Preuve automatique dans le calcul propositionnel et les logiques trivalentes

J.A. Alonso, E. Briales, A. Riscos

Université de Séville

Introduction

Nous présentons une application des bases de Gröbner (bases standard) d'idéaux de polynômes la vérification des tautologies dans le Calcul Propositionnel et dans trois types de logiques trivalentes.

L'idée base est de transformer les formules en polynômes, et de trouver l'équivalent algèbrique de la déduction: nous verons des théorèmes faisant la liaison entre déduction et critères de réduction algèbrique ([2], [3], [4]).

A.- Bases de Gröbner dans $k[X_1, \ldots, X_n]$

Soit $k[X_1, \ldots, X_n]$ l'ensemble des polynômes sur $X_1, \ldots, X_n$, et avec les coefficients dans un corps k. Tout polynôme p peut s'écrire $p = c_1.t_1 + \cdots + c_m.t_m$ où c_i sont les coefficients, et t_i son les monômes ordonnés: $t_1 > \cdots > t_m$ par l'ordre lexicographique. On notera $L(p) = c_1.t_1$.

Un ensemble fini de polynômes, $F \subseteq k[X_1, \ldots, X_n]$ permet définir une rélation de réduction $\longrightarrow_F$ par:
$p \longrightarrow_F q$ ssi il existe $r \in F$ et un monôme a tels que

(i) $a.L(r)$ est un monôme de p

(ii) $q = p - a.r$

Si F est clair, on notera $\longrightarrow_F$ simplement par $\longrightarrow$; $\xrightarrow{*}$ est la clôture réflexive et transitive de $\longrightarrow$. On notera par $I(F)$ l'idéal engendré par F.

On utilisera la charactérisation suivante:

F est una base de Gröbner ssi
$I(F) = \{p : p \xrightarrow{*} 0\}$ ssi
pour tout p $\exists! q$, $\longrightarrow$-irréductible, tel que $p \xrightarrow{*} q$.

Par exemple, pour m premier, l'ensemble

$$F_m = \{X_1^m - X_1, \ldots, X_n^m - X_n\}$$

est toujours une base de Gröbner dans l'anneau $\mathbf{Z}_m[X_1, \ldots, X_n]$.

B.- Tautologies dans le Calcul Propositionnel

Soit $\mathbf{P}(X_1, \ldots, X_n)$ l'ensemble des propositions construites avec les connecteurs usuels $\neg$ (non), $\vee$ (ou), $\wedge$ (et), $\rightarrow$ (si ... alors ...), $\leftrightarrow$ (ssi) et les variables X_1,...,X_n.

Dans $\mathbf{Z}_2$ on définit les opérations $\neg'$, $\vee'$, $\wedge'$, $\rightarrow'$, $\leftrightarrow'$ par les tableaux

			$a\vee' b$		$a\wedge' b$		$a\rightarrow' b$		$a\leftrightarrow' b$	
a	$\neg' a$	b	0	1	0	1	0	1	0	1
0	1	a								
1	0	0	0	1	0	0	1	1	1	0
		1	1	1	0	1	0	1	0	1

ou, de façon équivalente

$$\begin{aligned} \neg' a &= a + 1 \\ a \vee' b &= a.b + a + b \\ a \wedge' b &= a.b \\ a \rightarrow' b &= a.b + a + 1 \\ a \leftrightarrow' b &= a + b + 1 \end{aligned}$$

Le sens logique de 1 sera "vrai" et de 0 sera "faux".

Les opérations ont eté définies suivant le théorème de Stone [6]. On notera les propositions par P, Q.

Définition B.1. *Une réalisation est une application*

$$v : \{X_1, \ldots, X_n\} \rightarrow \mathbf{Z}_2$$

Toute réalisation peut s'étendre, de façon unique, une application

$$v' : P(X_1, \ldots, X_n) \rightarrow \mathbf{Z}_2$$

telle que

$$\begin{aligned} v'(X_i) &= v(X_i), \quad 1 \leq i \leq n \\ v'(P \wedge Q) &= v'(P) \wedge' v'(Q) \\ v'(\neg P) &= \neg' v'(P) \\ v'(P \vee Q) &= v'(P) \vee' v'(Q) \\ v'(P \wedge Q) &= v'(P) \wedge' v'(Q) \\ v'(P \rightarrow Q) &= v'(P) \rightarrow' v'(Q) \\ v'(P \leftrightarrow Q) &= v'(P) \leftrightarrow' v'(Q) \end{aligned}$$

comme on peut déduire facilement des lois de formation des propositions.

Définition B.2. *P est une tautologie, $\models P$, ssi $v'(P) = 1$ pour toute réalisation v.*

Définition B.3. *On définit, récursivement, une application*

$$B : \mathbf{P}(X_1, \ldots, X_n) \to \mathbf{Z}_2[X_1, \ldots, X_n]$$

par

$$B(P) = \begin{cases} Xi, & \text{si } P \text{ est } X_i \text{ et } 1 \leq i \leq n; \\ B(Q) + 1, & \text{si } P \text{ est } \neg Q; \\ B(Q)B(R) + B(Q) + B(R), & \text{si } P \text{ est } Q \vee R; \\ B(Q)B(R), & \text{si } P \text{ est } Q \wedge R; \\ B(Q)B(R) + B(Q) + 1, & \text{si } P \text{ est } Q \to R; \\ B(Q) + B(R) + 1, & \text{si } P \text{ est } Q \leftrightarrow R; \end{cases}$$

A nouveau, les lois des formation des propositions nous garantissent la bonne définition.

Lemme B.4. *Pour toute réalisation v, il existe un homomorphisme unique*

$$v^* : \mathbf{Z}_2[X_1, \ldots, X_n] \to \mathbf{Z}_2$$

tel que $v^*(X_i) = v(X_i), 1 \leq i \leq n$.

La preuve se fait en considérant maintenant la structure des polynômes.
En plus, on peut tester facilement la commutativité du diagramme:

$$\begin{array}{ccc} \mathbf{P}(X_1, \ldots, X_n) & \xrightarrow{B} & \mathbf{Z}_2[X_1, \ldots, X_n] \\ {\scriptstyle v'}\downarrow & & {\scriptstyle v^*}\downarrow \\ \mathbf{Z}_2 & \xrightarrow{id} & \mathbf{Z}_2 \end{array}$$

On arrive au résultat fondamental de cette section. On considère l'ensemble $F = F_2 = \{X_1^2 + X_1, \ldots, X_n^2 + X_n\}$. On a:

Théorème B.5. *$\models P$ ssi $B(P) \xrightarrow{*} 1$ [et P est contradictoire ssi $B(P) \xrightarrow{*} 0$].*

La preuve repose sur les lemmes

Lemme B.6. *Si $p \xrightarrow{*} q$, alors $v^*(p) = v^*(q)$, pour toute réalisation v.*

Lemme B.7. *$p \xrightarrow{*} 0$ ssi $v^*(p) = 0$ pour toute réalisation v.*

qui sont des résultats strictement algèbriques.

Comme nous avons annoncé, le théorème B.5 met en rélation un aspect exclusivement logique avec un aspect exclusivement algèbrique.

Exemples.

$$
\begin{array}{ll}
P_1 = ((x \to \neg y) \to \neg y) & B(P_1) \xrightarrow{*} (xy + y + 1) \\
P_2 = (x \vee \neg x) & B(P_2) \xrightarrow{*} (1) \\
P_3 = (((x \to \neg x) \to x) \to x) & B(P_3) \xrightarrow{*} (1) \\
P_4 = ((x \to y) \vee (y \to x)) & B(P_4) \xrightarrow{*} (1) \\
P_5 = (x \to (y \to x)) & B(P_5) \xrightarrow{*} (1) \\
P_6 = (x \wedge (x \to y) \to y) & B(P_6) \xrightarrow{*} (1) \\
P_7 = ((\neg\neg x \to x) \to x \vee \neg x) & B(P_7) \xrightarrow{*} (1) \\
P_8 = (x \wedge \neg x) & B(P_8) \xrightarrow{*} (0)
\end{array}
$$

C.- Tautologies dans les Logiques Trivalentes

On va maintenant décrire le même processus pour les systèmes de Łucasiewicz, Gödel et Kleene, de logique trivalente.

On définit trois ensembles d'opérations sur $\mathbf{Z}_3$ (qui ont ses équivalents polynomiales, comme nous verons après):

a	$\neg'_L a$
0	1
1	0
2	2

a	$a\vee'_L b$			$a\wedge'_L b$			$a\to'_L b$			$a\leftrightarrow'_L b$		
b	0	1	2	0	1	2	0	1	2	0	1	2
0	0	1	2	0	0	0	1	1	1	1	0	2
1	1	1	1	0	1	2	0	1	2	0	1	2
2	2	1	2	0	2	2	2	1	1	2	2	1

a	$\neg'_G a$
0	1
1	0
2	0

a	$a\vee'_G b$			$a\wedge'_G b$			$a\to'_G b$			$a\leftrightarrow'_G b$		
b	0	1	2	0	1	2	0	1	2	0	1	2
0	0	1	2	0	0	0	1	1	1	1	0	0
1	1	1	1	0	1	2	0	1	2	0	1	2
2	2	1	2	0	2	2	0	1	1	0	2	1

a	$\neg'_K a$
0	1
1	0
2	2

a	$a\vee'_K b$			$a\wedge'_K b$			$a\to'_K b$			$a\leftrightarrow'_K b$		
b	0	1	2	0	1	2	0	1	2	0	1	2
0	0	1	2	0	0	0	1	1	1	1	0	2
1	1	1	1	0	1	2	1	0	2	0	1	2
2	2	1	2	0	2	2	2	1	2	2	2	2

Maintenant, une réalisation est une application

$$v : \{X_1, \ldots, X_n\} \to \mathbf{Z}_3,$$

et peut s'étendre, de façon unique, à une application

$$v^T : \mathbf{P}(X_1, \ldots, X_n) \to \mathbf{Z}_3$$

telle que

$$v^T(R) = \begin{cases} v(X_i), & \text{si } R \text{ est } X_i \text{ et } 1 \leq i \leq n; \\ \neg_T v^T(P), & \text{si } R \text{ est } \neg P; \\ v^T(P) \vee_T v^T(Q), & \text{si } R \text{ est } P \vee Q; \\ v^T(P) \wedge_T v^T(Q), & \text{si } R \text{ est } P \wedge Q; \\ v^T(P) \to_T v^T(Q), & \text{si } R \text{ est } P \to Q; \\ v^T(P) \leftrightarrow_T v^T(Q), & \text{si } R \text{ est } P \leftrightarrow Q \end{cases}$$

où $T = L$, G ou K.

De même, on dira que P est une T-tautologie, $\models_T P$, ssi $v^T(P) = 1$ pour toute réalisation v. On définit, tout comme à B, les trois fonctions

$$L, G, K : \mathbf{P}(X_1, \ldots, X_n) \to \mathbf{Z}_3[X_1, \ldots, X_n]$$

récursivement par:

$$\begin{aligned} L(X_i) &= X_i \qquad (1 \leq i \leq n) \\ L(\neg P) &= 2p + 1 \\ L(P \vee Q) &= 2p^2.q^2 + p^2.q + p.q^2 + p.q + p + q \\ L(P \wedge Q) &= p^2.q^2 + 2p^2.q + 2p.q^2 + 2p.q \\ L(P \to Q) &= p^2.q^2 + 2p^2.q + 2p.q^2 + 2p.q + 2p + 1 \\ L(P \leftrightarrow Q) &= 2p^2.q^2 + p^2.q + p.q^2 + p.q + 2p + 2q + 1 \end{aligned}$$

$$\begin{aligned} G(X_i) &= X_i \qquad (1 \leq i \leq n) \\ G(\neg P) &= 2p^2 + 1 \\ G(P \vee Q) &= 2p^2.q^2 + p^2.q + p.q^2 + p.q + p + q \\ G(P \wedge P) &= p^2.q^2 + 2p^2.q + 2p.q^2 + 2p.q \\ G(P \to Q) &= 2p^2.q^2 + 2p^2.q + p.q^2 + 2p^2 + 2pq + 1 \\ G(P \leftrightarrow Q) &= p^2.q^2 + 2p^2 + p.q + 2q^2 + 1 \end{aligned}$$

$$\begin{aligned} K(X_i) &= X_i \qquad (1 \leq i \leq n) \\ K(\neg P) &= 2p + 1 \\ K(P \vee Q) &= 2p^2.q^2 + p^2.q + p.q^2 + p.q + p + q \\ K(P \wedge Q) &= p^2.q^2 + 2p^2.q + 2p.q^2 + 2p.q \\ K(P \to Q) &= 2p^2.q^2 + 2p^2 + p.q^2 + 2p.q + p + 1 \\ K(P \leftrightarrow Q) &= 2p.q + 2p + 2q + 1 \end{aligned}$$

Pour chaque réalisation v, il existe un homomorphisme unique

$$v^* : \mathbf{Z}_3[X_1, \ldots, X_n] \to \mathbf{Z}_3$$

tel que $v^*(X_i) = v(X_i)$, $1 \leq i \leq n$. En plus, on obtient la commutativité du diagramme:

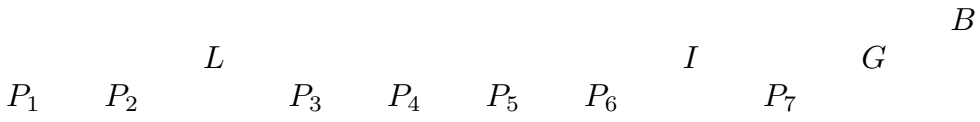
$$\begin{array}{ccc} \mathbf{P}(X_1, \ldots, X_n) & \xrightarrow{T} & \mathbf{Z}_3[X_1, \ldots, X_n] \\ {\scriptstyle v^T}\downarrow & & \downarrow{\scriptstyle v^*} \\ \mathbf{Z}_3 & \xrightarrow{id} & \mathbf{Z}_3 \end{array}$$

Si on prend maintenant l'ensemble $F = F_3 = \{X_1^3 + 2X_1, \ldots, X_n^3 + 2X_n\}$ on a le

Théorème C.1. $\models_T P$ *ssi* $T(P) \xrightarrow{*} 1$.

qui nous permet de programmer facilement la vérification automatique des tautologies dans les trois systèmes considérés.

Dans le diagramme suivant on voit la situation rélative des tautologies. Les exemples P_1 à P_7, dejà vus, ont la position qu'on indique.



I = Intuitionisme.

Notez que, dans le système de Kleene, il n'y a pas de tautologies.

Pourquoi ces trois types de logique trivalente? Le système de Łucasiewicz fut le premier historiquement; le sens logique du "2"est celui d'être "pas définible"; le système nous permet la définition d'opérateurs modales, dont nous parlerons à la fin. Il faut signaler que les opérateurs modales ne sont pas définibles dans le Calcul Propositionnel.

Dans le système de Gödel le sens logique du "2" n'a pas d'importance. Gödel prouva que l'Intuitionisme n'est pas définible par des tableaux, et il introduit son système parce que c'est une bonne aproximation (en fait, il y a des systèmes d'axiomes pour l'Intuitionisme, de façon telle qu'en ajoutant un nouveau axiome, on obtient les axiomes de Gödel). Malheureusement les tautologies intuitionistes sont contenues dans les G-Tautologies, donc notre automatisme algèbrique sert plutôt à prouver des non-théorèmes.

Dans le système de Kleene, le sens logique du "2" est celui d'être "pas encore défini" ou "inconnu". Comme on a dejà dit, il n'y a pas de K-Tautologies, mais notre procéssus permet de tester aisement des formules avec les mêmes valeurs de verité.

Exemple.
$Q_1 = (x \to y)$
$Q_2 = (\neg x \vee y)$
$K(Q_1) \xrightarrow{*} (1 + 2x + xy^2 + x^2y + 2x^2y^2)$

$K(Q_2) \xrightarrow{*} (1 + 2x + xy^2 + x^2y + 2x^2y^2)$
tandis que
$L(Q_1) \xrightarrow{*} (1 + 2x + 2xy + 2xy^2 + 2x^2y + x^2y^2)$
$L(Q_2) \xrightarrow{*} (1 + 2x + xy^2 + x^2y + 2x^2y^2)$
et
$G(Q_1) \xrightarrow{*} (1 + 2xy + xy^2 + 2x^2 + 2x^2y + 2x^2y^e 2)$
$G(Q_2) \xrightarrow{*} (1 + 2x^2 + x^2y)$

La méthode décrite peut s'appliquer à tous les types de logique trivalente (ex. Bochvar), et même à des logiques polivalentes (avec un nombre premier de valeurs), de façon toute naturelle.

D.- Déduction dans le Calcul Propositionnel

Définition D.1. *Q est une conséquence tautologique de (ou, on peut déduire Q à partir de) $P_1, \ldots, P_m$, $\{P_1, \ldots, P_m\} \models Q$, ssi pour toute réalisation v, si $v'(P_1) = \cdots = v'(P_m) = 1$, alors $v'(Q) = 1$.*

Dans le Calcul Propositionnel, on a la charactérisation équivalente:

$$\{P_1, \ldots, P_m\} \models Q \quad \Longleftrightarrow \quad \models P_1 \wedge \cdots \wedge P_m \rightarrow Q$$

qui va nous permettre d'utiliser les résultats de la section A. Malheureusement cette charactérisation n'est pas valable dans les logiques non-classiques. En effet, on considére dans $\mathbf{P}(X_1, \ldots, X_n)$ la rélation d'équivalence $P \simeq Q$ ssi $v'(P) = v'(Q)$ pour toute réalisation v. L'ensemble des classes d'équivalence, muni de l'extension naturelle des opérations $\neg$, $\vee$, $\wedge$ c'est une algèbre booléenne $< \mathbf{P}^*(X_1, \ldots, X_n), \neg, \vee, \wedge >$ nommée algèbre de Lindenbaum-Tarski. Le point c'est que si $\mathbf{B}(X_1, \ldots, X_n)$ est l'anneau booléen associé par le théorème de Stone, on a le

Théorème D.2. *L'application*

$$\theta : \mathbf{B}(X_1, \ldots, X_n) \rightarrow \mathbf{Z}_2[X_1, \ldots, X_n]/I(F_2)$$

définie par $\theta(\overline{P}) = \overline{B(P)}$ est un isomorphisme d'anneaux.

Notez que $\overline{P}$ est une classe de propositions équivalentes par la rélation $\simeq$, et que $\overline{B(P)}$ est une classe de polynômes équivalents par la rélation induite par l'idéal $I(F_2)$. Ce théorème, et aussi sa preuve, sont exclusivement techniques. Le résultat important c'est le

Théorème D.3. *Les conditions suivantes sont équivalentes:*
(i) $\{P_1, \ldots, P_m\} \models Q$
(ii) $\theta(\overline{Q}) + \overline{1} \in (\theta(\overline{P_1}) + \overline{1}, \ldots, \theta(\overline{P_m}) + \overline{1})$
(iii) $B(Q) + 1 \in (B(P_1) + 1, \ldots, B(P_m) + 1, X_1^2 + X1, \ldots, X_n^2 + X_n)$
où $\overline{1}$ répresente la classe des tautologies; par exemple, on peut écrire $\overline{1} = \overline{X_1 \vee \neg X_1}$.

La preuve repose sur les lemmes

Lemme D.4. $\overline{p_1} \cdots \overline{p_m}.(\overline{q} + \overline{1}) = \overline{0}$ *ssi* $\overline{q} + \overline{1} \in (\overline{p_1} \cdots \overline{p_m} + \overline{1})$

Lemme D.5. $(\overline{p_1} \cdots \overline{p_m} + \overline{1}) = (\overline{p_1} + \overline{1}, \ldots, \overline{p_m} + \overline{1})$

qui sont des résultats faciles sur les classes de polynômes.

Le majeur intérêt du théorème D.3 c'est l'équivalence $(i) \iff (iii)$; en effet, si on calcule une base standard pour l'idéal, la preuve automatique des conséquences est presque triviale. Voici l'algorithme:

$$AX = \{P_1, \ldots, P_m\}$$

$$F := BG\{p_1 + 1, \ldots, p_m + 1, X_1^2 + X_1, \ldots, X_n^2 + X_n\}$$

$$Q$$

$$h := FN(q + 1)$$

$$h = 0 \qquad\qquad AX \models Q$$

$$AX \not\models Q$$

Exemple 1. Pour l'ensemble

$$AX_1 = \{\neg e \to (\neg a \wedge \neg b \wedge (c \vee d)), a \wedge (\neg b \vee \neg c) \to d, \neg b \to \neg a, c \leftrightarrow \neg d\}$$

on obtient

$$F_1 = \{ae + a, be + b, ab + a, c + d + 1, a^2 + a, b^2 + b, d^2 + d, e^2 + e\}$$

Si

$$Q_{1.1} = \neg e \to \neg a \wedge \neg b \qquad \text{et} \qquad Q_{1.2} = a \to (b \leftrightarrow c)$$

on a

$$h_{1.1} = 0 \qquad \text{et} \qquad h_{1.2} = ad$$

respectivement.

Pour le calcul de la base de Gröbner, nous avons développé un algorithme du type Buchberger [1] pour le cas spécial $\mathbf{Z}_2$, avec un critére de réduction des paires critiques, dû à Chazarain [2]. Cette méthode présente, face à la méthode habituelle de Résolution de Robinson, les avantages suivantes:

- Nous pouvous travailler avec des formules quelconques, tandis que la résolution a besoin de formules en forme de clauses.

- Le procéssus de résolution est formellement égal (c.à.d. également complexe) que le calcul d'une base de Gröbner. Notre algorithme, en faisant les calculs une seule fois, "compile" les axiomes; le changement de proposition Q n'oblige pas à refaire les calculs; la résolution doit refaire tout le procéssus chaque fois qu'on change la formule Q.
- Notre méthode permet de tester très aisement l'équivalence d'ensembles d'axiomes: il suffit de voir qu'on obtient la même base. Par exemple, si

  $$AX_2 = \{a \to b, c \vee d, b \to e, \neg(c \wedge d)\}$$

  alors

  $$F_2 = \{ae + a, a^2 + a, ab + a, b^2 + b, be + b, d^2 + d, c + d + 1, e^2 + e\}$$

  donc, l'ensemble AX_1 est équivalent à l'ensemble AX_2.
- De même, on peut tester l'inconsistance d'un ensemble d'axiomes. Par exemple, si

  $$AX_3 = \{b \to a \wedge d, \neg c \vee b, a \to \neg d, c \wedge d\},$$

  alors $F_3 = \{1\}$: l'idéal est l'anneau tout entier, donc AX_3 est inconsistante

E.- Logique Modale

Pour finir, on dira quelques mots sur logique modale.
Dans le système de Łucasiewicz, on peut définir deux nouveaux connecteurs:

$$P : \text{"P est possible"}$$
$$P : \text{"P est nécessaire"}.$$

On considère alors l'ensemble des propositions $\mathbf{P}'(X_1, \ldots, X_n)$ avec les connecteurs $\neg$, , , $\vee$, $\wedge$, $\to$, $\leftrightarrow$. Le point c'est que si on définit sur $\mathbf{Z}_3$ les óperations ${}_L$, ${}_L$ par

a	${}_L a$	${}_L a$
0	1	0
1	0	1
2	1	0

on étend v^L par

$$v^L(P) =_L v^L(P);$$
$$v^L(P) =_L v^L(P)$$

et L par

$$L(P) = L(P)^2;$$
$$L(P) = 2L(P)^2 + 2L(P)$$

on arrive à

Théorème E.1. $\models'_L P$ *ssi* $L(P) \xrightarrow{*} 1$.

Références

[1] Buchberger, B *Gröbner Basis: An Algorithmic Method in Polynomial Ideal Theory.* Dans "Recent Trends in Multidimensional Systems Theory" (ed. N.K. Bose). Reidel, 1985, pp. 184-232.

[2] Chazarain, J. *The Lady, the Tiger and the Gröbner Basis.* Preprint n. 100 Université de Nice, mars, 1986.

[3] Hsiang, J., Dershowitz, N. *Rewrite Methods for Clausal and Nonclausal Theorem Proving.* Proc. 10th ICALP, July 1983.

[4] Kapur, D., Narendran, P. *An Equational Approach to Theorem Proving in First-Order Predicate Calculus.* Unplublished manuscript, G.E. Lab.,april, 1984.

[5] Rescher, N. *Many-valued Logic.* McGraw-Hill, 1969.

[6] Stone, M. *The Theory of Representation for Boolean Algebras.* Trans. AMS, 40, 1936.