Métodos algebraicos de razonamiento automático
José A. Alonso Jiménez
Sevilla, 4 de Julio de 1988

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.

El capítulo 1 es un estudio detallado de las relaciones canónicas. Una relación binaria $\longrightarrow$ en un conjunto E es canónica si para cada elemento x de E existe un único elemento y tal que $x \longrightarrow^* y$ (i.e. existen $x_1, \ldots, x_n$ tales que $x = x_1 \longrightarrow x_2 \longrightarrow \cdots \longrightarrow x_n = y$) e y es $\longrightarrow$-irreducible (i.e. no existe ningún z de E tal que $y \longrightarrow z$). La finalidad de este capítulo es la demostración de condiciones equivalentes a la de canonicidad que nos permitan construir algoritmos para calcular bases de Gröbner.

En capítulo 2 estudiamos las bases de Gröbner en $\mathbf{Z}_p[X_1, \ldots, X_n]$ y damos nuevos criterios para la eliminación de reducciones innecesarias en el algoritmo de construcción de bases de Gröbner.

En el capítulo 3 usamos las bases de Gröbner para resolver algoritmicamente problemas de los cálculos proposicionales. Está dividido en dos partes. En la primera, estudiamos el cálculo proposicional clásico. Demostramos que una proposicion Q es consecuencia de un conjunto finito de proposiciones $\{P_1, \ldots, P_m\}$ si, y sólo si, $ST(Q) + 1$ pertenece al ideal de $\mathbf{Z}_2[X_1, \ldots, X_n]$ engendrado por $\{ST(P_i) + 1 : 1 \leq i \leq m\} \cup \{X_i^2 + X_i : 1 \leq i \leq n\}$, donde ST es la aplicación del conjunto de proposiciones en el anillo $\mathbf{Z}_2[X_1, \ldots, X_n]$ definida recursivamente por:

$$ST(P) = \begin{cases} P, & \text{si } P \text{ es una variable;} \\ ST(Q) + 1, & \text{si } P \text{ es } \neg Q; \\ ST(Q)ST(R), & \text{si } P \text{ es } Q \wedge R. \end{cases}$$

La segunda condición es decidible mediante bases de Gröbner, lo que nos permite construir un algoritmo algebraico para decidir la deducibilidad. Otros problemas que se resuelven utilizando métodos análogos son el de la validez (dada una proposición, determinar si es válida), el de la consistencia (dado un conjunto de proposiciones, determinar si es consistente) y el de la equivalencia (dados dos conjuntos de proposiciones determinar si son equivalentes). En la segunda parte estudiamos los cálculos proposicionales polivalentes. Demostramos que en un cálculo proposicional con un número primo, p, de valores de verdad, una proposición Q es consecuencia de un conjunto finito de proposiciones $\{P_1, \ldots, P_m\}$ si, y sólo si, $ST(Q)+1$ pertenece al ideal de $\mathbf{Z}_p[X_1, \ldots, X_n]$

engendrado por $\{ST(P_i)+1 : 1 \leq i \leq m\} \cup \{X_i^p - X_i : 1 \leq i \leq n\}$, donde ST es la aplicación del conjunto de proposiciones en el anillo $\mathbf{Z}_p[X_1, \ldots, X_n]$ definida recursivamente por:

$$ST(P) = \begin{cases} P, & \text{si } P \text{ es una variable;} \\ ST_k(ST(Q_1), \ldots, ST(Q_r)), & \text{si } P \text{ es } k(Q_1, \ldots, Q_r). \end{cases}$$

y para cada conectiva r-aria k, ST_k es la aplicación de $\mathbf{Z}_p[X_1, \ldots, X_n]^r$ en el anillo $\mathbf{Z}_p[X_1, \ldots, X_n]$ definida por:

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

y $H_k : \mathbf{Z}_p^r \to \mathbf{Z}_p$ es la tabla de verdad de la conectiva k. La segunda condición es decidible mediante bases de Gröbner, lo que nos permite construir un algoritmo algebraico para decidir la deducibilidad. Análogamente a lo obtenido en la primera parte, damos algoritmos algebraicos para la validez, la inconsistencia y la equivalencia. Finalmente, mostramos cómo transformar los anteriores algoritmos para cálculos proposicionales con un número no-primo de valores de verdad.

En el capítulo 4 usamos las bases de Gröbner para resolver algoritmicamente problemas de la lógica monádica. Demostramos que si $\mathbf{L}$ es un lenguaje de primer orden cuyos símbolos no lógicos son las constantes $c_1, \ldots, c_r$ y los símbolos de predicados monádicos $p_1, \ldots, p_m$ y $\mathbf{L}'$ es el lenguaje obtenido añadiéndole a $\mathbf{L}$ 2^m nuevas constantes $c_{r+1}, \ldots, c_n$, una sentencia B de $\mathbf{L}$ es consecuencia de un conjunto de sentencias $\{A_1, \ldots, A_s\}$ si, y sólo si, $ST(B)+1$ pertenece al ideal de $\mathbf{Z}_2[X_1, \ldots, X_{mn}]$ engendrado por $\{ST(A_i)+1 : 1 \leq i \leq s\} \cup \{X_i^2 - X_i : 1 \leq i \leq mn\}$, donde ST es la aplicación del conjunto de las sentencias de $\mathbf{L}'$ en el anillo $\mathbf{Z}_2[X_1, \ldots, X_{mn}]$ definida recursivamente por:

$$ST(P) = \begin{cases} X_{(i-1)n+j}, & \text{si } P \text{ es } p_i c_j; \\ ST(Q)+1, & \text{si } P \text{ es } \neg Q; \\ ST(Q)ST(R), & \text{si } P \text{ es } Q \wedge R; \\ \prod_{i=1}^{n} ST(Q_x[c_i]), & \text{si } P \text{ es } \forall x Q. \end{cases}$$

Como consecuencia del teorema, obtenemos algoritmos algebraicos para los problemas de la deducibilidad, validez, inconsistencia y equivalencia.

El apéndice contiene una implementación en Le-Lisp versión 15 de los anteriores algoritmos y una sesión realizada con dicho programa.

BIBLIOGRAFIA

[1] Boolos, G. y Jeffrey, R. *Computability and Logic.* Cambridge University Press, 1974.

[2] Buchberger, B. Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory. En Bose, N.K. (ed), *Recent Trends in Multidimensional Systems Theory,* Reidel, 1985, pp. 184-231.

[3] Buchberger, B. y Loos, R. Algebraic Simplification. En B. Buchberger, G.E. Collins y R. Loos (eds.), *Computer Algebra: Symbolic and Algebraic Computation,* Springer-Verlag, 1982, pp. 11-43.

[4] Chazarain, J. *The Lady, the Tiger and the Gröbner Basis.* Prepublication de l'Université de Nice, n. 100, 1986.

[5] Hsiang, J. Refutational Theorem Proving Using Term-Rewriting Systems. *Artificial Intelligence 25,* 3 (1985), pp 255-300.

[6] Huet, G. Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems. *Journal of the Association for Computing Machinery 27,* 4 (1980), pp. 797-821.

[7] Kandry-Rody, A. y Kapur, D. Algorithms for Computing Gröbner Bases for Polynomials over various Euclidean Rings. *Proc. EUROSAM 84,* Cambridge, 1984. *Lecture Notes in Computer Science 174,* Springer, pp.195-206.