le cnam

Algèbre de Boole et Probabilités

Cours 14 Équations booléennes

• Motivation

De nombreux problèmes appliqués conduisent à la résolution d'équations booléennees. Citons par exemple les problèmes dits de couverture où on doit recouvrir un ensemble donné par une famille de sous-ensembles, les questions de planification en intelligence artificielle, l'élaboration de la preuve automatique d'un théorème, les outils de preuve de cohérence d'un logiciel, les problèmes comme celui du jeu de "sudoku" qui se généralisent sous la forme de "Boolean SAT-isfiability Problem", ou problème de satisfaisabilité booléenne, la cohérerence d'un circuit de portes logiques, *etc.*

Par exemple, les deux circuits de la Figure 1 donent lieu aux équations $x \wedge \overline{x} = 1$ et $x \wedge y = 1$. La première équation n'a pas de solution puisque pour toute variable booléenne x, on a $x \wedge \overline{x} = 0$. La second équation a pour solution $x = y = 1$.

Figure 1. Quelle que soit la variable booléenne x, le circuit de portes logiques logiques de la figure de gauche ne peut jamais fournir comme sortie la valeur "1" qui exprime la vérité. Ce n'est pas le cas pour la porte de la figure de droite : avec $x = y = 1$, on réussit à imposer $x \wedge y = 1$.

• Étude d'un exemple

On se donne la fonction f de trois variables booléennes a, b et c définie par $f(a,b,c) = (a \vee b \vee c)\,(\overline{a} \vee \overline{b} \vee c)\,(a \vee \overline{b} \vee \overline{c})\,(\overline{a} \vee b \vee \overline{c})$. Le problème présenté Figure 2 est équivalent à la résolution de l'équation $f(a,b,c) = 1$.

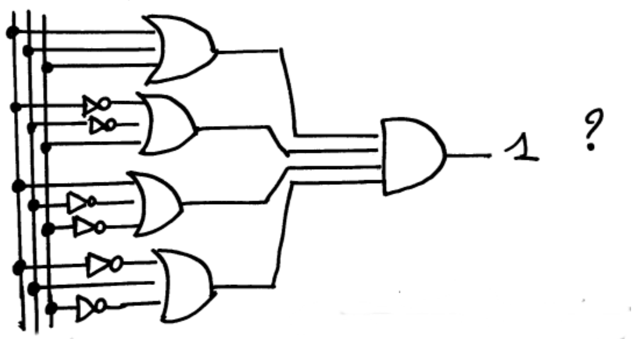

Figure 2. Est-il possible de trouver des valeurs pour les variables booléennes a, b et c de sorte que la sortie de ce réseau de portes logiques soit égale à 1 ?

François Dubois, janvier 2022.

a	0	0	0	0	1	1	1	1
b	0	0	1	1	0	0	1	1
c	0	1	0	1	0	1	0	1
$a \vee b \vee c$	0	1	1	1	1	1	1	1
$\overline{a} \vee \overline{b} \vee c$	1	1	1	1	1	1	0	1
$a \vee \overline{b} \vee \overline{c}$	1	1	1	0	1	1	1	1
$\overline{a} \vee b \vee \overline{c}$	1	1	1	1	1	0	1	1
$f(a, b, c)$	0	1	1	0	1	0	0	1

Table 1. Table de vérité de la fonction booléenne f définie par
$f(a, b, c) = (a \vee b \vee c)\,(\overline{a} \vee \overline{b} \vee c)\,(a \vee \overline{b} \vee \overline{c})\,(\overline{a} \vee b \vee \overline{c})$.

Nous pouvons commencer par construire une table de vérité de la fonction f (Table 1). Il est alors facile de constater à la lecture de la table de vérité de la fonction f que l'équation $f(a, b, c) = 1$ a exactement quatre solutions : 001, 010, 100 et 111.

On peut aussi utiliser l'algèbre de Boole et transformer l'expression de f en une somme de produits. On écrit $f(a, b, c) = g(a, b, c)\, d(a, b, c)$ avec $g(a, b, c) = (a \vee b \vee c)\,(\overline{a} \vee \overline{b} \vee c)$ et $d(a, b, c) = (a \vee \overline{b} \vee \overline{c})\,(\overline{a} \vee b \vee \overline{c})$. On a alors
$g(a, b, c) = a\overline{b} \vee ac \vee \overline{a}b \vee bc \vee \overline{a}c \vee \overline{b}c \vee c \; = a\overline{b} \vee \overline{a}b \vee c$ et
$d(a, b, c) = ab \vee a\overline{c} \vee \overline{a}\overline{b} \vee \overline{b}\overline{c} \vee \overline{a}\overline{c} \vee b\overline{c} \vee \overline{c} \; = ab \vee \overline{a}\overline{b} \vee \overline{c}$. On en déduit
$f(a, b, c) = g(a, b, c)\, d(a, b, c) = (a\overline{b} \vee \overline{a}b \vee c)\,(ab \vee \overline{a}\overline{b} \vee \overline{c})$
$\qquad = a\overline{b}\overline{c} \vee \overline{a}b\overline{c} \vee abc \vee \overline{a}\overline{b}c$. On a $f(a, b, c) = 1$ si et seulement si l'un des quatre produits de cette expression est égal à 1, c'est à dire si
$(a, b, c) = (1, 0, 0)$ ou $(a, b, c) = (0, 1, 0)$ ou $(a, b, c) = (1, 1, 1)$ ou $(a, b, c) = (0, 0, 1)$. On retrouve à l'ordre près la liste des solutions obtenues grâce aux tables de vérité.

- Cas où la résolution est simple

On veut résoudre une équation de la forme $f(x_1, x_2, \ldots, x_n) = 1$ avec une fonction booléenne f qui s'écrit comme somme de produits, c'est à dire $f = \vee_{j=1}^{m} p_j$. On a $f(x_1, x_2, \ldots, x_n) = 1$ si et seulement si $(p_1 = 1)$ ou $(p_2 = 1)$ ou... ou $(p_m = 1)$. Il suffit alors d'expliciter la solution de l'équation $(p_j = 1)$ pour les m produits p_j.

Dans l'exemple précédent, on a une somme de mintermes :
$f(a, b, c) = a\overline{b}\overline{c} \vee \overline{a}b\overline{c} \vee abc \vee \overline{a}\overline{b}c$. L'égalité à 1 des différents mintermes conduit immédiatement à la solution proposée plus haut.

Autre exemple avec $f(a, b, c) = ab \vee \overline{c}$. L'équation $f(a, b, c) = 1$ est équivalente à $ab = 1$ ou $\overline{c} = 1$, c'est à dire $a = b = 1$ ou $c = 0$. La liste des solutions s'explicite alors facilement ; l'équation $f(a, b, c) = 1$ a pour solutions 111, 110, 010, 000, 100. On constate que la solution $(a, b, c) = (1, 1, 0)$ satisfait aux deux équations.

- Comment se ramener au cas où la résolution est simple

On se donne quatre fonctions booléennes f_j de n variables pour $1 \leq j \leq 4$. On a donc
$f_j = f_j(x_1, x_2, \ldots, x_n)$. On suppose qu'on doit résoudre un système de quatre équations qui s'écrivent sous la "forme canonique" $f_j(x_1, x_2, \ldots, x_n) = 1$, ce pour toute valeur de j :
$f_1(x_1, x_2, \ldots, x_n) = 1,\; f_2(x_1, x_2, \ldots, x_n) = 1,\; f_3(x_1, x_2, \ldots, x_n) = 1,\; f_4(x_1, x_2, \ldots, x_n) = 1.$

Proposition. Les quatre équations $f_1 = 1$, $f_2 = 1$, $f_3 = 1$, $f_4 = 1$ sont équivalentes à l'unique équation $(f_1 f_2 f_3 f_4)(x_1, x_2, ..., x_n) = 1$.
On peut ramener un système de plusieurs équations écrites sous forme canonique $f_j = 1$ à une seule équation obtenue avec la fonction produit $f = f_1 f_2 f_3 f_4$. Il suffit ensuite de résoudre l'équation $f(x_1, x_2, ..., x_n) = 1$.

La preuve de cette proposition résulte des propriétés de la conjonction "et". On a $f_1 f_2 f_3 f_4 = 1$ si et seulement si $f_j = 1$ pour toute valeur de j. Le cas général d'un nombre quelconque d'équations se traite de façon similaire.

- Rappels d'algèbre de Boole

Dans ce paragraphe, nous ne cherchons pas à donner un catalogue exhaustif des propriétés des principaux opérateurs logiques ; mais juste pointer du doigt des simplifications possibles qui ne sautent pas toujours au yeux.
On a bien sûr d'abord les relations classiques $a \vee a = a$, $aa = a \wedge a = a$, $a\overline{a} = a \wedge \overline{a} = 0$ et $a \vee \overline{a} = 1$.
On dispose des lois de De Morgan : $\overline{ab} = \overline{a} \vee \overline{b}$ et $\overline{a \vee b} = \overline{a} \wedge \overline{b} = \overline{a}\,\overline{b}$.
On a aussi la règle d'absorption $a \vee ab = a$; en effet, $a \vee ab = a(1 \vee b) = a \wedge 1 = a$.
Cette règle prend aussi la forme un peu moins intuitive suivante : $a \vee \overline{a}b = a \vee b$. Cette relation résulte du calcul suivant : $a \vee \overline{a}b = a \vee ab \vee \overline{a}b = a \vee (a \vee \overline{a})b = a \vee b$.
Enfin, un produit de la forme $(a \vee b)(a \vee c)$ se transforme en $a \vee bc$ puisqu'on a
$(a \vee b)(a \vee c) = aa \vee ac \vee ab \vee bc = (a \vee ac \vee ab) \vee bc = a \vee bc$.

L'inégalité $f \leq g$ de deux fonctions booléennes est équivalente à chacune des quatre relations suivantes : $f \vee g = g$, $f \wedge g = f$, $\overline{f} \vee g = 1$, $f \wedge \overline{g} = 0$.
La preuve de cette propriété est d'abord une conséquence des propriétés fondamentales des treillis. D'une part $f \leq g$ équivaut à $\sup(f, g) = f \vee g = g$ et d'autre part, $f \leq g$ équivaut à $\inf(f, g) = f \wedge g = f$, ce qui établit les deux premiѐres relations.
Si $f \leq g$, alors $\overline{f} \vee g = \overline{f} \vee (f \vee g) = (\overline{f} \vee f) \vee g = 1$. Réciproquement, si $\overline{f} \vee g = 1$, alors $f(\overline{f} \vee g) = f$, c'est à dire $fg = f$, une des relations qui prouvent l'équivalence avec $f \leq g$.
Enfin, si $f \leq g$, alors $f \wedge \overline{g} = (f \wedge g) \wedge \overline{g} = f \wedge (g \wedge \overline{g}) = 0$ et si $f \wedge \overline{g} = 0$, alors $f\overline{g} \vee g = g$.
Il suffit de remarquer que selon l'une des règles d'absorption énoncées juste au-dessus,
$f\overline{g} \vee g = f \vee g$ et en déduire $f \vee g = g$, c'est à dire $f \leq g$.

- Théorème : transformation d'une équation en une équation sous forme canonique

Si f et g sont des fonctions booléennes arbitraires, la relation $f = g$ est équivalente à la relation $fg \vee \overline{f}\,\overline{g} = 1$.
Si $f = g$, on a d'une part $fg = ff = f$ et d'autre part $\overline{f} = \overline{g}$ donc $\overline{f}\,\overline{g} = \overline{f}$. On en déduit que $fg \vee \overline{f}\,\overline{g} = f \vee \overline{f} = 1$. Réciproquement, si la relation $fg \vee \overline{f}\,\overline{g} = 1$ est vraie, on a d'une part $(fg \vee \overline{f}\,\overline{g})f = f$, donc $fg = f$. On a d'autre part $(fg \vee \overline{f}\,\overline{g})g = g$ et $fg = g$. Les deux conclusions partielles expriment que $f = fg = g$ et la propriété est établie. □

- Un exemple classique

Il s'agit du système de trois équations à quatre inconnues $a(b \vee d) = 1$, $\overline{a} \vee \overline{d} = bc$ et
$\overline{a}c \vee bd = 0$. Une table de vérité permet de donner la solution de ces équations booléennes.

a	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
b	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
c	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
d	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$b \vee d$	0	1	0	1	1	1	1	1	0	1	0	1	1	1	1	1
$a(b \vee d)$	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1
$\overline{a} \vee \overline{d}$	1	1	1	1	1	1	1	1	1	0	1	0	1	0	1	0
$b\,c$	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1
$\overline{a} \vee \overline{d} = b\,c$	0	0	0	0	0	0	1	1	0	1	0	1	0	1	1	0
$\overline{a}\,c$	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0
$b\,d$	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1
$\overline{a}\,c \vee b\,d = 0$	1	1	0	0	1	0	0	0	1	1	1	1	1	0	1	0
système de trois équations	0	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0

Table 2. Résolution du système booléen $a(b \vee d) = 1$, $\overline{a} \vee \overline{d} = b\,c$ et $\overline{a}\,c \vee b\,d = 0$.

Il suffit ensuite de lire les trois solutions qui correspondent à la valeur “1” sur la dernière ligne : 1001, 1011, 1110.

On peut étudier le système de trois équations en mettant d'abord en évidence les solutions de chacune des équations avec un diagramme de Karnaugh. Comme chacune des équations a une structure spécifique, nous faisons trois diagrammes de Karnaugh pour chacune des équations aux Figures 3, 4 et 5. Puis nous prenons aux Figures 6 et 7 les parties communes aux diagrammes de Karnaugh associés à chaque équation. On peut alors lire les trois solutions sur la Figure 7 : 1001, 1011 et 1110. Ce sont bien celles obtenues avec la table de vérité.

		ab			
		00	01	11	10
cd	00			•	
	01			•	
	11			•	
	10			•	

		ab			
		00	01	11	10
cd	00				
	01			•	•
	11			•	•
	10				

		ab			
		00	01	11	10
cd	00			•	
	01			•	•
	11			•	•
	10			•	

Figure 3. Diagrammes de Karnaugh des relations booléennes $a\,b = 1$ (à gauche), $a\,d = 1$ (au milieu) et $a(b \vee d) = a\,b \vee a\,d = 1$ (à droite).

		ab			
		00	01	11	10
cd	00	•	•	•	•
	01	•	•		
	11	•	•		
	10	•	•	•	•

		ab			
		00	01	11	10
cd	00				
	01				
	11		•	•	
	10		•	•	

		ab			
		00	01	11	10
cd	00				
	01			•	•
	11		•		•
	10		•	•	

Figure 4. Diagrammes de Karnaugh des relations booléennes $\overline{a} \vee \overline{d} = 1$ (à gauche), $b\,c = 1$ (au milieu) et $\overline{a} \vee \overline{d} = b\,c$ (à droite).

		ab			
		00	01	11	10
cd	00				
	01				
	11	•	•		
	10	•	•		

		ab			
		00	01	11	10
cd	00				
	01		•	•	
	11		•	•	
	10				

		ab			
		00	01	11	10
cd	00	•	•	•	•
	01	•			•
	11				•
	10			•	•

Figure 5. Diagrammes de Karnaugh des relations booléennes $\overline{a}c = 1$ (à gauche), $bd = 1$ (au milieu) et $\overline{a}c \vee bd = 0$ (à droite).

		ab			
		00	01	11	10
cd	00			•	
	01			•	•
	11			•	•
	10			•	

		ab			
		00	01	11	10
cd	00				
	01			•	•
	11		•		•
	10		•	•	

		ab			
		00	01	11	10
cd	00	•	•	•	•
	01	•			•
	11				•
	10			•	•

Figure 6. Diagrammes de Karnaugh des équations booléennes $a(b \vee d) = 1$ (à gauche), $\overline{a} \vee \overline{d} = bc$ (au milieu) et $\overline{a}c \vee bd = 0$ (à droite).

		ab			
		00	01	11	10
cd	00				
	01				•
	11				•
	10			•	

Figure 7. Diagramme de Karnaugh des solutions du système d'équations booléennes $a(b \vee d) = 1, \overline{a} \vee \overline{d} = bc$ et $\overline{a}c \vee bd = 0$ obtenu en prenant l'intersection des trois diagrammes de la Figure 6.

Enfin, l'algèbre de Boole permet de résoudre le système $a(b \vee d) = 1, \overline{a} \vee \overline{d} = bc, \overline{a}c \vee bd = 0$. On l'écrit sous la forme $f_1 = 1,\ f_2 = 1$ et $f_3 = 1$ avec $f_1(a,b,c,d) = ab \vee ad$, $f_2(a,b,c,d) = (\overline{a} \vee \overline{d})\,bc \vee \overline{(\overline{a} \vee \overline{d})}\;\overline{bc}$ et $f_3(a,b,c,d) = \overline{(\overline{a}c \vee bd)}$. On transforme les expressions de f_2 et f_3 pour faire apparaître une somme de produits :
$f_2 = \overline{a}bc \vee bc\overline{d} \vee ad\,(\overline{b} \vee \overline{c}) \ = \overline{a}bc \vee bc\overline{d} \vee a\overline{b}d \vee a\overline{c}d$,
$f_3 = (a \vee \overline{c})\,(\overline{b} \vee \overline{d}) \ = a\overline{b} \vee \overline{b}\overline{c} \vee a\overline{d} \vee \overline{c}\overline{d}$. Il suffit maintenant d'évaluer la fonction $f = f_1\,f_2\,f_3$ et de la transformer en une somme de produits :

$$f = (ab \vee ad)\,(\overline{a}bc \vee bc\overline{d} \vee a\overline{b}d \vee a\overline{c}d)\,(a\overline{b} \vee \overline{b}\overline{c} \vee a\overline{d} \vee \overline{c}\overline{d})$$
$$= (abc\overline{d} \vee ab\overline{c}d \vee a\overline{b}d \vee a\overline{c}d)\,(a\overline{b} \vee \overline{b}\overline{c} \vee a\overline{d} \vee \overline{c}\overline{d})$$
$$= abc\overline{d} \vee a\overline{b}d \vee a\overline{b}\overline{c}d \ = abc\overline{d} \vee a\overline{b}d.$$

Les solutions sont alors faciles à expliciter. On a $f(a,b,c,d) = 1$ si et seulement si le quadruplet (a,b,c,d) est égal à une des trois chaînes de quatre bits suivantes : 1110, 1011 ou 1001. Ce sont bien les trois solutions trouvées avec les autres méthodes.

• Méthode de résolution algébrique
Si nous avons à résoudre un système de k équations booléennes, on peut suivre la procédure suivante.
1 - Écrire toutes les équations sous la forme $f_j = 1$. Pour cela, on utilise la propriété générale qui exprime qu'une équation de la forme $f = g$ est équivalent à la relation $f\,g \vee \overline{f}\,\overline{g} = 1$.
2 - Transformer le système de k équations en une seue équation équivalente. On pose
$f = f_1\, f_2 \ldots f_k$ et il suffit de résoudre l'équation $f = 1$.
3 - Transformer l'expression de la fonction booléenne f en somme de produits pour se ramener à des solutions découplées : $f = \vee_{\ell=1}^{m} p_\ell$. Alors l'équation $f = 1$ est équivalente à
$(p_1 = 1)$ ou $(p_2 = 1)$ ou ... ou $(p_\ell = 1)$ ou ... ou $(p_m = 1)$.

Exercices

• Système de deux équations
On se propose dans cet exercice de résoudre le système booléen suivant, composé des deux équations $x\,y = zt$ et $x \vee y = z \vee t$. On utilisera successivement trois méthodes classiques :
a) une table de vérité, b) un ou plusieurs diagrammes de Karnaugh, c) l'algèbre de Boole.

• Système de trois équations
On se propose maintenant de résoudre le système booléen $\overline{a} \vee c\overline{d} = b$ $a \vee \overline{c}d = b$ $\overline{c} \vee ab = 1$ successivement avec les trois méthodes classiques de l'exercice précédent :
a) table de vérité
b) diagramme de Karnaugh
c) algèbre de Boole.

• Problème de couverture
Soient $x_1 = 11$, $x_2 = 22$, $x_3 = 31$, $x_4 = 131$, $x_5 = 212$, $x_6 = 332$ et $E = \{x_1, x_2, x_3, x_, x_5, x_6\}$.
On considère les parties suivantes de E :
A_1 est l'ensemble des nombres qui finissent par 1,
A_2 est l'ensemble des nombres qui n'ont que deux chiffres,
A_3 est l'ensemble des nombres qui contiennent le chiffre 3,
A_4 est l'ensemble des nombres pairs,
A_5 est l'ensemble des nombres qui se lisent de la même façon de gauche à droite ou de droite à gauche.
L'exercice consiste à chercher comment choisir des parties A_i pour recouvrir l'ensemble E.
a) Dessiner un diagramme cartésien de 6 lignes et 5 colonnes représentant l'appartenance des éléments $x_1, x_2, x_3, x_4, x_5, x_6$ aux ensembles A_1, A_2, A_3, A_4, A_5.
On introduit des variables booléennes a_i avec $1 \leq i \leq 5$ telles que $a_i = 1$ quand la partie A_i est choisie et $a_i = 0$ sinon.
b) Écrire les 6 équations qui lient a_1, a_2, a_3, a_4 et a_5.
c) Résoudre le système précédent avec la méthode de votre choix.
d) En déduire toutes les façons de recouvrir E par des parties A_i.
e) Comment peut-on choisir le moins possible d'ensembles A_i pour recouvrir l'ensemble E ?