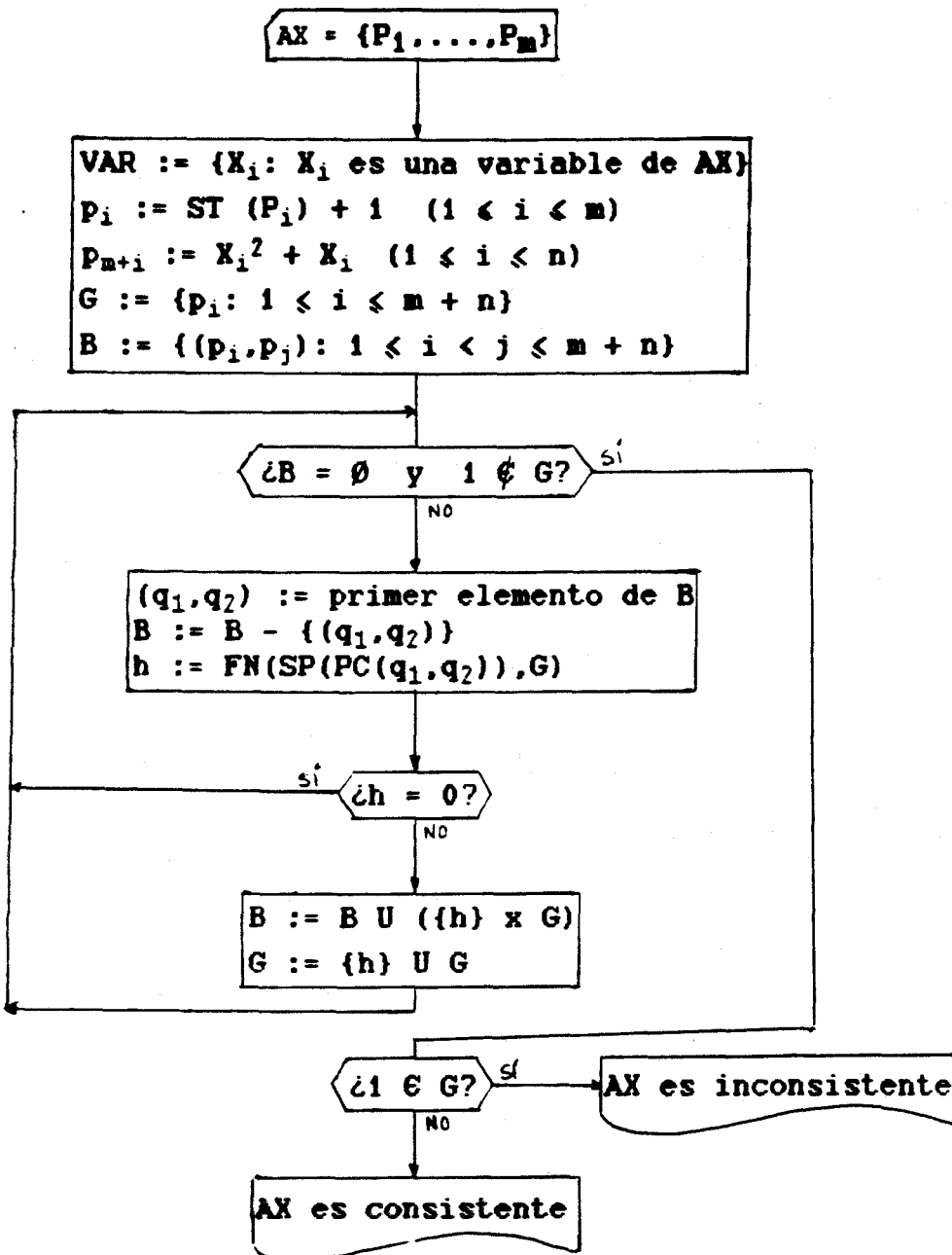
Aplicando el algoritmo anterior al conjunto de axiomas

$$AX = \{b \rightarrow a \ \& \ b, \neg c \vee b, \neg a * \neg d, c \ \& \ d\}$$

obtenemos que AX es inconsistente.

### 3.1.E.6.- Nota

Para determinar si un conjunto es consistente no es necesario calcular la base de Gröbner, podemos hacerlo mediante el siguiente algoritmo



termina determinando si el conjunto AX es consistente o inconsistente.

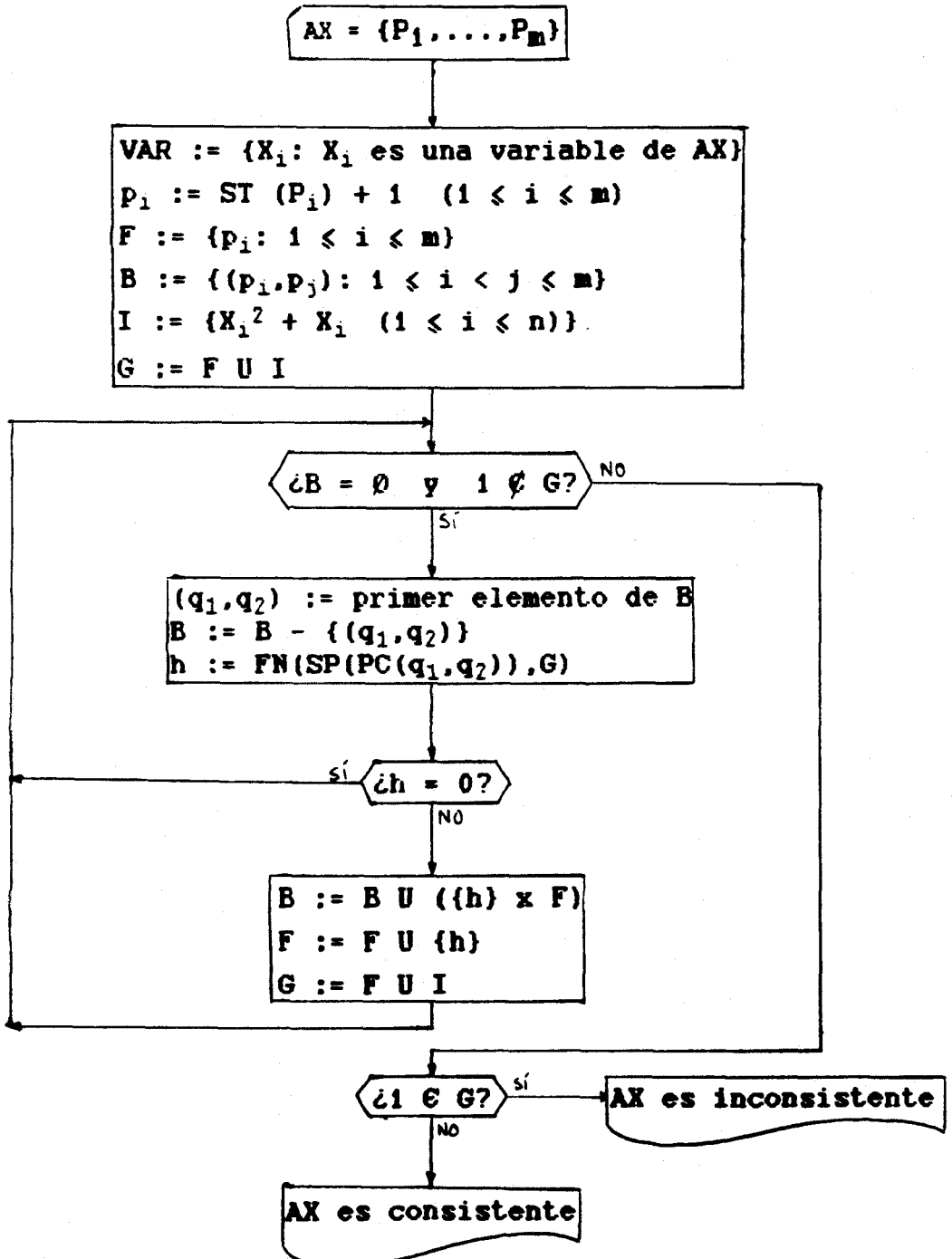
#### Demostración

Es una consecuencia inmediata del Corolario 3.1.D.5, 2.8.8 y 2.5.4.



**3.1.E.7.- Nota**

En el algoritmo anterior no es suficiente usar los polinomios  $X_i^2 + X_i$  para reducir, es necesario usarlos para formar pares críticos; es decir, el siguiente procedimiento para determinar si el conjunto de axiomas AX es consistente es incorrecto



Demostración

Sea  $AX = \{ X_1 \& X_2, \neg X_1 \& X_3 \}$ . El conjunto  $AX$  es inconsistente pero aplicándole al algoritmo anterior obtenemos

$$p_1 = ST(X_1 \& X_2) + 1 =$$

$$= X_1 X_2 + 1$$

$$p_2 = ST(\neg X_1 \& X_3) + 1 =$$

$$= X_1 X_3 + X_3 + 1$$

$$G = \{p_1, p_2\} \cup \{X_i^2 + X_i : 1 \leq i \leq 3\}$$

$$h_1 = FN(SP(PC(p_1, p_2), G)) =$$

$$= X_2 X_3 + X_2 + X_3$$

$$G = G \cup \{h_1\}$$

$$FN(SP(PC(p_1, h_1), G)) = 0$$

$$FN(SP(PC(p_2, h_1), G)) = 0$$

Puesto que  $1 \notin G$ , el algoritmo da como resultado " $AX$  es consistente". En cambio, aplicando el Algoritmo 3.1.E.6, obtenemos  $p_1$  y  $p_2$  como antes,

$$p_{2+i} = X_i^2 + X_i \quad (1 \leq i \leq 3)$$

$$G = \{p_i : 1 \leq i \leq 5\}$$

$$h_1 = FN(SP(PC(p_1, p_2), G)) = X_2 X_3 + X_2 + X_3$$

$$G = G \cup \{h_1\}$$

$$h_2 = FN(SP(PC(p_1, p_3), G)) = X_1 + 1$$

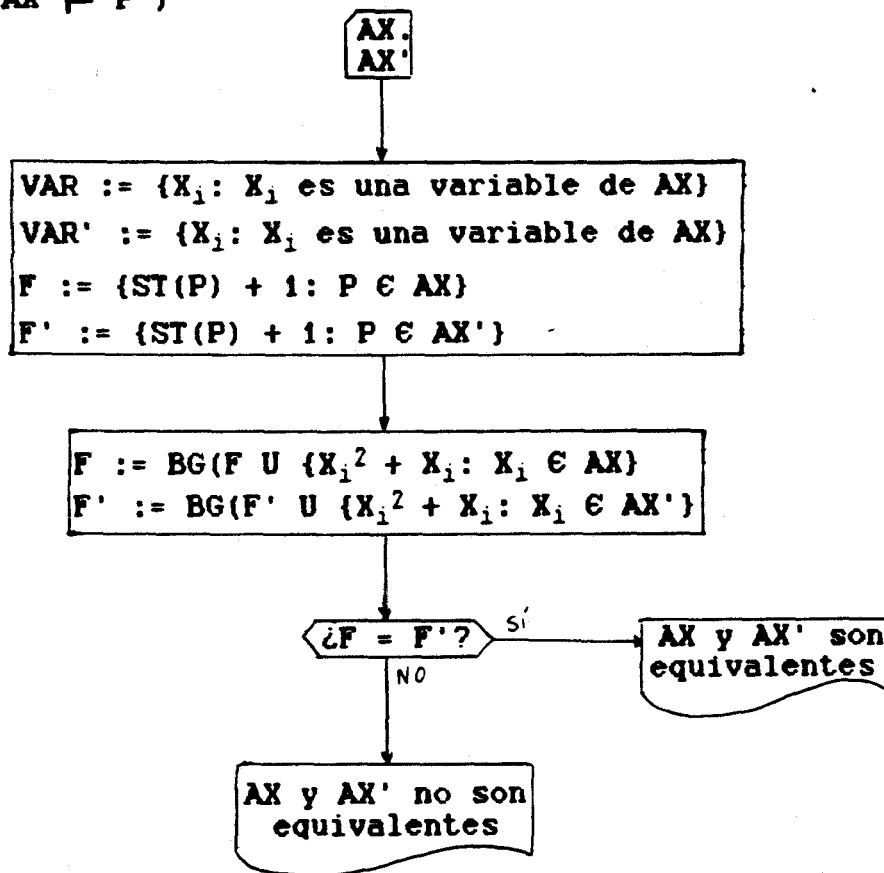
$$G = G \cup \{h_2\}$$

$$h_3 = FN(SP(PC(p_2, h_2), G)) = 1$$

Por tanto, " $AX$  es consistente".

**3.1.E.8.- Algoritmo (de equivalencia)**

Dados dos conjuntos de axiomas  $AX$  y  $AX'$  el siguiente procedimiento decide si los conjuntos  $AX$  y  $AX'$  son equivalentes (es decir, si para todo  $P \in AX$ ,  $AX' \models P$  y para todo  $P' \in AX'$ ,  $AX \models P'$ )

**3.1.E.9.- Ejemplo**

Dado el conjunto de axiomas

$$AX = \{ \neg e \rightarrow (\neg a \ \& \ \neg b \ \& \ (c \vee d)),$$

$$a \ \& \ (\neg b \vee \neg c) \rightarrow d,$$

$$\neg b \rightarrow \neg a,$$

$$c \leftrightarrow \neg d),$$

Los polinomios correspondientes a los elementos de  $AX$  son:

$$p_1 = ST(\neg e \rightarrow (\neg a \ \& \ \neg b \ \& \ (c \vee d))) =$$

$$= abcde + abcd + abce + abde + acde + bcde + abc + abd + acd + ace + ade + bcd + bce + bde + cde + ac + ad + bc + bd + cd + ce + de + c + d + e$$

$$p_2 = ST(a \& (\neg b \vee \neg c) \rightarrow d) =$$

$$= abcd + abc + ad + a + 1$$

$$p_3 = ST(\neg b \rightarrow \neg a) =$$

$$= ab + a + 1$$

$$p_4 = ST(c \leftrightarrow \neg d) =$$

$$= c + d.$$

La base de Gröbner reducida del ideal generado por

$$\{p_1 + 1, p_2 + 1, p_3 + 1, p_4 + 1,$$

$$a^2 + a, b^2 + b, c^2 + c, d^2 + d, e^2 + e\}$$

es

$$F = \{ae + a, be + b, ab + a, c + d + 1,$$

$$a^2 + a, b^2 + b, d^2 + d, e^2 + e\}$$

Puesto que F coincide con la base de Gröbner reducida obtenida en el Ejemplo 3.1.E.2, los conjuntos de axiomas

$$AX = \{\neg e \rightarrow (\neg a \& \neg b \& (c \vee d)),$$

$$a \& (\neg b \vee \neg c) \rightarrow d,$$

$$\neg b \rightarrow \neg a,$$

$$c \leftrightarrow \neg d\},$$

y

$$AX' = \{a \rightarrow b, b \rightarrow e, c \vee d, \neg(c \& d)\},$$

son equivalentes.

3.2.- CÁLCULO PROPOSICIONAL POLIVALENTE3.2.A.- DEFINICIONES3.2.A.1.- Definición

Dado un conjunto finito de variables, VAR; un conjunto finito de conectivas, CON, (disjunto con el anterior) y una función de aridad,  $ar : CON \rightarrow \mathbb{N}$ , se define el conjunto de proposiciones  $P(VAR, CON)$  recursivamente como sigue:

(a) Si  $X \in VAR$ , entonces  $X \in P(VAR, CON)$ .

(b) Si  $k \in CON$ ,  $m = ar(k)$  y  $P_1, \dots, P_m \in P(VAR, CON)$ ,

entonces  $k(P_1, \dots, P_m) \in P(VAR, CON)$ .

Usaremos las letras  $X_1, \dots, X_n$  para representar los elementos de VAR y las letras P, Q, R, ... para representar los elementos de  $P(VAR, CON)$ .

En lo que sigue  $r$  es un número entero mayor que 1.

Vamos a definir un Cálculo Proposicional  $r$ -valente.

Para cada conectiva  $k$  está definida una función

$H_k : Z_r^{ar(k)} \rightarrow Z_r$  (la tabla de verdad de la conectiva  $k$ ).

Una valoración de verdad es una aplicación

$$v : VAR \rightarrow Z_r$$

Para cada valoración  $v$ , la aplicación

$$V : P_{CON, ar}(VAR) \rightarrow Z_r$$

está definida por

$$V(P) = \begin{cases} v(X), & \text{si } X \in VAR \\ H_k(V(P_1), \dots, V(P_{ar(k)})), & \text{si } P \text{ es } k(P_1, \dots, P_{ar(k)}) \end{cases}$$

Una proposición  $P$  es una tautología si para toda valoración  $v$ ,  $V(P) = 1$ .

Una proposición  $Q$  es una consecuencia tautológica de un conjunto de proposiciones  $\{P_1, \dots, P_m\}$  si para toda valoración  $v$ ,

$$V(P_1) = \dots = V(P_m) = 1 \implies V(Q) = 1$$

Por  $\{P_1, \dots, P_m\} \models Q$  indicaremos que  $Q$  es una consecuencia tautológica de  $\{P_1, \dots, P_m\}$ .

**3.2.A.2.- Ejemplos**

(a) El cálculo trivalente de Lukasiewicz tiene la conectiva monaria  $\sim$  y las conectivas binarias  $\vee, \&$ ,  $\rightarrow$  y  $\leftrightarrow$ . Las correspondientes tablas de verdad son:

a	$H_{\sim}(a)$	$H_{\vee}$			$H_{\&}$			$H_{\rightarrow}$			$H_{\leftrightarrow}$			
		a\b	0	1	2	0	1	2	0	1	2	0	1	2
0	1	0	0	1	2	0	0	0	1	1	1	1	0	2
1	0	1	1	1	1	0	1	2	0	1	2	0	1	2
2	2	2	2	1	2	0	2	2	2	1	1	2	2	1

(b) El cálculo modal trivalente de Lukasiewicz, se obtiene añadiéndole al anterior las conectivas monarias  $L$  y  $M$  y las tablas de verdad

a	$H_L(a)$	$H_M(a)$
0	0	0
1	1	1
2	0	1

Las fórmulas LP y MP se interpretan por "P es necesaria" y "P es posible", respectivamente.

(d) El cálculo trivalente de Gödel tiene las conectiva monaria  $\neg$  y las conectivas binarias  $\vee$ ,  $\&$ ,  $\rightarrow$  y  $\leftrightarrow$ . Las correspondientes tablas de verdad son:

a	$H_{\neg}(a)$	$H_{\vee}$			$H_{\&}$			$H_{\rightarrow}$			$H_{\leftrightarrow}$			
		a\b	0	1	2	0	1	2	0	1	2	0	1	2
0	1	0	0	1	2	0	0	0	1	1	1	1	0	0
1	0	1	1	1	1	0	1	2	0	1	2	0	1	2
2	0	2	2	1	2	0	2	2	0	1	1	0	2	1

(d) El cálculo r-valente de Lukasiewicz tiene el mismo conjunto de conectivas que el trivalente y sus tablas de verdad se definen por:

$$H_{\neg}(a) = r - a + 1;$$

$$H_{\vee}(a,b) = \min(a, b);$$

$$H_{\&}(a,b) = \max(a, b);$$

$$H_{\rightarrow}(a,b) = \begin{cases} 1, & \text{si } a \geq b, \\ 1 + b - a, & \text{si } a < b; \end{cases}$$

$$H_{\leftrightarrow}(a,b) = 1 + |a - b|;$$

(d) El cálculo r-valente de Gödel tiene el mismo conjunto de conectivas que el trivalente y sus tablas de verdad se definen por:

$$H_{\neg}(a) = \begin{cases} 1, & \text{si } a = r \\ r, & \text{si } a \neq r; \end{cases}$$

$$H_{\vee}(a,b) = \min(a, b);$$

$$H_{\>}(a,b) = \text{máx}(a, b);$$

$$H_{\>}(a,b) = \begin{cases} 1, & \text{si } a \geq b, \\ b, & \text{si } a < b; \end{cases}$$

$$H_{\leq}(a,b) = \begin{cases} 1, & \text{si } a = b, \\ \text{máx}(a, b), & \text{si } a \neq b; \end{cases}$$

### 3.2.A.3.- Teorema

Sea  $P$  un cálculo proposicional  $r$ -valente,  $p$  un entero mayor que  $r$  y  $P'$  el cálculo proposicional  $p$ -valente que tiene el mismo lenguaje que  $P$  y la tabla de verdad de cada conectiva  $k$ ,  $H'_k : Z_p^{\text{ar}(k)} \rightarrow Z_p$ , está definida por

$$H'_k(u_1, \dots, u_{\text{ar}(k)}) = H_k(u'_1, \dots, u'_{\text{ar}(k)})$$

donde  $H_k$  es la tabla de verdad de  $k$  en  $P$  y  $u'_i = \min(u_i, r-1)$

Entonces una proposición  $P$  es una tautología en  $P$  sii lo es en  $P'$ .

### 3.2.A.4.- Nota

En lo que sigue nos limitaremos a estudiar los cálculos proposicionales con un número primo de valores de verdad y en el caso de un número compuesto,  $r$ , de valores de verdad lo que hacemos es buscar el menor primo mayor o igual que  $r$  y extender el cálculo como en el Teorema anterior.



**3.2.B.- POLINOMIOS ASOCIADOS A PROPOSICIONES****3.2.B.1.- Notación**

En lo que sigue, usaremos las siguientes notaciones:

- $p$  es un número primo,
- $P_p(X_1, \dots, X_n)$  es un cálculo proposicional  $p$ -valente en las variables  $X_1, \dots, X_n$ ,
- $Z_p[X_1, \dots, X_n]$  es el anillo de los polinomios en  $X_1, \dots, X_n$  con coeficientes en  $Z_p$ .

**3.2.B.2.- Definición**

Para cada conectiva  $k$  de aridad  $r$  la aplicación

$$ST_k : (Z_p[X_1, \dots, X_n])^r \dashrightarrow Z_p[X_1, \dots, X_n]$$

está definida por:

$$ST_k(q_1, \dots, q_r) = \sum_{\substack{0 \leq i_1 \leq p-1 \\ \dots \\ 0 \leq i_r \leq p-1}} H_k(i_1, \dots, i_r) \prod_{m=1}^r \prod_{\substack{j=0 \\ j \neq i_m}}^{p-1} (q_m - j)^{(i_m - j)},$$

**3.2.B.3.- Ejemplos**

(a) En el cálculo trivalente de Lukasiewicz, las funciones  $ST_k$  son:

$$ST_{\neg}(a) = 2a + 1,$$

$$ST_{\vee}(a, b) = 2a^2 b^2 + a^2 b + ab^2 + ab + a + b,$$

$$ST_{\&}(a, b) = a^2 b^2 + 2a^2 b + 2ab^2 + 2ab,$$

$$ST_{\rightarrow}(a, b) = a^2 b^2 + 2a^2 b + 2ab^2 + 2ab + 2a + 1,$$

$$ST_{\leftarrow}(a, b) = 2a^2 b^2 + a^2 b + ab^2 + ab + 2a + 2b + 1.$$

[donde  $a, b \in Z_3[X_1, \dots, X_n]$  y las operaciones se realizan en  $Z_3[X_1, \dots, X_n]$ ].

(b) En el cálculo modal trivalente de Lukasiewicz, las funciones  $ST_k$  son, además de las anteriores:

$$ST_I(a) = 2a^2 + 2a,$$

$$ST_M(a) = a^2.$$

[donde  $a \in Z_3[X_1, \dots, X_n]$  y las operaciones se realizan en  $Z_3[X_1, \dots, X_n]$ ].

(c) En el cálculo trivalente de Gödel, las funciones  $ST_k$  son:

$$ST_{\neg}(a) = 2a^2 + 1,$$

$$ST_{\vee}(a,b) = 2a^2 b^2 + a^2 b + ab^2 + ab + a + b,$$

$$ST_{\&}(a,b) = a^2 b^2 + 2a^2 b + 2ab^2 + 2ab,$$

$$ST_{\supset}(a,b) = 2a^2 b^2 + 2a^2 b + ab^2 + 2a^2 + 2ab + 1,$$

$$ST_{\langle \cdot \rangle}(a,b) = a^2 b^2 + 2a^2 + ab + 2b^2 + 1.$$

[donde  $a, b \in Z_3[X_1, \dots, X_n]$  y las operaciones se realizan en  $Z_3[X_1, \dots, X_n]$ ].

#### 3.2.B.4.- Nota

Si  $k$  es una conectiva y  $r = ar(k)$ , entonces para todo  $(i_1, \dots, i_r) \in Z_p^r$

$$ST_k(i_1, \dots, i_r) = H_k(i_1, \dots, i_r).$$

#### 3.2.B.5.- Definición

La aplicación

$$ST : P_p(X_1, \dots, X_n) \dashrightarrow Z_p[X_1, \dots, X_n]$$

está definida por:

$$ST(P) = \begin{cases} X_i, & \text{si } P \text{ es } X_i \text{ e } i \in \{1, \dots, n\} \\ ST_k(ST(P_1), \dots, ST(P_r)), & \text{si } P \text{ es } k(P_1, \dots, P_r) \end{cases}$$

### 3.2.B.5.- Definición

Para cada valoración  $v$ , la aplicación

$$V^* : Z_D[X_1, \dots, X_n] \dashrightarrow Z_D$$

es el homomorfismo definido por:

$$V^*(p) = \begin{cases} 1, & \text{si } p \text{ es } 1 \\ v(X_i), & \text{si } P \text{ es } X_i \\ V^*(q) + V^*(r), & \text{si } p \text{ es } q + r \\ V^*(q)V^*(r), & \text{si } p \text{ es } qr \end{cases}$$

### 3.2.B.6.- Lema

Para toda valoración  $v$ ,  $V = V^* \circ ST$ .

#### Demostración

Por inducción sobre la longitud de las proposiciones.

**3.2.C.- CARACTERIZACIÓN ALGEBRAICA DE LAS TAUTOLOGÍAS****3.2.C.1.- Notación**

En lo que sigue, usaremos las siguientes notaciones:

- $F = \{X_1^p - X_1, \dots, X_n^p - X_n\} \subseteq Z_p[X_1, \dots, X_n]$ ;
- $I = I(F)$  es el ideal de  $Z_p[X_1, \dots, X_n]$  generado por  $F$ ;
- $\text{---}\rightarrow$  es la relación de reducción definida por  $F$  en  $Z_p[X_1, \dots, X_n]$ .

**3.2.C.2.- Lema**

$F$  es una base de Gröbner.

**Demostración**

Por 2.9.2, ya que los líderes de los elementos de  $F$  son primos entre sí.

**3.2.C.3.- Lema**

Para toda valoración  $v$ ,

$$q \in I \implies V^*(q) = 0.$$

**Demostración**

Sea  $q \in I$ . Existen polinomios  $r_1, \dots, r_n$  tales que  $q = r_1(X_1^p - X_1) + \dots + r_n(X_n^p - X_n)$ . Por el Teorema de Fermat,  $a^p - a = 0$ , para todo  $a \in Z_p$ . Puesto que  $V^*$  es un homomorfismo,  $V^*(q) = 0$ .

**3.2.C.4.- Lema**

Para toda valoración  $v$ ,

$$p \text{ ---}\rightarrow^* q \implies V^*(p) = V^*(q).$$

Demostración

Análoga a la del Lema 3.1.C.4.

3.2.C.5.- Lema

$q \in I \iff$  para toda valoración  $v$ ,  $V^*(q) = 0$ .

Demostración

( $\implies$ ) Lema 3.2.C.3.

( $\impliedby$ ) Por inducción sobre  $n$ :

Para  $n = 1$ : Sea  $q'$  la forma  $\text{---}$ -irreducible de  $q$ .

Existen  $a_0, \dots, a_{p-1} \in Z_p$  tales que

$$q' = a_{p-1} X_1^{p-1} + \dots + a_1 X_1 + a_0.$$

Para cada  $i \in \{0, \dots, p-1\}$ , sea  $v_i$  la valoración definida por  $v_i(X_1) = i$ . Por el Lema 3.2.C.4,  $V_i^*(q) = V_i^*(q')$  para todo  $i \in \{0, \dots, p-1\}$ . Luego,

$$0 = V_0^*(q) = V_0^*(q') = a_0,$$

$$0 = V_1^*(q) = V_1^*(q') = a_{p-1} + \dots + a_1 + a_0,$$

$$0 = V_2^*(q) = V_2^*(q') = 2^{p-1} a_{p-1} + \dots + 2a_1 + a_0,$$

$$0 = V_3^*(q) = V_3^*(q') = 3^{p-1} a_{p-1} + \dots + 3a_1 + a_0,$$

.....

$$0 = V_{p-1}^*(q) = V_{p-1}^*(q') = (p-1)^{p-1} a_{p-1} + \dots + (p-1)a_1 + a_0.$$

Puesto que el determinante del sistema es

$$\begin{vmatrix} 0 & 0 & \dots & 0 & 1 \\ 2^{p-1} & 2^{p-2} & \dots & 2 & 1 \\ 3^{p-1} & 3^{p-2} & \dots & 3 & 1 \\ \dots & \dots & \dots & \dots & \dots \\ (p-1)^{p-1} & (p-1)^{p-2} & \dots & (p-1) & 1 \end{vmatrix} \neq 0.$$

$$a_0 = a_1 = \dots = a_{p-1} = 0 \text{ y } q' = 0.$$

Supongamos el resultado cierto para  $n - 1$ . Sea  $q'$  la forma ---->-irreducible de  $q$ . Existen  $q_0, \dots, q_{p-1} \in \mathbb{Z}_p[X_1, \dots, X_{n-1}]$  tales que

$$q' = q_{p-1} X_n^{p-1} + \dots + q_1 X_n + q_0.$$

Sea  $v$  una valoración de  $\{X_1, \dots, X_{n-1}\}$ . Para cada  $i \in \{0, \dots, p - 1\}$ , sea  $v_i$  la valoración definida por

$$v_i(X_j) = \begin{cases} v(X_j), & \text{si } j \in \{1, \dots, n - 1\} \\ i, & \text{si } j = n. \end{cases}$$

Por el Lema 3.2.C.4, para todo  $i \in \{0, \dots, p - 1\}$ ,  $V_i^*(q) = V_i^*(q')$ . Luego,

$$0 = V_0^*(q) = V_0^*(q') = V^*(q_0),$$

$$0 = V_1^*(q) = V_1^*(q') = V^*(q_{p-1}) + \dots + V^*(q_1) + V^*(q_0),$$

$$0 = V_2^*(q) = V_2^*(q') = 2^{p-1} V^*(q_{p-1}) + \dots + 2V^*(q_1) + V^*(q_0),$$

.....

$$0 = V_{p-1}^*(q) = V_{p-1}^*(q') =$$

$$= (p-1)^{p-1} V^*(q_{p-1}) + \dots + (p-1)V^*(q_1) + V^*(q_0).$$

Como en el caso anterior,  $V^*(q_0) = V^*(q_1) = \dots = V^*(q_{p-1}) = 0$ .

Por la hipótesis de inducción,  $q_0 = q_1 = \dots = q_{p-1} = 0$ .

Luego,  $q' = 0$ .

### 3.2.C.6.- Teorema

$P$  es una tautología sii  $ST(P) \text{ ---->}^* 1$ .

#### Demostración

$P$  es una tautología

$\langle == \rangle$  para toda valoración  $v$ ,

$$V(P) = 1 \quad \text{[por 3.2.A.1]}$$

$\langle == \rangle$  para toda valoración  $v$ ,

$$V^*(ST(P)) = 1 \quad \text{[por 3.2.B.5]}$$

<===> para toda valoración  $v$ ,

$$V^*(ST(P) - 1) = 0$$

<===>  $ST(P) - 1 \in I$  [por 3.2.C.5]

<===>  $ST(P) - 1 \dashrightarrow^* 0$  [por 2.5.4]

<===>  $ST(P) \dashrightarrow^* 1$ .

### 3.2.C.7.- Ejemplo

Dadas las fórmulas

$$P_1 = x \vee \neg x,$$

$$P_2 = ((x \rightarrow \neg x) \rightarrow x) \rightarrow x,$$

$$P_3 = x \rightarrow (y \rightarrow x),$$

$$P_4 = (\neg\neg x \rightarrow x) \rightarrow (x \vee \neg x),$$

estudiar su validez en los sistemas trivalentes de Gödel y Lukasiewicz.

#### Solución

Representaremos por  $ST_L$  y  $ST_G$  las funciones  $ST$  correspondientes a los sistemas trivalentes de Lukasiewicz y Gödel, respectivamente.

$$ST_L(P_1) = 2x^4 + 2x^3 + 2x + 1 \dashrightarrow^*$$

$$\dashrightarrow^* 2x^2 + x + 1.$$

$$ST_G(P_1) = 2x^6 + x^5 + x^4 + 2x^2 + 1 \dashrightarrow^*$$

$$\dashrightarrow^* 2x^2 + x + 1.$$

$$ST_L(P_2) = x^{22} + x^{21} + 2x^{18} + 2x^{17} + 2x^{16} + 2x^{15} + x^{14} + x^{11} +$$

$$+ 2x^{10} + 2x^9 + 2x^6 + 2x^3 + 2x^2 + 2x + 1 \dashrightarrow^*$$

$$\dashrightarrow^* 1.$$

$$ST_G(P_2) = 2x^{30} + x^{29} + 2x^{27} + 2x^{24} + x^{23} + x^{22} + x^{21} + x^{20} +$$

$$+ x^{19} + 2x^{18} + 2x^{17} + 2x^{16} + x^{15} + 2x^{14} + x^{13} +$$

$$+ 2x^{11} + x^8 + x^6 + x^5 + 2x^4 + x^2 + 1 \dashrightarrow^*$$

$$\text{---}>^* 2x^2 + x + 1.$$

$$\begin{aligned} ST_L(P_3) = & x^6y^4 + x^6y^3 + x^6y^2 + 2x^5y^3 + x^5y^2 + 2x^4y^2 + 2x^4y + \\ & + 2x^3y^4 + 2x^3y^3 + x^3y^2 + 2x^3y + x^2y^3 + 2x^2y^2 + \\ & + 2x^2y + 2xy^2 + 1 \text{ ---}>^* \end{aligned}$$

$$\text{---}>^* 1.$$

$$\begin{aligned} ST_G(P_3) = & 2x^6y^4 + 2x^6y^3 + 2x^6y^2 + 2x^5y^4 + x^5y^3 + 2x^4y^4 + \\ & + x^3y^4 + x^3y^3 + x^3y + x^2y^4 + 2x^2y^3 + 2x^2y^2 + 2x^2y + \\ & + xy^4 + 2xy^2 + 1 \text{ ---}>^* \end{aligned}$$

$$\text{---}>^* 1.$$

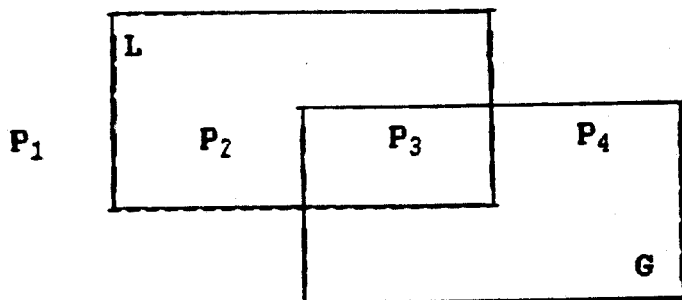
$$\begin{aligned} ST_L(P_4) = & x^{16} + x^{15} + x^{14} + x^{13} + 2x^{12} + x^{11} + 2x^{10} + x^8 + \\ & + 2x^6 + 2x^3 + 2x^2 + 2x + 1 \text{ ---}>^* \end{aligned}$$

$$\text{---}>^* 2x^2 + x + 1.$$

$$\begin{aligned} ST_G(P_4) = & 2x^{32} + x^{30} + x^{29} + 2x^{28} + 2x^{27} + 2x^{24} + x^{23} + x^{22} + \\ & + x^{20} + x^{18} + 2x^{16} + x^{15} + x^{14} + 2x^{10} + x^9 + 2x^8 + \\ & + x^6 + x^4 + 2x^2 + 1 \text{ ---}>^* \end{aligned}$$

$$\text{---}>^* 1.$$

Por tanto, las fórmulas válidas en el sistema de Lukasiewicz son  $P_2$  y  $P_3$ , y las válidas en el sistema de Gödel son  $P_3$  y  $P_4$ . Gráficamente,





**3.2.C.8.- Definición**

P es una contradicción si para toda valoración v,  
 $V(P) = 0$ .

**3.2.C.9.- Corolario**

P es una contradicción sii  $ST(P) \dashrightarrow^* 0$ .

**Demostración**

P es una contradicción

$\langle === \rangle$  para toda valoración v,

$$V(P) = 0 \quad \text{[por 3.2.C.8]}$$

$\langle === \rangle$  para toda valoración v,

$$V^*(ST(P)) = 0 \quad \text{[por 3.2.B.5]}$$

$\langle === \rangle$   $ST(P) \in I$  [por 3.2.C.5]

$\langle === \rangle$   $ST(P) \dashrightarrow^* 0$  [por 2.5.4]

**3.2.D.- CARACTERIZACIÓN ALGEBRAICA DE LA DEDUCCIÓN****3.2.D.1.- Lema**

Sean  $p_1, \dots, p_m, q \in Z_p[X_1, \dots, X_n]$ . Si  $I$  y  $J$  son los ideales de  $Z_p[X_1, \dots, X_n]$  engendrados por los conjuntos  $F = \{X_i^p - X_i : 1 \leq i \leq n\}$  y  $G = \{p_i : 1 \leq i \leq m\}$ , las condiciones siguientes son equivalentes:

(a)  $q \in I + J$  (i.e. el ideal engendrado por  $F \cup G$ ).

(b) Para toda valoración  $v$ ,

$$V^*(p_1) = \dots = V^*(p_m) = 0 \implies V^*(q) = 0.$$

**Demostración**

( $\implies$ ) Es una consecuencia inmediata del Lema 3.2.C.3 y de ser  $V^*$  homomorfismo.

( $\impliedby$ ) Dividimos el conjunto de las valoraciones en dos subconjuntos:

$$A = \{v : V^*(p_1) = \dots = V^*(p_m) = 0\},$$

$$B = \{v : \text{existe un } i(v) \in \{1, \dots, m\} \text{ tal que } V^*(p_{i(v)}) \neq 0\}$$

Consideremos el polinomio

$$q' = \begin{cases} q, & \text{si } B = \emptyset; \\ q \prod_{v \in B} (p_{i(v)} - V^*(p_{i(v)})), & \text{si } B \neq \emptyset. \end{cases}$$

Para toda valoración  $v$ ,  $V^*(q') = 0$ . Por el Lema 3.2.C.5,  $q' \in I$ .

Si  $B = \emptyset$ ,  $q = q' \in I \subseteq I + J$ .

Si  $B \neq \emptyset$ , podemos escribir

$$q' = q \prod_{v \in B} (p_{i(v)} - V^*(p_{i(v)})) = uq + p',$$

donde

$$u = \prod_{v \in B} (-V^*(p_i(v))) \in Z_p - \{0\}$$

y  $p' \in J$ . Luego,

$$uq = q' - p' \in I + J$$

y  $q \in I + J$ .

### 3.2.D.2.- Corolario

Las siguientes condiciones son equivalentes:

(a)  $1 \in I + J$

(b) no existe ninguna valoración  $v$ , tal que  $V^*(p_1) = \dots = V^*(p_m) = 0$ .

### 3.2.D.3.- Teorema

Sean  $P_1, \dots, P_m, Q$  proposiciones de un cálculo proposicional  $p$ -valente. Las siguientes condiciones son equivalentes:

(a)  $\{P_1, \dots, P_m\} \models Q$

(b)  $ST(Q)-1 \in (ST(P_1)-1, \dots, ST(P_m)-1, X_1^p - X_1, \dots, X_n^p - X_n)$

#### Demostración

$$\{P_1, \dots, P_m\} \models Q \iff$$

$\iff$  para toda valoración  $v$ ,

$$V(P_1) = \dots = V(P_m) = 1 \implies V(Q) = 1$$

$\iff$  para toda valoración  $v$ ,

$$V^*(ST(P_1)) = \dots = V^*(ST(P_m)) = 1 \implies V^*(ST(Q)) = 1$$

[por 3.2.B.6]

$\iff$  para toda valoración  $v$ ,

$$V^*(ST(P_1)-1) = \dots = V^*(ST(P_m)-1) = 0 \implies V^*(ST(Q)-1) = 0$$

[por ser  $V^*$  homomorfismo]

$\langle \implies \rangle \text{ ST}(Q)-1 \in (\text{ST}(P_1)-1, \dots, \text{ST}(P_m)-1, X_1^D - X_1, \dots, X_n^D - X_n)$

[por 3.2.D.1]

#### 3.2.D.4.- Corolario

Son equivalentes:

(a)  $\{P_1, \dots, P_m\}$  es inconsistente

(b)  $1 \in (\text{ST}(P_1)-1, \dots, \text{ST}(P_m)-1, X_1^D - X_1, \dots, X_n^D - X_n)$

#### Demostración

$\{P_1, \dots, P_m\}$  es inconsistente  $\langle \implies \rangle$

$\langle \implies \rangle$  no existe ninguna valoración  $v$ , tal que

$$V(P_1) = \dots = V(P_m) = 1$$

$\langle \implies \rangle$  no existe ninguna valoración  $v$ , tal que

$$V^*(\text{ST}(P_1)-1) = \dots = V^*(\text{ST}(P_m)-1) = 0 \quad [\text{por } 3.2.B.6]$$

$\langle \implies \rangle 1 \in (\text{ST}(P_1)-1, \dots, \text{ST}(P_m)-1, X_1^D - X_1, \dots, X_n^D - X_n)$

[por 3.2.D.2]

#### 3.2.D.5.- Nota

Los algoritmos de deducción para las lógicas polivalentes son los mismos que los desarrollados para la lógica clásica en 3.1.E.

## CAPITULO 4

### LÓGICA MONÁDICA

En este capítulo usamos las bases de Gröbner para resolver algorítmicamente problemas de la lógica monádica.

La sección 4.1 contiene las definiciones de la lógica monádica que usaremos en las restantes.

En la sección 4.2 definimos la aplicación  $G$  que asocia un polinomio de  $Z_2[X_1, \dots, X_n]$  a cada sentencia monádica.

En la sección 4.3 caracterizamos las sentencias válidas mediante el Teorema 4.3.8.

En la sección 4.4 damos condiciones equivalentes a  $\{A_1, \dots, A_m\} \models B$  (4.4.1) y a  $\{A_1, \dots, A_m\}$  es inconsistente (4.4.3) que nos permiten aplicar a la lógica monádica los algoritmos de la sección 3.1.E para el cálculo proposicional clásico.

## 4.1.- DEFINICIONES

### 4.1.1.- Definición

Un lenguaje monádico  $L$  está formado por un conjunto de variables ( $x, y, z, \dots$ ), un conjunto de constantes un conjunto de símbolos de predicados monádicos, las conectivas  $\neg$  (negación) y  $\&$  (conjunción) y el cuantificador universal  $\forall$ .

### 4.1.2.- Definición

Los términos de un lenguaje monádico son las variables y las constantes. Usaremos la letra  $t$  como metavariable para designar términos.

### 4.1.3.- Definición

(a) Si  $p$  es un símbolo de predicado y  $t$  es un término de  $L$ ,  $pt$  es una fórmula atómica de  $L$ .

(b) Si  $A$  es una fórmula de  $L$ ,  $\neg A$  también lo es.

(c) Si  $A$  y  $B$  son fórmulas de  $L$ ,  $A \& B$  también lo es.

(d) Si  $A$  es una fórmula de  $L$ ,  $(\forall x)A$  también lo es.

Usaremos las letras  $A, B, C, \dots$  como metavariables sobre fórmulas.

### 4.1.4.- Definición

(1) Una estancia de una variable  $x$  en una fórmula  $A$  es ligada si dicha estancia ocurre en una parte de  $A$  de la forma  $(\forall x)B$ . En caso contrario, se dice que la estancia es libre.

(2) Una variable  $x$  es libre (resp. ligada) en una fórmula  $A$  si  $A$  tiene alguna estancia libre (resp. ligada) de  $x$ .

(3) Una sentencia de  $L$  es una fórmula de  $L$  sin variables libres. Representaremos por  $\text{Sent}(L)$  el conjunto de las sentencias de  $L$ .

(4) Una proposición de  $L$  es una sentencia de  $L$  sin cuantificadores. Representaremos por  $P(L)$  el conjunto de proposiciones de  $L$ .

#### 4.1.5.- Definición

$A_{x_1, \dots, x_s}[t_1, \dots, t_s]$  es la fórmula obtenida sustituyendo simultáneamente todas las estancias libres de  $x_1, \dots, x_s$  en  $A$  por  $t_1, \dots, t_s$  respectivamente.

#### 4.1.6.- Definición

Usaremos las siguientes abreviaturas:

- (1)  $A \vee B$  como abreviatura de  $\neg(\neg A \ \& \ \neg B)$ .
- (2)  $A \rightarrow B$  como abreviatura de  $\neg A \vee B$ .
- (3)  $A \leftrightarrow B$  como abreviatura de  $(A \rightarrow B) \ \& \ (B \rightarrow A)$
- (4)  $(\exists x)A$  como abreviatura de  $\neg(\forall x)\neg A$

#### 4.1.7.- Definición

Una  $L$ -estructura  $M$  consta de:

- (1) Un conjunto no vacío  $M$ , que denominaremos universo de  $M$ .
- (2) Para cada constante  $c$  de  $L$ , un elemento  $M(c)$  de  $M$ .
- (3) Para cada símbolo de predicado  $p$  de  $L$ , un subconjunto  $M(p)$  de  $M$ .

**4.1.8.- Definición**

Sea  $M$  una  $L$ -estructura. Para cada elemento  $a$  de  $M$  elegimos un nuevo símbolo de constante  $a$ . Al lenguaje obtenido añadiéndole a  $L$  una nueva constante  $a$  por cada elemento  $a$  de  $M$  lo notaremos por  $L(M)$ .

**4.1.9.- Definición**

Para cada nueva constante  $a$  de  $L(M)$  definimos  $M(a)$  como el elemento de  $M$  representado por  $a$ .

**4.1.10.- Definición**

Sea  $A$  una sentencia de  $L(M)$ . El valor de verdad de  $A$  en  $M$  se define recursivamente por:

- (1) Si  $A$  es  $pt$ ,  $M(A) = 1$  sii  $M(t) \in M(p)$
- (2) Si  $A$  es  $\neg B$ ,  $M(A) = H_{\neg}(M(B))$
- (3) Si  $A$  es  $B \& C$ ,  $M(A) = H_{\&}(M(B), M(C))$
- (4) Si  $A$  es  $(\forall x B)$ ,  $M(A) = 1$  sii  $M(B_x[a]) = 1$  para todo  $a \in M$ .

**4.1.11.- Definición**

(1) Una  $M$ -estancia de una fórmula  $A$  de  $L$  es una fórmula cerrada de  $L(M)$  de la forma  $A_{x_1, \dots, x_s}[a_1, \dots, a_s]$  donde  $a_1, \dots, a_s$  son elementos de  $M$ .

(2) Una fórmula  $A$  de  $L$  es válida en  $M$ ,  $M \models A$ , si para toda  $M$ -estancia  $A'$  de  $A$ ,  $M(A') = 1$ .

(3)  $M$  es un modelo de  $A$  si  $M \models A$ .



(4) A es válida,  $\models A$ , si es válida en todas las L-estructuras.

(5) A es consistente si tiene algún modelo.

(6) M es un modelo de  $\{A_1, \dots, A_s\}$  si  $M \models A_i$  para todo  $i$  ( $1 \leq i \leq s$ ).

(7) A es una consecuencia de  $\{A_1, \dots, A_s\}$ ,  $\{A_1, \dots, A_s\} \models A$  si todos los modelos de  $\{A_1, \dots, A_s\}$  son modelos de A.

(8)  $\{A_1, \dots, A_s\}$  es consistente si tiene algún modelo e inconsistente en caso contrario.

#### 4.1.12.- Notación

En lo que sigue utilizaremos las siguientes notaciones:

(1) L es el lenguaje monádico que tiene las constantes  $c_1, \dots, c_r$  y los símbolos de predicados monádicos  $p_1, \dots, p_m$ .

(2)  $n = r + 2^m$ .

(3) L' es el lenguaje obtenido añadiéndole a L las  $2^m$  nuevas constantes  $c_{r+1}, \dots, c_n$ .

#### 4.1.13.- Definición

Una valoración de L' es una aplicación  $v$  del conjunto  $\{p_i c_j : 1 \leq i \leq m, 1 \leq j \leq n\}$  en  $Z_2$ . Para cada valoración  $v$  se define una aplicación  $V : P(L') \rightarrow Z_2$  recursivamente como sigue:

$$V(A) = \begin{cases} v(A), & \text{si } A \text{ es atómica;} \\ H_{\neg}(V(B)), & \text{si } A \text{ es } \neg B; \\ H_{\&}(V(B), V(C)), & \text{si } A \text{ es } B \& C. \end{cases}$$

**4.1.14.- Definición**

Una proposición  $A$  de  $L'$  es una tautología si para toda valoración de verdad  $v$  de  $L'$ ,  $V(A) = 1$ .

**4.2.- POLINOMIOS ASOCIADOS A FÓRMULAS****4.2.1.- Definición**

$F: \text{Sent}(L') \rightarrow P(L')$  se define recursivamente como

$$F(A) = \begin{cases} A & , \text{ si } A \text{ es atómica} \\ \neg F(B) & , \text{ si } A \text{ es } \neg B \\ F(B) \ \& \ F(C) & , \text{ si } A \text{ es } B \ \& \ C \\ F(B_x[c_1]) \ \& \ \dots \ \& \ F(B_x[c_n]) & , \text{ si } A \text{ es } \forall xB \end{cases}$$

**4.2.2.- Notas**

- (a)  $F(B \vee C) = F(B) \vee F(C)$
- (b)  $F(B \rightarrow C) = F(B) \rightarrow F(C)$
- (c)  $F(B \leftrightarrow C) = F(B) \rightarrow F(C)$
- (d)  $F(\exists xB) = F(B_x[c_1]) \vee \dots \vee F(B_x[c_n])$

**4.2.3.- Definición**

$G: \text{Sent}(L') \rightarrow Z_2[X_1, \dots, X_{mn}]$  se define recursivamente

por

$$G(A) = \begin{cases} X_{(i-1)n+j} & \text{si } A \text{ es } P_i C_j; \\ G(B) + 1. & \text{si } A \text{ es } \neg B; \\ G(B)G(C). & \text{si } A \text{ es } B \ \& \ C; \\ G(B_x[c_1]) \dots G(B_x[c_n]). & \text{si } A \text{ es } \forall xB \end{cases}$$

**4.2.4.- Notas**

- (a)  $G(B \vee C) = G(B)G(C) + G(B) + G(C).$
- (b)  $G(B \rightarrow C) = G(B)G(C) + G(B) + 1.$
- (c)  $G(B \leftrightarrow C) = G(B) + G(C) + 1.$

$$(d) G(\exists xB) = \sum_{j=1}^s \{ \prod_{i=1}^s G(B_x[c_{i(j)}]) : 1 \leq i(1) < \dots < i(s) \leq n \}$$

#### 4.2.5.- Definición

ST : P(L')  $\rightarrow$   $Z_2[X_1, \dots, X_{mn}]$  se define recursivamente por

$$ST(A) = \begin{cases} X_{(i-1)n+j}, & \text{si } A \text{ es } p_i c_j; \\ ST(B) + 1, & \text{si } A \text{ es } \neg B; \\ ST(B) \cdot ST(C), & \text{si } A \text{ es } B \& C. \end{cases}$$

#### 4.2.6.- Notación

En lo que sigue,  $F = \{X_i^2 + X_i : 1 \leq i \leq mn\}$  y escribiremos  $\rightarrow_F$  en lugar de  $\rightarrow$ .

#### 4.2.7.- Lema

Una proposición A de L' es una tautología si, y sólo si,  $ST(A) \rightarrow^* 1$ .

#### Demostración

Ver 3.1.C.7

#### 4.2.8.- Lema

$$G = ST \circ F.$$

#### Demostración

Por inducción sobre la longitud de las sentencias.

. Si A es atómica, A es  $p_i c_j$  para algún  $i \in \{1, \dots, m\}$  y  $j \in \{1, \dots, n\}$ . Sea  $k = (i - 1)n + j$ .

$$\begin{aligned} (ST \circ F)(A) &= ST(F(A)) = \\ &= ST(A) = \quad \quad \quad \text{[por 4.2.1]} \end{aligned}$$

$$= X_k = \quad \text{[por 4.2.5]}$$

$$= G(A). \quad \text{[por 4.2.3]}$$

. Si A es  $\neg B$ ,

$$(ST.F)(A) = ST(F(\neg B)) =$$

$$= ST(\neg F(B)) = \quad \text{[por 4.2.1]}$$

$$= ST(F(B)) + 1 = \quad \text{[por 4.2.5]}$$

$$= G(B) + 1 = \quad \text{[por hip. ind.]}$$

$$= G(\neg B) = \quad \text{[por 4.2.3]}$$

$$= G(A).$$

. Si A es B & C,

$$(ST.F)(A) = ST(F(B \& C)) =$$

$$= ST(F(B) \& F(C)) = \text{[por 4.2.1]}$$

$$= ST(F(B))ST(F(C)) = \text{[por 4.2.5]}$$

$$= G(B)G(C) = \quad \text{[por hip. ind.]}$$

$$= G(B \& C) = \quad \text{[por 4.2.3]}$$

$$= G(A).$$

**4.3.- CARACTERIZACIÓN ALGEBRAICA DE LA VALIDEZ.****4.3.1.- Lema**

Si  $A$  es una sentencia consistente de  $L$ , existe un modelo  $M'$  de  $A$  tal que  $\text{card}(M') \leq 2^n$ .

**Demostración**

Sea  $N$  un modelo de  $A$  y  $N$  el universo de  $N$ . En  $N$  definimos la relación

$$a R b \text{ sii } N(p_i a) = N(p_i b) \text{ para todo } i \in \{1, \dots, m\}$$

(donde  $a$  y  $b$  son las nuevas constantes que se añaden a  $L$  para denotar los elementos  $a$  y  $b$  de  $N$ ).  $R$  es una relación de equivalencia en  $N$ . En cada clase  $[a]$ , elegimos un elemento  $a'$ . Sea  $M$  el conjunto formado por dichos elementos y  $M$  la  $L(N)$ -estructura de universo  $M$  definida por

$$M(a) = a', \text{ para todo } a \in N;$$

$$M(c_i) = M(N(c_i)), \text{ para todo } i \in \{1, \dots, r\};$$

$$M(p_j) = \{a' : a \in N(p_j)\}, \text{ para todo } j \in \{1, \dots, m\}$$

Que la restricción de  $M$  a  $L$ ,  $M|_L$ , es un modelo de  $A$  tal que  $\text{card}(M|_L) \leq 2^n$  es una consecuencia inmediata de los siguientes Lemas:

$$\text{Lema I: } \text{card}(M) \leq 2^n$$

Lema II: Para toda fórmula  $B$  de  $L(N)$  con  $s$  ( $s \geq 0$ ) variables libres  $x_1, \dots, x_s$  y todo  $(a_1, \dots, a_s) \in N^s$ ,

$$N(B_{x_1, \dots, x_s}[a_1, \dots, a_s]) = M(B_{x_1, \dots, x_s}[a_1', \dots, a_s']).$$

En efecto,  $\text{card}(M|_L) = \text{card}(M) \leq 2^n$  por el Lema I; y, por el Lema II,  $M(A) = N(A) = 1$ .

Demostración de Lema I 

La aplicación  $s: M \rightarrow Z_2^n$  definida por

$$s(a') = (N(p_1 a'), \dots, N(p_n a'))$$

es inyectiva. Luego,  $\text{card}(M) \leq \text{card}(Z_2^n) = 2^n$ .

 Demostración del Lema II 

Por inducción sobre la longitud de las fórmulas:

· Si  $B$  es atómica, existe un  $i \in \{1, \dots, n\}$  y un término  $t$  de  $L(N)$  tales que  $B$  es  $p_i t$ .

· Si existe un  $a \in N$  tal que  $t$  es  $a$ ,

$$N(B) = 1 \iff N(p_i a) = 1$$

$$\iff a \in N(p_i)$$

$$\iff a' \in M(p_i)$$

$$\iff M(p_i a) = 1 \quad [\text{pues } M(a) = a']$$

$$\iff M(B) = 1$$

· Si existe un  $j \in \{1, \dots, r\}$  tal que  $t$  es  $c_j$ , entonces existe un  $a \in N$  tal que  $a = N(c_j)$ . Por tanto,  $M(c_j) = M(N(c_j)) = a'$ .

$$N(B) = N(p_i c_j) =$$

$$= N(p_i a) =$$

$$= M(p_i a) = \quad [\text{por el caso anterior}]$$

$$= M(p_i a') = \quad [M(a) = a']$$

$$= M(p_i c_j) = \quad [M(c_j) = a']$$

$$= M(B).$$

· En caso contrario,  $t$  es una variable  $x$

$$N(B_x[a]) = N(p_i a) =$$

$$= M(p_i a) = \quad [\text{por el caso 1}]$$

$$= M(p_i a') = \quad [M(a) = a']$$

$$= M(B_x[a'])$$

• Si B es  $\neg C$ ,

$$\begin{aligned}
 N(B_{x_1, \dots, x_s}[a_1, \dots, a_s]) &= \\
 &= N(\neg C_{x_1, \dots, x_s}[a_1, \dots, a_s]) = \\
 &= H_{\neg}(N(C_{x_1, \dots, x_s}[a_1, \dots, a_s])) = \\
 &= H_{\neg}(M(C_{x_1, \dots, x_s}[a_1, \dots, a_s])) = \\
 &\quad \text{[hip. ind]} \\
 &= M(\neg C_{x_1, \dots, x_s}[a_1, \dots, a_s]) = \\
 &= M(B_{x_1, \dots, x_s}[a_1, \dots, a_s])
 \end{aligned}$$

• Si B es C & D, se demuestra análogamente.

• Si B es  $\forall y C$ ,

$$\begin{aligned}
 N(B_{x_1, \dots, x_s}[a_1, \dots, a_s]) &= 1 \iff \\
 \iff N(\forall y C_{x_1, \dots, x_s}[a_1, \dots, a_s]) &= 1 \\
 \iff \text{para todo } b \in N, & \\
 N((C_{x_1, \dots, x_s}[a_1, \dots, a_s])_y[b]) &= 1 \\
 \iff \text{para todo } b \in N, & \\
 N(C_{x_1, \dots, x_s, y}[a_1, \dots, a_s, b]) &= 1 \\
 \iff \text{para todo } b \in N, & \\
 M(C_{x_1, \dots, x_s, y}[a_1', \dots, a_s', b']) &= 1 \\
 \quad \text{[por hip. ind.]} & \\
 \iff \text{para todo } b' \in M, & \\
 M(C_{x_1, \dots, x_s, y}[a_1', \dots, a_s', b']) &= 1 \\
 \iff \text{para todo } b' \in M, & \\
 M((C_{x_1, \dots, x_s}[a_1', \dots, a_s'])_y[b']) &= 1 \\
 \iff M(\forall y C_{x_1, \dots, x_s}[a_1', \dots, a_s']) &= 1 \\
 \iff M(B_{x_1, \dots, x_s}[a_1', \dots, a_s']) &= 1.
 \end{aligned}$$



**4.3.2.- Lema**

Si  $M$  es un modelo finito de una sentencia  $A$  de  $L$ , existe un modelo  $N$  de  $A$  tal que  $\text{card}(N) = \text{card}(M) + 1$ .

**Demostración**

Sea  $b_0$  un elemento distinto de los de  $M$ ,  $N = M \cup \{b_0\}$  y  $a_0$  un elemento fijo de  $M$ . Sea  $N$  la  $L$ -estructura de universo  $N$  definida por

$$N(c_i) = M(c_i) \text{ , para todo } i \in \{1, \dots, r\};$$

$$N(p_j) = \begin{cases} M(p_j) & \text{, si } a_0 \notin M(p_j); \\ M(p_j) \cup \{b_0\} & \text{, si } a_0 \in M(p_j). \end{cases}$$

Además, para cada elemento  $a$  de  $M$ , la constante añadida a  $L$  para formar  $L(N)$  es la misma que se añade para formar  $L(M)$ . Que  $N$  es un modelo de  $A$  es una consecuencia inmediata del siguiente Lema:

**Lema:** Para toda fórmula  $B$  de  $L(M)$  con  $s$  ( $s \geq 0$ ) variables libres  $x_1, \dots, x_s$ ,

$$N(B_{x_1, \dots, x_s}[b_0, \dots, b_0]) = M(B_{x_1, \dots, x_s}[a_0, \dots, a_0]).$$

**Demostración** (Por inducción sobre la longitud de  $B$ ):

• Si  $B$  es atómica, existe un  $i \in \{1, \dots, m\}$  y un término  $t$  de  $L(M)$  tales que  $B$  es  $p_i t$ .

• Si  $t$  es una variable,  $x$

$$N(B_x[b_0]) = 1 \iff N(p_i b_0) = 1$$

$$\iff b_0 \in N(p_i)$$

$$\iff a_0 \in M(p_i)$$

$$\iff M(p_i a_0) = 1$$

$$\iff M(B_x[a_0]) = 1$$

• Si  $t$  es una constante,  $M(t) = N(t) = b_0$  y

$$\begin{aligned}
 N(B) = 1 & \iff N(p_i t) = 1 \\
 & \iff N(t) \in N(p_i) \\
 & \iff M(t) \in M(p_i) \\
 & \iff M(p_i t) = 1 \\
 & \iff M(B) = 1.
 \end{aligned}$$

• Si B es  $\neg C$ ,

$$\begin{aligned}
 N(B_{x_1, \dots, x_s}[b_0, \dots, b_0]) &= \\
 &= N(\neg C_{x_1, \dots, x_s}[b_0, \dots, b_0]) \\
 &= H_{\neg}(M(C_{x_1, \dots, x_s}[b_0, \dots, b_0])) = \\
 &= H_{\neg}(N(C_{x_1, \dots, x_s}[a_0, \dots, a_0])) = [\text{hip. ind.}] \\
 &= N(\neg C_{x_1, \dots, x_s}[a_0, \dots, a_0]) = \\
 &= N(B_{x_1, \dots, x_s}[a_0, \dots, a_0])
 \end{aligned}$$

• Si B es C & D, se demuestra análogamente.

• Si B es  $\forall y C$ ,

$$\begin{aligned}
 N(B_{x_1, \dots, x_s}[b_0, \dots, b_0]) = 1 & \iff \\
 \iff N(\forall y C_{x_1, \dots, x_s}[b_0, \dots, b_0]) = 1 \\
 \iff \text{para todo } b \in N, \\
 & N((C_{x_1, \dots, x_s}[b_0, \dots, b_0])_y [b]) = 1 \\
 \iff \text{para todo } a \in M, \\
 & N((C_{x_1, \dots, x_s}[b_0, \dots, b_0])_y [a]) = 1 \\
 \iff \text{para todo } a \in M, \\
 & N((C_y[a])_{x_1, \dots, x_s}[b_0, \dots, b_0]) = 1 \\
 \iff \text{para todo } a \in M, \\
 & M((C_y[a])_{x_1, \dots, x_s}[a_0, \dots, a_0]) = 1 \\
 & [\text{hip. ind.}] \\
 \iff \text{para todo } a \in M, \\
 & M((C_{x_1, \dots, x_s}[a_0, \dots, a_0])_y [a]) = 1 \\
 \iff N(\forall y C_{x_1, \dots, x_s}[a_0, \dots, a_0]) = 1
 \end{aligned}$$

$$\implies N(B_{x_1, \dots, x_s}[a_0, \dots, a_0]) = 1$$

$$N(B_{x_1, \dots, x_s}[a_0, \dots, a_0]) = 1 \implies$$

$$\implies N(\forall y C_{x_1, \dots, x_s}[a_0, \dots, a_0]) = 1$$

$\implies$  para todo  $a \in M$ ,

$$N((C_{x_1, \dots, x_s}[a_0, \dots, a_0])_y[a]) = 1$$

$\implies$  para todo  $a \in N - \{b_0\} = M$

$$\begin{aligned} N((C_{x_1, \dots, x_s}[b_0, \dots, b_0])_y[a]) &= \\ = N((C_y[a])_{x_1, \dots, x_s}[b_0, \dots, b_0]) &= \\ = N((C_y[a])_{x_1, \dots, x_s}[a_0, \dots, a_0]) &= \end{aligned}$$

[por hip. ind.]

$$\begin{aligned} &= N((C_{x_1, \dots, x_s}[a_0, \dots, a_0])_y[a]) = \\ &= 1 \end{aligned}$$

para  $a = b_0$ :

$$\begin{aligned} N((C_{x_1, \dots, x_s}[b_0, \dots, b_0])_y[a]) &= \\ = N(C_{x_1, \dots, x_s, y}[b_0, \dots, b_0, b_0]) &= \\ = N(C_{x_1, \dots, x_s, y}[a_0, \dots, a_0, a_0]) &= \end{aligned}$$

[por hip. ind.]

$$= 1$$

$\implies$  para todo  $a \in N$ ,

$$N(C_{x_1, \dots, x_s}[b_0, \dots, b_0])_y[b] = 1$$

$$\implies N(\forall y C_{x_1, \dots, x_s}[b_0, \dots, b_0]) = 1$$

$$\implies N(B_{x_1, \dots, x_s}[b_0, \dots, b_0]) = 1.$$

### 4.3.3.- Teorema

Si  $A$  es una sentencia consistente de  $L$ , tiene un modelo de cardinal  $2^{\aleph}$ .

Demostración

Es una consecuencia inmediata de los Lemas 4.3.1 y 4.3.2

4.3.4.- Definición

Una L'-estructura  $M'$  es adecuada si para cada  $a' \in M'$ , existe un  $i \in \{1, \dots, n\}$  tal que  $M'(c_i) = a'$ .

4.3.5.- Lema

Sea  $M'$  una L'-estructura adecuada. Para toda sentencia  $A$  de  $L$ ,  $M'(A) = M'(F(A))$ .

Demostración

(Por inducción sobre la longitud de  $A$ )

• Si  $A$  es atómica,  $F(A) = A$  y  $M'(A) = M'(F(A))$ .

• Si  $A$  es  $\neg B$ ,

$$\begin{aligned} M'(A) &= M'(\neg B) = \\ &= H_{\neg}(M'(B)) = \\ &= H_{\neg}(M'(F(B))) = \quad [\text{hip. de ind.}] \\ &= M'(\neg F(B)) = \\ &= M'(F(\neg B)) = \\ &= M'(F(A)). \end{aligned}$$

• Si  $A$  es  $B \& C$ , se demuestra análogamente.

• Si  $A$  es  $\forall x B$ , se verifica el siguiente Lema:

Lema: Para todo  $a' \in M'$ ,  $M'(B_x[a']) = 1$  si y solo si para todo  $i \in \{1, \dots, n\}$ ,  $M'(B_x[c_i]) = 1$ .

Usando el lema tenemos:

$$M'(A) = 1 \iff M'(\forall x B) = 1$$

$$\iff \text{para todo } a' \in M', M'(B_x[a']) = 1$$

$\langle == \rangle$  para todo  $i \in \{1, \dots, n\}$ ,  $M'(B_x[c_i]) = 1$

[por el Lema]

$\langle == \rangle M'(B_x[c_1]) \cdot \dots \cdot B_x[c_n] = 1$

$\langle == \rangle M'(F(A)) = 1$

#### Demostración del Lema

( $== \rangle$ ) Sea  $i \in \{1, \dots, n\}$ .

$$M'(B_x[c_i]) = M'(B_x[M'(c_i)]) = 1.$$

( $\langle ==$ ) Sea  $a' \in M'$ . Existe un  $i \in \{1, \dots, n\}$  tal que  $M'(c_i) = a'$ . Luego,  $M'(B_x[a']) = M'(B_x[c_i]) = 1$ .

#### 4.3.6.- Lema

Si  $A$  es una sentencia consistente de  $L$ , existe una  $L'$ -estructura adecuada  $M'$  que es un modelo de  $A$ .

#### Demostración

Por el teorema 4.3.3 (aplicado a  $A$  como sentencia de  $L'$ ), existe una  $L'$ -estructura  $M$  tal que  $M(A) = 1$  y  $\text{card}(M) = 2^n$ . Sea  $M = \{a_i : 1 \leq i \leq 2^n\}$  el universo de  $M$  y  $M'$  la  $L'$ -estructura de universo  $M$  definida por

$$M'(c_i) = \begin{cases} M(c_i), & \text{si } 1 \leq i \leq r; \\ a_{i-r}, & \text{si } r+1 \leq i \leq n; \end{cases}$$

$$M'(p_j) = M(p_j), \quad \text{si } 1 \leq j \leq m.$$

$M'$  es adecuada y  $M'(A) = M(A) = 1$ .

#### 4.3.7.- Teorema

Una sentencia  $A$  de  $L$  es válida sii  $F(A)$  es una tautología.

Demostración

( $\implies$ ) Supongamos que  $F(A)$  no es una tautología. Existe una valoración  $v$  de  $L'$  tal que  $V(F(A)) = 0$ . Sea  $M'$  la  $L'$ -estructura de universo  $M' = \{c_1, \dots, c_n\}$  definida por

$$M'(c_i) = c_i, \text{ para } 1 \leq i \leq n;$$

$$M'(p_j) = \{c_i : v(p_j c_i) = 1\}, \text{ para } 1 \leq j \leq m.$$

$M'$  es adecuada. Por el Lema 4.3.5,

$$M'(A) = M'(F(A)) = V(F(A)) = 0$$

Por tanto,  $A$  no es válida.

( $\impliedby$ ) Supongamos que  $A$  no es válida. Entonces  $\neg A$  es consistente. Por el Lema 4.3.6, existe una  $L'$ -estructura adecuada  $M'$  tal que  $M'(\neg A) = 1$ . Sea  $v$  la valoración definida por  $v(p_i c_j) = M'(p_i c_j)$  para  $i \in \{1, \dots, m\}$  y  $j \in \{1, \dots, n\}$ .

$$\begin{aligned} \text{Entonces } V(F(A)) &= M'(F(A)) = \quad [\text{por la def de } \underline{V}] \\ &= M'(A) = \quad [\text{por el Lema 4.3.5}] \\ &= 0 \end{aligned}$$

Por tanto,  $F(A)$  no es una tautología.

4.3.8.- Teorema

Una sentencia  $A$  de  $L$  es válida sii  $G(A) \dashv\dashv^* 1$ .

Demostración

$A$  es válida  $\iff F(A)$  es una tautología [por 4.1.14]

$\iff ST(F(A)) \dashv\dashv^* 1$  [por 4.2.7]

$\iff G(A) \dashv\dashv^* 1$  [por 4.2.8]

4.3.9.- Ejemplo

Demostrar que la sentencia

$$(\forall x)p_1x \dashv\dashv (\exists x)p_1x$$

es válida.

### Demostración

En este caso,  $L = \{p_1\}$ ,  $m = 1$ ,  $r = 0$  y  $n = 2$ . Añadimos dos constantes y formamos  $L' = L \cup \{c_1, c_2\}$ . Sea A la sentencia  $(\forall x)p_1x \rightarrow (\exists x)p_1x$ .

$$\begin{aligned}
 G(A) &= \\
 &= G((\forall x)p_1x)G((\exists x)p_1x) + G((\forall x)p_1x) + 1 = \\
 &= (G(p_1c_1) \cdot G(p_1c_2)) (G(p_1c_1) + G(p_1c_2) + G(p_1c_1) \cdot G(p_1c_2)) p_1c_1 + \\
 &\quad + (G(p_1c_1) \cdot G(p_1c_2)) + 1 = \\
 &= (X_1X_2)(X_1+X_2+X_1X_2) + (X_1X_2) + 1 = \\
 &= X_1^2 X_2 + X_1X_2^2 + X_1^2 X_2^2 + X_1X_2 + 1 \text{ ---}>^* \\
 &\text{---}>^* X_1X_2 + X_1X_2 + X_1X_2 + X_1X_2 + 1 = \\
 &= 1.
 \end{aligned}$$

### 4.3.10.- Ejemplo

Demostrar que la sentencia

$$(\exists x)(\forall y)[p_1x \rightarrow p_1y]$$

es válida.

### Demostración

Sean L y L' como en el caso anterior y sea A la sentencia  $(\exists x)(\forall y)[p_1x \rightarrow p_1y]$ .

$$\begin{aligned}
 G(A) &= G((\forall y)[p_1c_1 \rightarrow p_1y]) + G((\forall y)[p_1c_2 \rightarrow p_1y]) + \\
 &\quad + G((\forall y)[p_1c_1 \rightarrow p_1y]) \cdot G((\forall y)[p_1c_2 \rightarrow p_1y]) \\
 G((\forall y)[p_1c_1 \rightarrow p_1y]) &= \\
 &= G(p_1c_1 \rightarrow p_1c_1) \cdot G(p_1c_1 \rightarrow p_1c_2). \\
 G(p_1c_1 \rightarrow p_1c_1) &= \\
 &= G(p_1c_1) \cdot G(p_1c_1) + G(p_1c_1) + 1 = \\
 &= X_1^2 + X_1 + 1 \text{ ---}>^*
 \end{aligned}$$

---->\* 1.

$$\begin{aligned} G(p_1c_1 \rightarrow p_1c_2) &= \\ &= G(p_1c_1) \cdot G(p_1c_2) + G(p_1c_1) + 1 = \\ &= X_1X_2 + X_1 + 1. \end{aligned}$$

Luego,

$$G((\forall y) [p_1c_1 \rightarrow p_1y]) \text{ ---->* } X_1X_2 + X_1 + 1.$$

Análogamente,

$$G((\forall y) [p_1c_2 \rightarrow p_1y]) \text{ ---->* } X_1X_2 + X_2 + 1.$$

Por tanto,

$$\begin{aligned} G(A) \text{ ---->* } &(X_1X_2 + X_1 + 1) + (X_1X_2 + X_2 + 1) + \\ &(X_1X_2 + X_1 + 1)(X_1X_2 + X_2 + 1) \text{ ---->*} \\ &\text{---->* } 1. \end{aligned}$$

#### 4.3.11.- Ejemplo

Demostrar que la sentencia

$$(\exists x)p_1x \rightarrow (\forall x)p_1x$$

no es válida.

#### Demostración

Sean L y L' como en los ejemplos anteriores y sea A la sentencia  $(\exists x)p_1x \rightarrow (\forall x)p_1x$ .

$$\begin{aligned} G(A) &= \\ &= G((\exists x)p_1x)G((\forall x)p_1x) + G((\exists x)p_1x) + 1 = \\ &= (G(p_1c_1)+G(p_1c_2)+G(p_1c_1) \cdot G(p_1c_2)) \cdot (G(p_1c_1) \cdot G(p_1c_2) + \\ &\quad + (G(p_1c_1)+G(p_1c_2)+G(p_1c_1) \cdot G(p_1c_2)) + 1 = \\ &= (X_1+X_2+X_1X_2)(X_1X_2) + (X_1+X_2+X_1X_2) + 1 \text{ ---->*} \\ &\text{---->* } X_1+X_2+1 \end{aligned}$$

que es irreducible. Por tanto, A no es válida.



#### 4.4. CARACTERIZACIÓN ALGEBRAICA DE LA DEDUCCIÓN

##### 4.4.1.- Teorema

Sean  $A_1, \dots, A_s, B$  sentencias de  $L$ . Las siguientes condiciones son equivalentes:

$$(1) \{A_1, \dots, A_s\} \models B.$$

$$(2) G(B)+1 \in (G(A_1)+1, \dots, G(A_s)+1, X_1^2 + X_1, \dots, X_{mn}^2 + X_{mn})$$

##### Demostración

$$\{A_1, \dots, A_s\} \models B \iff$$

$$\iff \models A_1 \& \dots \& A_s \rightarrow B$$

$$\iff F(A_1 \& \dots \& A_s \rightarrow B) \text{ es una tautología [por 4.3.7]}$$

$$\iff F(A_1) \& \dots \& F(A_s) \rightarrow F(B) \text{ es una tautología}$$

$$\text{[por 4.2.1 y 4.2.2]}$$

$$\iff ST(F(B)) + 1 \in (ST(F(A_1)) + 1, \dots, ST(F(A_s)) + 1,$$

$$X_1^2 + X_1, \dots, X_{mn}^2 + X_{mn}) \text{ [por 3.1.D.4]}$$

$$\iff G(B) + 1 \in (G(A_1) + 1, \dots, G(A_s) + 1,$$

$$X_1^2 + X_1, \dots, X_{mn}^2 + X_{mn}) \text{ [por 4.2.8]}$$

##### 4.4.2.- Ejemplo

Demostrar que

$$\{p_1c_1, \neg p_1c_2\} \models \neg(\forall x)(\forall y)[p_1x \leftrightarrow p_1y].$$

##### Demostración

Sean  $A_1, A_2$  y  $B$  las sentencias  $p_1c_1, \neg p_1c_2$  y  $\neg(\forall x)(\forall y)[p_1x \leftrightarrow p_1y]$ , respectivamente. En este caso  $L = \{p_1, c_1, c_2\}$ ,  $m = 1$ ,  $r = 2$ ,  $n = 4$  y  $L' = L \cup \{c_3, c_4\}$ .

Por 4.4.1, tenemos que probar que

$$G(B)+1 \in (G(A_1)+1, G(A_2)+1, X_1^2 + X_1, \dots, X_4^2 + X_4)$$

Lo haremos calculando una base de Gröbner,  $F$ , del ideal

$(G(A_1)+1, G(A_2)+1, X_1^2 + X_1, \dots, X_4^2 + X_4)$  y comprobando que  $G(B)+1 \dashrightarrow_F^* 0$ .

$$G(A_1) + 1 = G(p_1c_1) + 1 = X_1 + 1$$

$$G(A_2) + 1 = G(-p_1c_2) + 1 = G(p_1c_2) = X_2$$

$F = \{X_1 + 1, X_2, X_3^2 + X_3, X_4^2 + X_4\}$  es una base del ideal.

Vamos a calcular la forma normal de  $G(B)+1$  respecto de  $F$ .

$$\begin{aligned} G(B)+1 &= G((\forall x)(\forall y)[p_1x \leftrightarrow p_1y]) = \\ &= \prod_{i=1}^4 G((\forall y)[p_1c_i \leftrightarrow p_1y]) \\ &= \prod_{i=1}^4 \prod_{j=1}^4 G(p_1c_i \leftrightarrow p_1c_j) = \\ &= \prod_{i=1}^4 \prod_{j=1}^4 (G(p_1c_i) + G(p_1c_j) + 1) = \\ &= \prod_{i=1}^4 \prod_{j=1}^4 (X_i + X_j + 1) \dashrightarrow^* \\ &\dashrightarrow^* 0, \end{aligned}$$

puesto que uno de los factores es  $X_1 + X_2 + 1$  que se reduce a 0.

#### 4.4.3.- Corolario

Sea  $\{A_1, \dots, A_n\}$  un conjunto de sentencias de  $L$ . Son equivalentes:

- (1)  $\{A_1, \dots, A_n\}$  es inconsistente.
- (2)  $1 \in (G(A_1)+1, \dots, G(A_n)+1, X_1^2 + X_1, \dots, X_{nn}^2 + X_{nn})$

**4.4.4.- Nota**

Los algoritmos de deducción son los mismos que los desarrollados para el cálculo proposicional clásico en 3.1.E.

## APÉNDICES

El apéndice A es un programa en LE\_LISP versión 15 que contiene los algoritmos para el cálculo proposicional clásico y bases de Gröbner en  $Z_2[X_1, \dots, X_n]$ .

El apéndice B es una sesión correspondiente al programa anterior.

## ;APÉNDICE A: ;CÁLCULO PROPOSICIONAL CLÁSICO (PROGRAMA)

### ;NOTACIONES

;variables globales:

; variables (por defecto (x y z))  
; axiomas (por defecto ())  
; base (por defecto (((2 0 0)(1 0 0)),...))

;parametros usuales:

; pol: polinomio usual (x<sup>2</sup> y<sup>3</sup> + x y<sup>2</sup> + 1), (0), ...  
; lpol: lista de pol's  
; p : polinomio como lista de exponentes ((2 3 0)(1 2 0)(0 0 0)), (), ...  
; m : monomio como lista de exponentes (2 3 0)  
; lp : lista de p's

;Las conectivas que usamos son: - (negación), \* (disyunción), & (conjunción),  
(implicación), (->) (equivalencia)

;definición de formula (1) si p es una variable entonces p es una formula  
(2) si f1 y f2 son formulas entonces (- f1), (f1 & f2),  
(f1 \* f2), (f1 -> f2), (f1 (->) f2) tambien lo son

;criterios para eliminar parentesis:

(1) escribir p en lugar de (p)  
(2) jerarquia de conectivas: (-), (->), &, \*, -  
(3) asociación por la derecha (ej (p & q & r) en lugar de ((p) & ((q) & (r)))

### ;FUNCIONES DE LECTURA Y ESCRITURA

```
(setq variables '(x y z))
;el valor por defecto si no se usa llevar
(de llevar ())
;lee las variables y calcula la base por defecto al cambiar las variables
(print "deme la lista de variables")
(setq variables (read))
;base (mapcar 'leepol (mapcar '(lambda (a)(list a 2 '+ a))variable
variables )

(de leepol (pol))
;transforma un polinomio usual en lista de exponentes
(cond
  ((equal pol '(0)) ())
  ((null pol) ())
  (t (cons (mapcar '(lambda (a) (cond ((null a) 0)
                                     ((numberp (cadr a))
                                      (t 1) ))
                (mapcar '(lambda (a)
                          (member a
                                   (firstn (- (length pol)
                                             (length (member '+ pol)
                                                                pol) ) )
                                   variables ) )
                (leepol (cdr (member '+ pol)))))))))

(de escribep (p))
;inversa de leepol
(if (null p) '(0)
    (cdr (apply
          'append
          (pairlis
           (makelist (length p) '+)
           (mapcar
            '(lambda (l)
              (or (apply 'append (mapcar '(lambda (a)
                                           (cond ((= 0 (cdr a)) ())
                                                 ((= 1 (cdr a)) (list (car a)))
                                                 (t (list (car a) (cdr a))))))
                1) )
            '(1) )
          (mapcar '(lambda (m) (pairlis variables m ())) p) )
```

```
( ) ) ) )
```

```
(de pp (f)
```

```
  ;pone los parentesis de f eliminados por la jerarquia de las conectivas
  (cond ((null f) ())
        ((atom f) f)
        ((= 1 (length f)) (pp (car f)))
        ((member '<-> f)
         (list (pp (firstn (- (length f)(length (member '<-> f))) f))
               '<->
               (pp (cdr (member '<-> f)))))
        ((member '-> f)
         (list (pp (firstn (- (length f)(length (member '-> f))) f))
               '->
               (pp (cdr (member '-> f)))))
        ((member '& f)
         (list (pp (firstn (- (length f)(length (member '& f))) f))
               '&
               (pp (cdr (member '& f)))))
        ((member '* f)
         (list (pp (firstn (- (length f)(length (member '* f))) f))
               '*
               (pp (cdr (member '* f)))))
        ((member '- f) (list '- (pp (cdr f))))
        (t 'formula_erronea)))
```

---

```
;ARITMETICA DE POLINOMIOS EN  $Z_2[X_1, \dots, X_N]$ 
```

```
(de mayor-orden-lex (m1 m2)
```

```
  ;t. si m1 > m2 en el orden lexicografico y () en caso contrario
  (cond ((equal m1 m2) ())
        (( (car m1)(car m2)) t)
        (( (car m1)(car m2)) ())
        (t (mayor-orden-lex (cdr m1) (cdr m2))))
```

```
(de mayor (m1 m2)
```

```
  ;t. si m1 > m2 en el orden diagonal y () en caso contrario
  (let ((g1 (apply '+ m1))
        (g2 (apply '+ m2)))
    (cond (( g1 g2) t)
          (( g1 g2) ())
          (t (mayor-orden-lex m1 m2))))
```

```
(de suma (p1 p2)
```

```
  ;suma polinomios ordenados por mayor
  (cond ((null p1) p2)
        ((null p2) p1)
        ((equal (car p1)(car p2)) (suma (cdr p1)(cdr p2)))
        ((mayor (car p1)(car p2)) (cons (car p1)(suma (cdr p1) p2)))
        (t (cons (car p2) (suma p1 (cdr p2))))))
```

```
(de producto (p1 p2)
```

```
  ;multiplica polinomios ordenados por mayor
  (cond ((or (null p1)(null p2)) ())
        (t (suma (mapcar '(lambda (a) (mapcar '+ a (car p1))) p2)
                  (producto (cdr p1) p2))))))
```

---

```
;ALGORITMO DE BASE DE GROBNER
```

```
(de sp-pc (p1 p2)
```

```
  ;Lema 2.6.3
  (lets ((m1 (car p1))(m2 (car p2))(u (mapcar 'max m1 m2)))
        (suma (producto (list (mapcar '- u m1)) p1)
              (producto (list (mapcar '- u m2)) p2))))
```

```

(de selector (p lp)
  :selecciona un sucesor (Lema 2.8.3)
  (suma p
    (any '(lambda (pp)
      (any '(lambda (a)
        (if (every '<= (car pp) a)
            (producto (list (mapcar '- a (car pp))) pp) )
          p) )
      lp) ) )

(de fn (p lp)
  :forma normal de p respecto de lp (Lema 2.8.5)
  (let ((s (selector p lp)))
    (if (equal p s) p (fn s lp))))

(de pares (lp)
  :los pares no-ordenados de elementos de lp
  (if lp (append (mapcar '(lambda (a) (list (car lp) a)) (cdr lp))
    (pares (cdr lp))))

(de lid-prim (par)
  :0, si los líderes de los elementos de par son primos relativos;
  :(), si no lo son
  (every 'zerop (mapcar '* (caar par) (caadr par))) )

(de bg (lpol)
  :base de Grobner del ideal generado por lpol (algoritmo 2.9.3)
  (mapcar 'escribep
    (prog (b g h)
      (setq g (mapcar '(lambda (p) (sort 'mayor p))
        (mapcar 'leepol lpol))
        b (pares g))
      etiql
      (if (null b)(return g))
      (when (lid-prim (car b))(setq b (cdr b))(go etiql))
      (setq h (fn (apply 'sp-pc (car b)) g) b (cdr b))
      (if (null h) (go etiql))
      (setq b (append b (mapcar '(lambda (a) (list h a)) g) )
        g (cons h g) )
      (go etiql) ) ) )

-----

```

#### :BASE DE GROBNER REDUCIDA

```

(de elimina (l)
  :elimina las repeticiones y los elementos ()
  (cond ((null l)())
    ((or (null (car l)) (member (car l) (cdr l)))
      (elimina (cdr l)))
    (t (cons (car l) (elimina (cdr l))))))

(de dif (l1 l2)
  :diferencia de los conjuntos l1 y l2
  (cond ((null l1) ())
    ((member (car l1) l2) (dif (cdr l1) l2))
    (t (cons (car l1) (dif (cdr l1) l2)))))

(de reduce (lp)
  :da un sistema irreducible de generadores del ideal generado por lp
  (prog (f lpinicial lreducida)
    (setq f lp)
    etiql
    (setq lpinicial (copy f) lreducida ())
    (while f
      (setq lreducida (cons (fn (car f)(append lreducida (cdr f)
        lreducida)
          f (cdr f)))
        (setq lreducida (reverse (elimina lreducida))))))

```

```

(if (equal lpinicial lpreducida) lpreducida
    (setq f (copy lpreducida))
    (go etiq1)))

(de bg-r (lpol)
  :base de Grobner reducida del ideal generado por lpol
  (mapcar 'escribep
    (reduce
      (prog (b g h)
        (setq g (reduce (mapcar '(lambda (p) (sort 'mayor p))
                              (mapcar 'leepol lpol)))
              b (pares g))
        etiq1
        (if (null b)(return g))
        (when (lid-prim (car b))(setq b (cdr b))(go etiq1))
        (setq h (fn (apply 'sp-pc (car b)) g)
              b (cdr b))
        (if (null h) (go etiq1))
        (setq b (append b (mapcar '(lambda (a) (list h a)) g)
              g (cons h g) )
        (go etiq1) ) ) ) )

```

---

**: DEDUCCIÓN**

```

(de st1 (f)
  :polinomio correspondiente a la formula f (escrita sin suprimir parentesis)
  (cond ((atom f) (leepol (list f)))
        ((equal (car f) '-') (suma (st1 (cadr f))(leepol '(1))))
        ((equal (cadr f) '&) (producto (st1 (car f))(st1 (caddr f))))
        ((equal (cadr f) '*') (suma (suma (st1 (car f))(st1 (caddr f)))
                                     (producto (st1 (car f))(st1 (caddr f))))
        ((equal (cadr f) '-') (suma (producto (st1 (car f))(st1 (caddr f)))
                                     (suma (st1 (car f))(leepol '(1))))
        ((equal (cadr f) '<-') (suma (suma (st1 (car f))(st1 (caddr f)))
                                     (leepol '(1))))
        (t (print "formula erronea"))))

(de st (f) (st1 (pp f)))
  :polinomio correspondiente a la formula f

(setq axiomas ()) ;el valor por defecto si no se usa leeax
  base (mapcar 'leepol (mapcar '(lambda (a) (list a 2 '+ a)) variables))

(de leeax ()
  :lee los axiomas y calcula la base
  (print "deme la 'lista de axiomas")
  (setq axiomas (eval (read)))
  base (mapcar 'leepol
    (let ((ff (mapcar '(lambda (a) (list a 2 '+ a)) variables)
          (if (null axiomas) ff
              (bg-r

                (append
                  (mapcar '(lambda (f)
                          (escribep (st (list '- f))
                                axiomas)
                          ff))))))
    axiomas)

(de esde (f)
  :determina si f es deducible (Algoritmo 3.1.E.1)
  (if (null (fn (st (list '- f)) base))
      'es_deducible
      'no_es_deducible))

```



## APÉNDICE B:

## CÁLCULO PROPOSICIONAL CLÁSICO (SESIÓN)

? ; EJEMPLO 2.8.9: Calcular una base de Gröbner del ideal de

? ; de  $\mathbb{Z}_2[a,b,c,d]$  generado por

? ;  $\{bd + b + d + 1, cd + d, ab + b\}$

?

? (llevar)

deme la lista de variables

? (a b c d)

= (a b c d)

? (bg '((b d + b + d + 1) (c d + d) (a b + b)))

= ((a c + a + c + 1) (a d + a + d + 1) (b c + b + c + 1)

(b d + b + d + 1) (c d + d) (a b + b))

? (bg-r '((b d + b + d + 1) (c d + d) (a b + b)))

= ((a c + a + c + 1) (a d + a + d + 1) (b c + b + c + 1)

(b d + b + d + 1) (c d + d) (a b + b))

? ; -----

? ; EJEMPLO 3.1.C.8: Estudiar la validez de la fórmula

? ;  $(x_1 \rightarrow x_2) \vee (x_2 \rightarrow x_1)$

?

? (llevar)

deme la lista de variables

? (x1 x2)

= (x1 x2)

? (esde '((x1 -> x2) \* (x2 -> x1)))

= es\_deducible

? ;el polinomio asociado por ST a la fórmula anterior es

? (escribep (st '((x1 -> x2) \* (x2 -> x1))))

= (x1 2 x2 2 + x1 2 x2 + x1 x2 2 + x1 x2 + 1)

? ;-----

? ;EJEMPLO 3.1.C.10: Estudiar la validez de la fórmula

? ;(x1 <-> x2) & (x1 <-> ~ x2)

?

? (esde '((x1 <-> x2) & (x1 <-> ~ x2)))

= no\_es\_deducible

? ;el polinomio asociado por ST a la fórmula anterior es

? (escribep (st '((x1 <-> x2) & (x1 <-> ~ x2))))

= (x1 2 + x2 2 + x1 + x2)

? ;la forma irreducible del polinomio anterior es

? (escribep (fn (st '((x1 <-> x2) & (x1 <-> ~ x2))) base))

= (0)

? ;por tanto, la fórmula es una contradicción

? ;-----

? ;EJEMPLO 3.1.C.13: Estudiar la validez de la fórmula

? ;(x1 <-> x2) & (x1 <-> x3)

?

? (leear)

deme la lista de variables

? (x1 x2 x3)

= (x1 x2 x3)

? (esde '((x1 <-> x2) & (x1 <-> x3)))

= no\_es\_deducible

? ;el polinomio asociado por ST a la fórmula anterior es

? (escribep (st '((x1 <-> x2) & (x1 <-> x3))))

= (x1 2 + x1 x2 + x1 x3 + x2 x3 + x2 + x3 + 1)

? ;la forma irreducible del polinomio anterior es

? (escribep (fn (st f13) base))

= (x1 x2 + x1 x3 + x2 x3 + x1 + x2 + x3 + 1)

? ;por tanto, la fórmula es contingente; un modelo es

? ;v(x1) = v(x2) = v(x3) = 0 y un contramodelo es

? ;v'(x1) = v'(x2) = 0, v'(x3) = 1

? ;-----

? ;EJEMPLO 3.1.E.2: Dado el conjunto de axiomas

? ;AX = {a -> b, b -> e, c v d, ~ (c & d)}, decidir si las

? ;fórmulas Q1 = ~e -> ~a & ~b y Q2 = a -> (b <-> c) son

? ;consecuencias de AX.

?

? (leevar)

deme la lista de variables

? (a b c d e)

= (a b c d e)

? (leeax)

deme la 'lista de axiomas

? '((a -> b)(b -> e)(c \* d)(- (c & d)))

= ((a -> b) (b -> e) (c \* d) (- (c & d)))

? (esde '(- e -> (- a & - b)))

= es\_deducible

? (esde '(a -> (b <-> c)))

= no\_es\_deducible

?

? ;la base de Gröbner de correspondiente al conjunto de

? ;axiomas anterior es

? (mapcar 'escribep base)

= ((a e + a) (a b + a) (b e + b) (c + d + 1) (a 2 + a)  
(b 2 + b) (d 2 + d) (e 2 + e))

? ;la forma irreducible de ST(Q2) respecto de la base

? ;anterior es

? (escribep (fn (st '(a -> (b <-> c))) base))

= (a d + 1)

? ;por tanto, la formula (a -> (b <-> c)) es equivalente

? ;respecto de AX con la formula  $\neg(a \& d)$ . Vamos a

? ;comprobarlo

? (esde '((a -> (b <-> c)) <-> - (a & d)))

= es\_deducible

? ;-----

? ;EJEMPLO 3.1.E.5: Decidir la consistencia del siguiente

? ;conjunto de axiomas

? ;{b -> a & b,  $\neg c \vee b$ ,  $\neg a \vee \neg d$ , c & d}

?

? (leevar)

deme la lista de variables

? (a b c d)

= (a b c d)

? (leeax)

deme la 'lista de axiomas

? '( (b -> a & b) (- c \* b) (- a \* - d) (c & d) )

= ((b -> a & b) (- c \* b) (- a \* - d) (c & d))

? ;la base de Gröbner correspondiente al conjunto de axiomas

? ;anterior es

? (mapcar 'escribep base)

= ((1))

? ;por tanto, el conjunto de axiomas es inconsistente

? ;-----

? ;EJEMPLO 3.1.E.9: Decidir la equivalencia de los siguien-

? ;tes conjuntos de fórmulas:

? ;AX = { $\neg e \rightarrow \neg a \ \& \ \neg b \ \& \ (c \vee d)$ ,  $a \ \& \ (\neg b \vee \neg c) \rightarrow d$ ,

? ;  $\neg b \rightarrow \neg a$ ,  $c \leftrightarrow \neg d$ }

? ;AX' = { $a \rightarrow b$ ,  $b \rightarrow e$ ,  $c \vee d$ ,  $\neg (c \ \& \ d)$ }

? (leevar)

deme la lista de variables

? (a b c d e)

= (a b c d e)

? (leeax)

? '((- e -> - a & - b & (c \* d)) (a & (- b \* - c) -> d)

(- b -> - a) (c <-> - d))

= ((- e -> - a & - b & (c \* d)) (a & (- b \* - c) -> d)

(- b -> - a) (c <-> - d))

? ;la base de Gröbner correspondiente a AX es

? (mapcar 'escribep base)

= ((a e + a) (b e + b) (a b + a) (c + d + 1) (a 2 + a)

(b 2 + b) (d 2 + d) (e 2 + e))

? (leeax)

deme la 'lista de axiomas

? '((a -> b)(b -> e)(c \* d)(- (c & d)))

= ((a -> b) (b -> e) (c \* d) (- (c & d)))

? ;la base de Gröbner correspondiente a  $AX'$  es

? (mapcar 'escriber base)

= ((a e + a) (a b + a) (b e + b) (c + d + 1) (a 2 + a)  
 (b 2 + b) (d 2 + d) (e 2 + e))

? ;puesto que coincide con la base anterior,  $AX$  y  $AX'$  son

? ;equivalentes

## **BIBLIOGRAFIA**

**ACKERMAN, R.**

- [1967] *Introduction to Many Valued Logics*  
Routledge & Kegan Paul Ltd.

**ALONSO, J.A.; BRIALES, E. Y RISCOS, A.**

- [19--] Demostración automática de teoremas en lógicas no-clásicas.

*Congress on Computational Geometry and Topology  
and Computation in Teaching Mathematics,*  
Sevilla, Septiembre 1986.

**BOOLOS, G. y JEFFREY, R.**

- [1974] *Computability and Logic*  
Cambridge University Press.

**BUCHBERGER, B.**

- [1979] A Criterion for Detecting Unnecessary Reductions  
in the Construction of Gröbner-Bases.

*Proc. EUROSAM 79, Marseille, June 1979, (ed. W.  
Ng), Springer-Verlag.*

LNCS Vol. 72, pp. 3-21.

- [1985] Basic Features and Development of the Critical-  
pair/completion procedure.

*Proc. 1st Conf. on Rewriting Techniques and  
Applications, Dijon, May 1985 (ed. J.P.*

*Jouannaud), Springer-Verlag.*

LNCS Vol. 202, pp. 1-45.

- [1985] Gröbner-Bases: An Algorithmic Method in Polynomial  
Ideal Theory.

*Recent Trends in Multidimensional Systems theory*  
(ed. N.K. Bose), Reidel, pp. 184-231.

**BUCHBERGER, B. y LOOS, R.**

- [1982] Algebraic Simplification

*Computer Algebra: Symbolic and Algebraic Computa-  
tion, (ed. B. Buchberger, G.E. Collins y R.*

*Loos), Springer-Verlag, pp. 11-43.*

CAVINESS, B.F.

- [1985] Computer Algebra: Past and Future  
*Journal of Symbolic Computation*, Vol 2 (1986), pp.  
217-236

CHAILLOUX, J.

- [1985] *Le\_Lisp de l'INRIA. Version 15. Manuel de  
référence*

CHANG, C.L. y LEE, R.C.T.

- [1983] *Symbolic Logic and Mechanical Theorem Proving*  
Academic Press.

CHAZARAIN, J.

- [1986] The Lady, the Tiger and the Gröbner Basis.  
*Prepublication de l'Université de Nice*, nº 100.

CHAZARAIN, J. y RISCOS, A.

- [19--] Multivalued Logic and Gröbner Basis (with applica-  
tion to modal logic).  
No publicado.

DUNHAM, B. y WANG, H.

- [1976] Towards Feasible Solutions of th Tautology Problem  
*Annals of Mathematical Logic*, Vol 10 (1976), pp.  
117-154.

HSIANG, J.

- [1985] Refutational Theorem Proving Using Term-Rewriting  
Systems.  
*Artificial Intelligence*, Vol 25 (1985), pp 255-300
- [1985] Two Results in Term Rewriting Theorem Proving.  
*Proc. 1st Conf. on Rewriting Techniques and  
Applications*, Dijon, May 1985 (ed. J.P.  
Jouannaud), Springer-Verlag.  
LNCS Vol. 202, pp. 301-324.

HSIANG, J. y DERSHOWITZ, N.

- [1983] Rewrite Methods for Clausal and Non-clausal Theo-  
rem Proving.  
*Proc. ICALP 83, 10th Colloquium*, Barcelona,  
Springer-Verlag.  
LNCS Vol. 154, pp. 331-346.



HUET, G.

[1980] **Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems.**  
*Journal of the Association for Computing Machinery*  
Vol 27 (1980), pp. 797-821.

[1986] **Deduction and Computation**  
*Fundamentals of Artificial Intelligence* (ed. W. Bibel y Ph. Jorrand), Springer-Verlag, pp. 39-74

HUET, G. y OPPEN, D.C.

[1980] **Equations and Rewrite Rules.**  
*Formal Language Theory: Perspective and Open Problems* (ed. R.V. Book), Academic Press, pp. 345-405.

JOUANNAUD, J.P. y LESCANNE, P.

[1986] **La Réécriture**  
*Technique et Science Informatiques*, Vol 5, no 6,  
pp. 433-452.

KANDRY-RODY, A. y KAPUR, D.

[1984] **Algorithms for Computing Gröbner Bases for Polynomials over various Euclidean Rings.**  
*Proc. EUROSAM 84*, Cambridge (ed. J. Fitch),  
Springer-Verlag.  
LNCS Vol 174, pp. 195-206.

[1984] **Computing the Gröbner Basis of an Ideal in Polynomial Rings over the Integers.**  
*3rd MACSYMA Users Conf.*, Schenectady, New York.

KAPUR, D. y NARENDRA,

[1985] **An Equational Approach to Theorem Proving in First-Order Predicate Calculus.**  
*Rep. no. 84CRD322*, General Electric, Schenectady,  
New York.

KNUTH, E. y BENDIX, B.

[1970] **Simple Word Problem in Universal Algebra.**  
*Proc. of the Conf. on Computational Problems in Abstract Algebra*, Oxford (ed. J. Leech),  
Pergamon Press, pp. 263-298.

KÜCHLIN, W.

- [1985] A Confluence Criterion Based on the Generalised Newman Lemma.  
*Proc. EUROCAL 85*, Linz, (ed. B.F. Caviness)  
Springer-Verlag.  
LNCS Vol 204, pp. 390-399.

LOOS, R.

- [1983] Introducción (Computer Algebra Symbolic and Algebraic Computation)  
*Computer Algebra: Symbolic and Algebraic Computation*, (ed. B. Buchberger, G.E. Collins y R. Loos), Springer-Verlag, pp. 11-43.

LOVELAND, D.W.

- [1978] *Automated Theorem Proving: A Logical Basis*.  
North-Holland.
- [1983] Automated Theorem Proving: A Quarter Century Review.  
*Automated Theorem Proving: After 25 Years* (ed. W.W. Bledsoe y D.W. Loveland), American Mathematical Society.  
Contemporary Mathematics, Vol 29, pp. 1-46.

MOISIL, GR.C.

- [1969] *The Algebraic Theory of Switching Circuits*  
Pergamon Press.

MUSSER, D.R. y KAPUR, D.

- [1982] Rewrite Rules Theory and Abstract Data Type Analysis.  
*Proc. EUROCAM 82*, Marseille (ed. J. Calmet),  
Springer-Verlag.  
LNCS Vol 144, pp. 77-90.

QUEINNEC, C.

- [1984] *LISP, mode d'emploi*  
Eyrolles.

RESCHER, N.

- [1969] *Many-valued Logic*  
McGraw-Hill.

ROBINSON, J.A.

[1965] A Machine-Oriented Logic Based on the Resolution Principle.

*Journal of the Association for Computing Machinery*  
Vol 12 (1965), pp. 23-41.

ROY, J-P y KIREMITDJIAN, g

[1985] *Lire LISP (le langage de l'intelligence artificielle).*

Cedic Nathan.

SCHOENFIELD, J.R.

[1967] *Mathematical Logic*

Addison Wesley.

SIEKMANN, J. y WRICHTSON, G. (Eds.)

[1983] *The Automation of Reasoning, Vol I y II.*  
Springer-Verlag.

TURNER, R.

[1984] *Logics for Artificial Intelligence.*

Ellis Horwood Limited.

WATTS, D.E. y COHEN, J.K.

[1980] Computer-Implemented Set Theory.

*Amer. Math. Monthly, Vol 87 (7), pp. 557-560.*

WINKLER, F. y BUCHBERGER, B.

[1983] A Criterion for Eliminating Unnecessary Reductions  
in the Knuth-Bendix Algorithm.

*Proc. Colloquium on Algebra, Combinatorics and  
Logic in Computer Science, Győr, 1983, Colloquia  
Mathematica Societatis J. Bolyai, J. Bolyai  
Math. and North-Holland.*

WOS, L.

[1985] Automated Reasoning.

*Amer. Math. Monthly, Vol 92 (1985), pp. 85-92.*

# UNIVERSIDAD DE SEVILLA

Reunido el Tribunal Integrado por los abajo firmantes  
en el día de la fecha, para juzgar la Tesis Doctoral de  
D. José Antonio Alonso Jiménez  
titulada Métodos algebraicos de razonamientos automáticos

acordó otorgarle la calificación de APTO CUM LAUDE

Sevilla, 5 de julio 1980

El Vocal,

José María de la Cruz

El Presidente

José Vicente

El Vocal,

José María de la Cruz

El Secretario,

José María de la Cruz

El Vocal,

José María de la Cruz

El Doctorado,

José María de la Cruz