Chapitre 2

Éléments de logique

Une preuve mathématique d'un énoncé est une séquence valide d'implications qui commence par un ou plusieurs axiomes et termine par l'énoncé que l'on veut démontrer. Ce chapitre est consacré aux mécanismes élémentaires qui gouvernent ce procédé.

L'objet principal de notre étude sera les variables booléennes, nommé d'après le mathématicien britannique du $19^{\text{ème}}$ siècle, George Boole. Dans le langage courant, les variables booléennes correspondent à des déclarations qui peuvent être soit vraie soit fausse. Par exemple, la déclaration "la température de cette pièce est plus élevé que 21C" peut être vu comme une variable booléenne alors que "cette image est laide" non. En mathématique, une déclaration comme "tout entier positif est le produit de nombres premiers" est une variable booléenne (qui est toujours vraie dans ce cas). Un autre type de variable booléenne que vous avez peut être déjà vu en analyse est le suivant : $\forall \varepsilon > 0\, \exists \delta > 0 \colon |f(x_0) - f(x_0 - \varepsilon)| < \delta$. Ici, $f \colon \mathbb{R} \to \mathbb{R}$ et $x_0 \in \mathbb{R}$ sont des paramètres. Cette déclaration est équivalente à la suivante "f est continue à droite en x_0".

Ainsi, ce chapitre sera consacré à l'étude des variables booléennes et des fonctions sur de telles variables.

2.1. Variable et fonction booléennes

Une *variable booléenne* est un ensemble à deux éléments, souvent noté $\{0, 1\}$. En pratique, on pense à une variable booléenne X comme une boite qui peut contenir l'une ou l'autre de ces deux valeurs. Une collection $\{X_1, \ldots, X_n\}$ de n variables booléennes est l'ensemble $\{0, 1\}^n$, aussi connu sous le nom d'*hypercube* de dimension n, noté $\mathcal{H}_n$. En pratique, on peut voir $X_1, \ldots, X_n$ comme n boites qui peuvent contenir les valeurs $\{0, 1\}$ indépendamment.

Une *fonction booléenne* f de n variables est une fonction de l'hypercube $\mathcal{H}_n$ dans $\{0, 1\} = \mathcal{H}_1$. Il y a de nombreuses représentations équivalentes d'une telle fonctions booléenne. Nous allons les présenter à l'aide de la fonction f à trois variables qui associe à $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ et $(1, 1, 1)$ 1 et associe 0 aux autres entrées.

Le graphe. La façon la plus simple de représenter f est à l'aide de son graphe, donné ci-dessous :

x	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$f(x)$	0	1	1	0	1	0	0	1

La première ligne est une liste de tous les arguments possibles de la fonction et la deuxième ligne la valeur que prend la fonction sur l'argument correspondant.

La table de vérité. Une autre représentation équivalente de f est donnée par sa "table de vérité" :

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Dans cette représentation, les premières colonnes correspondent aux différents états des variables, et la dernière colonne correspond à la valeur de la fonction pour de tels arguments. Cette représentation est appelée table de vérité car la valeur 1 est souvent interprété comme "vrai" et la valeur 0 comme "faux" ;

Représentation en fibres. Dans cette représentation, on donne la liste des éléments de l'hypercube sur lesquels la fonction prend la valeur 1. On donne ainsi l'ensemble $f^{-1}(1)$:

$$\{(1,0,0),(0,1,0),(0,0,1),(1,1,1)\}.$$

Cette représentation montre que les fonctions booléennes sont essentiellement les sous-ensembles de l'hypercube.

Un avantage des deux premières représentations sur la troisième est qu'il est possible de représenter plusieurs fonctions booléenne en même temps.

Exemple 2.1. En plus de la fonctions booléenne f, considérons la fonction g de deux variables x et y qui vaut 1 ssi x et y valent tous les deux 1. La représentation simultanée de f et g par une table de vérité est :

x	y	z	$f(x,y,z)$	$g(x,y)$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	0
1	0	0	1	0
1	0	1	0	0
1	1	0	0	1
1	1	1	1	1

◇

Les trois représentations sont équivalentes dans le sens où deux fonctions booléennes sont identique ssi leur représentation dans l'une des formes donnée plus haut sont les mêmes. Plus tard dans ce chapitre nous rencontrerons des méthodes pour prouver des propriétés des fonctions booléennes qui utiliserons l'une de ces représentation.

2.2. Quelques fonctions booléennes élémentaires

La fonction $\mathbf{1}_n : \mathcal{H}_n \to \mathcal{H}_1$ est définie par $\mathbf{1}_n(x_1,\ldots,x_n) = 1$. Elle est appelée *tautologie* à n variables. Voici la table de vérité de $\mathbf{1}_1$:

x	$\mathbf{1}_1(x)$
0	1
1	1

La fonction $f : \mathcal{H}_1 \to \mathcal{H}_1$ donné par la table de vérité suivante est appelée fonction *négation*. Elle est notée $f(x) = \neg x$:

x	$\neg x$
0	1
1	0

Les fonctions à deux variables "Ou (OR) $\vee$", "Et (AND)$\wedge$", "Implication $\Rightarrow$", et "Ou-exclusif (XOR) $\oplus$" sont définies par :

x	y	$x \vee y$	$x \wedge y$	$x \Rightarrow y$	$x \oplus y$
0	0	0	0	1	0
0	1	1	0	1	1
1	0	1	0	0	1
1	1	1	1	1	0

Bien que ces fonctions sont distinctes, elles admettent des relations entre elles comme le montre le résultat suivant :

Théoréme 2.2. *On à les égalités suivantes :*

(a) $\neg(\neg x) = x$.

(b) $\neg x = \mathbf{1}_1(x) \oplus x$.

(c) $x \oplus y = (x \vee y) \wedge (\neg x \vee \neg y)$.

(d) $(x \Rightarrow y) = \neg x \vee y$.

(e) *(Loi de De Morgan)* $\neg(x \vee y) = \neg x \wedge \neg y$.

(f) *(Loi de De Morgan)* $\neg(x \wedge y) = \neg x \vee \neg y$.

(g) *(Distributivité)* $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

(h) *(Distributivité)* $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

(i) *(Distributivité)* $x \wedge (y + z) = (x \wedge y) + (x \wedge z)$.

Démonstration. On montre ces assertions en calculant la table de vérité des différentes fonctions concernées. Par définition, deux colonnes égales correspondent à la même fonction. Pour les points (a) et (b), on procède de la manière suivante :

x	$\neg x$	$\mathbf{1}_1(x)$	$\neg(\neg x)$	$\mathbf{1}_1(x) \oplus x$
0	1	1	0	1
1	0	1	1	0

Cela montre bien (a) et (b) car les tables de vérités de $\neg(\neg x)$ et x sont identique, comme le sont celles de $\neg x$ et $\mathbf{1}_1(x) \oplus x$.

Pour les points (c)–(f), on regarde les fonctions à 2 variables suivantes :

x	y	$\neg x$	$\neg y$	$\neg(x \vee y)$	$\neg(x \wedge y)$	$\neg x \vee \neg y$	$\neg x \vee y$	$\neg x \wedge \neg y$	$(x \vee y) \wedge (\neg x \vee \neg y)$
0	0	1	1	1	1	1	1	1	0
0	1	1	0	0	1	1	1	0	1
1	0	0	1	0	1	1	0	0	1
1	1	0	0	0	0	0	1	0	0

Ainsi, pour montrer (c), on compare la dernière colonne avec la table de vérité de $x \oplus y$ pour montrer que ces deux fonctions sont identiques. Les autres preuves sont similaires.

Pour la partie (g) on regarde les tables de vérité des fonctions à 3 variables suivantes :

x	y	z	$x \vee y$	$x \vee z$	$y \wedge z$	$(x \vee y) \wedge (x \vee z)$	$x \vee (y \wedge z)$
0	0	0	0	0	0	0	0
0	0	1	0	1	0	0	0
0	1	0	1	1	0	0	0
0	1	1	1	1	1	0	0
1	0	0	1	1	0	0	0
1	0	1	1	1	0	0	0
1	1	0	1	1	0	1	1
1	1	1	1	1	1	1	1

Pour la partie (h), en utilisant (g), (e) et (f) on voit que

$$\begin{aligned} \neg x \vee (\neg y \wedge \neg z) &= (\neg x \vee \neg y) \wedge (\neg x \vee \neg z) \\ &= \neg(x \wedge y) \wedge \neg(x \wedge z) \\ &= \neg((x \wedge y) \vee (x \wedge z)). \end{aligned}$$

En prenant l'opposé des deux côtés et en utilisant (e) et (f) à nouveau, on obtient

$$\begin{aligned} x \wedge \neg(\neg y \wedge \neg z) &= x \wedge (y \vee z) \\ &= (x \wedge y) \vee (x \wedge z). \end{aligned}$$

Pour la partie (i), on utilise encore une fois les tables de vérités :

x	y	z	$y+z$	$x \wedge (y+z)$	$x \wedge y$	$x \wedge z$	$x \wedge y + x \wedge z$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	0	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	0	0	1	1	0

Cela prouve l'assertion. □

2.3. Description ensembliste des fonctions booléennes

En comparant les résultats de la section précédente avec ceux du premier chapitre, on peut voir une certaine similarité. Il y a une bonne raison à cela comme on va le voir ici.

Théoréme 2.3. *Soit f et g des fonctions booléennes sur n variables, pour un certain $n \geq 1$. Dénotons $f^{-1}(1)$ par F et $g^{-1}(1)$ par G. On a :*

(a) *Si $h(x) = \neg f(x)$, alors $h^{-1}(1) = F^c$, où le complémentaire est pris par rapport a l'hypercube $\mathcal{H}_n$.*

(b) *Si $h(x) = f(x) \vee g(x)$, alors $h^{-1}(1) = F \cap G$.*

(c) *Si $h(x) = f(x) \wedge g(x)$, alors $h^{-1}(1) = F \cup G$.*

(d) *Si $h(x) = f(x) \oplus g(x)$, alors $h^{-1}(1) = F \Delta G$, où Δ est la différence symétrique (voir Exercice 3 de la feuille 1).*

Démonstration. (a) Pour tout $x \in \mathcal{H}_n$, on a $h(x) = 0$ ssi $f(x) = 1$, et l'assertion en découle.

(b) On a $h(x) = 1$ si $f(x) = 1$ ou si $g(x) = 1$. Donc, $x \in h^{-1}(1)$ si $x \in F$ ou $x \in G$, ce qui implique l'assertion.

(c) Preuve similaire à (b).

(d) On a $h(x) = 1$ ssi $f(x) \neq g(x)$. Ainsi, $x \in h^{-1}(1)$ ssi $x \in (F - G) \cup (G - F) = F \Delta G$. □

Cette connection entre les fonctions booléennes et la théorie des ensembles réduits la plupart des résultats du théorème 2.2 à leur pendant ensembliste donné au chapitre 1. On va illustrer cela pour les parties (c) et (e) de ce théorème.

Pour prouver la partie (c), supposons que f et g sont des fonctions booléennes. Notons de plus $F := f^{-1}(1)$ et $G := g^{-1}(1)$, et soit $h(x) = f(x) \oplus g(x)$. Alors, nous avons vu que $h^{-1}(1) = F \Delta G$. Il suffit donc de montrer que cet ensemble est égal à $(F \cup G) \cap (F^c \cup G^c)$. C'est justement ce qui est demander dans l'exercice (3)(f) sur la première feuille.

Pour prouver la partie (3), soit encore f et g des fonctions booléennes comme ci dessus. On doit alors montrer que $(F \cup G)^c = F^c \cap G^c$, ce que l'on a déjà prouvé dans le lemme 1.3.

2.4. Représentation des fonctions booléennes

Dans cette section on s'intéresse à des représentations variées des fonctions booléennes. On en a déjà vu 3 : le graphe, la table de vérité et la représentation en fibres. Un des problèmes avec ces représentations est que leur taille grossit très vite. En fait, si la fonction a n variables, alors son graphe et sa table de vérité on besoins de l'ordre de $n2^n$ entrées. De même, la taille de la représentation en fibre est proportionnelle à n fois la taille de la fibre, qui peut aussi être dans le pire cas 2^n.

Exemple 2.4. Soit la fonction booléenne à n variables f qui vaut 1 pour tous les $x \in \mathcal{H}_n$ qui ont un nombre impair d'entrée à 1. Alors $f^{-1}(1)$ est égal à 2^{n-1} (pourquoi ?). Mais $f(x_1, \dots, x_n) = \mathbf{1}_n(x_1, \dots, x_n) \oplus x_1 \oplus x_2 \oplus \cdots \oplus x_n$ est une représentation bien plus condensé de f (Voir Exercice**??**.) ◇

Dans cette section, nous allons voir trois nouvelles représentations des fonctions booléennes

2.4.1. La forme normale disjonctive (DNF)

Soit $x_1, \dots, x_n$ des variables booléennes. Une fonction $\lambda \in \{x_1, \neg x_1, x_2, \neg x_2, \dots, x_n, \neg x_n\}$ est appelée un *littéral* (par rapport à $x_1, \dots, x_n$). Si $\lambda_1, \dots, \lambda_m$ sont des littéraux, alors la fonction $C = \lambda_1 \wedge \lambda_2 \wedge \cdots \wedge \lambda_m$ est appelée une *clause conjonctive*.

Exemple 2.5. Soit x_1, x_2, x_3 des variables booléennes.
- x_2 et $\neg x_3$ sont des littéraux.
- x_1 est une variable booléenne, un littéral, et une clause conjonctive.
- $x_2 \wedge \neg x_3$ est une clause conjonctive, mais pas un littéral par rapport à x_1, x_2, x_3. C'est en revanche un littéral par rapport à une nouvelle variable $y := \neg x_2 \vee x_3$, car c'est la négation de cette variable par le théorème 2.2(e).

◇

Une fonction de la forme $C_1 \vee C_2 \vee \cdots \vee C_t$ où les C_i sont des clauses conjonctives est appelée une fonction sous la forme normale disjonctive (DNF). Une telle représentation, si elle existe, n'est certainement pas unique : il y à en effet un nombre infini de façons de construire une formule de la forme $C_1 \vee C_2 \vee \cdots \vee C_t$ avec n variables, car t peut potentiellement être n'importe quel entier positif. Mais il n'y a que 2^{2^n} fonctions booléennes différentes sur n variables (voir l'exercice **??**).

On montre maintenant que n'importe quelle fonction booléenne à une représentation sous forme DNF. La clef de ce résultat repose sur la représentation en fibre de la fonction et sur le théorème 2.3.

Théoréme 2.6. *Soit $f\colon \mathcal{H}_n \to \mathcal{H}_1$ une fonction booléenne à n variables. Alors, il existe $t \geq 0$ et des clauses conjonctives à n variables $C_1, \dots, C_t$ telles que $f = C_1 \vee \cdots \vee C_t$.*

Démonstration. On va commencer par montrer le théorème pour des fonctions booléennes $g\colon \mathcal{H}_n \to \mathcal{H}_1$ pour lesquelles $g^{-1}(1)$ a exactement un élément $(\varepsilon_1, \dots, \varepsilon_n)$. On définie les littéraux $\lambda_1, \dots, \lambda_n$ par

$$\lambda_i := \begin{cases} x_i & \text{if } \varepsilon_i = 1 \\ \neg x_i & \text{sinon.} \end{cases}$$

On veut montrer g est égal à la clause $\lambda_1 \wedge \cdots \wedge \lambda_n$. Pour voir cela, notez que cette clause est 1 ssi tous les λ_i sont égaux à 1, et chaque λ_i vaut 1 seulement sur ε_i.

Soit maintenant $f\colon \mathcal{H}_n \to \mathcal{H}_1$ une fonction booléenne quelconque et soit $F := f^{-1}(1)$. Supposons que

$$F = \{(\varepsilon_{11}, \dots, \varepsilon_{1n}), \dots, (\varepsilon_{t1}, \dots, \varepsilon_{tn})\},$$

avec $t = |F|$ (si $F = \emptyset$, on prend $t = 0$). Pour chaque éléments $(\varepsilon_{i1}, \dots, \varepsilon_{in})$ on définit la clause C_i comme décrit plus haut. Comme $\{(\varepsilon_{i1}, \dots, \varepsilon_{in})\} = C_i^{-1}(1)$, le théorème 2.3(c) implique que la fonction $C_1 \vee \cdots \vee C_t$ a la même représentation par fibre que f, et nous avons fini. □

Exemple 2.7. Regardons la preuve du théorème 2.6 dans le cas d'une fonction à trois variables f avec

$$f^{-1}(1) = \{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}.$$

Pour chaque éléments de cet ensemble, on construit une clause comme décrit dans la preuve ci-dessus.

$$\begin{aligned} (0,0,0) &\to \neg x_1 \wedge \neg x_2 \wedge \neg x_3 \\ (0,1,1) &\to \neg x_1 \wedge x_2 \wedge x_3 \\ (1,0,1) &\to x_1 \wedge \neg x_2 \wedge x_3 \\ (1,1,0) &\to x_1 \wedge x_2 \wedge \neg x_3 \end{aligned}$$

On obtient alors

$$f = (\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3).$$

◇

Étant donné la preuve du théorème et l'exemple ci-dessus, il semblerait que la représentation DNF d'une fonction ne soit pas nécessairement plus courte que ça représentation en fibre. C'est vrai si l'on suit la règle de construction à la lettre. Néanmoins, il est parfois possible d'obtenir une représentation plus courte.

Exemple 2.8. Soit la fonction $f\colon \mathcal{H}_3 \to \mathcal{H}_1$ avec

$$f^{-1}(1) = \{(1,1,0), (1,1,1), (0,1,1), (0,0,1)\}.$$

Par la procédure du théorème 2.6 on obtient

$$f = (x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3).$$

En regroupant les deux premiers termes cela donne

$$(x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge x_3) = (x_1 \wedge x_2) \vee (x_3 \wedge \neg x_3) = (x_1 \wedge x_2) \vee 0 = (x_1 \wedge x_2).$$

De manière similaire

$$(\neg x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3) = (\neg x_1 \wedge x_3) \wedge (x_2 \vee \neg x_2) = (\neg x_1 \wedge x_3) \wedge 1 = (\neg x_1 \wedge x_3).$$

Ainsi,

$$f = (x_1 \wedge x_2) \vee (\neg x_1 \wedge x_3).$$

◇

L'optimisation des fonctions booléennes est un domaine de recherche très actif avec d'immenses applications en conception matérielle, mais nous n'en parlerons pas plus ici. On mentionne seulement que la plupart des fonctions booléennes on une "grande" représentation DNF, c'est à dire que leur plus petite représentation DNF a un nombre de clauses qui est exponentiel en n.

2.4.2. La forme normale conjonctive (CNF)

Soit à nouveaux $x_1, \ldots, x_n$ des variables booléennes. Si $\lambda_1, \ldots, \lambda_m$ sont des littéraux par rapport à ces variables, une fonction $D = \lambda_1 \vee \lambda_2 \vee \cdots \vee \lambda_m$ est appelée une *clause disjonctive*. Une fonction $f\colon \mathcal{H}_n \to \mathcal{H}_1$ est dites sous *forme normale conjonctive (CNF)* si $f = D_1 \wedge \cdots \wedge D_t$ pour des clauses disjonctives $D_1, \ldots, D_t$.

Exemple 2.9. Soit x_1, x_2, x_3 des variables booléennes.

- x_1 est une variable booléenne, un littéral est une clause disjonctive.
- $x_2 \vee \neg x_3$ est une clause disjonctive, mais n'est pas un littéral par rapport à x_1, x_2, x_3. En revanche, c'est un littéral par rapport à une nouvelle variable $y := \neg x_2 \wedge x_3$, car c'est la négation de cette variable par le théorème 2.2(f).

◇

Le résultats suivant est immédiat.

Lemme 2.10. *Soit C une clause conjonctive par rapport aux variables booléennes $x_1, \ldots, x_n$. Alors $\neg C$ est une clause disjonctive par rapport aux mêmes variables. De manière similaire, si D est une clause disjonctive, alors $\neg D$ est une clause conjonctive.*

Démonstration. Soit $C = \lambda_1 \wedge \cdots \wedge \lambda_m$ où les λ_i sont des littéraux. Alors, $\neg C = \neg\lambda_1 \vee \cdots \vee \neg\lambda_m$ par application de la loi de De Morgan, théorème 2.2(f). Comme la négation d'un littéral est aussi un littéral, on voit que $\neg C$ est une clause disjonctive. L'autre résultat en découle immédiatement. □

En utilisant la représentation DNF des fonctions booléennes, on peut aisément montrer l'existence de la représentation CNF.

Théoréme 2.11. *Soit $f\colon \mathcal{H}_n \to \mathcal{H}_1$ une fonction booléenne à n variables. Alors, il existe $t \geq 0$ et des clauses disjonctives sur n variables $D_1, \ldots, D_t$ telles que $f = D_1 \wedge \cdots \wedge D_t$.*

Démonstration. Considérons la fonction $g = \neg f$, i.e., $g(x_1, \ldots, x_n) = \neg f(x_1, \ldots, x_n)$. Par application du théorème 2.6 cette fonction peut être représenté sous forme DNF : $g = C_1 \vee C_2 \vee \cdots \vee C_t$. Ainsi, $\neg g = f = \neg C1 \wedge \cdots \wedge \neg C_t$ par le théorème 2.2(e). Avec le lemme 2.10 chaque $\neg C_i$ est une clause disjonctive et le résultat en découle. □

2.4.3. La représentation comme fonction polynomiale

Une autre représentation des fonctions booléennes qui est beaucoup utilisée est la représentation comme fonctions polynomiale. Comme le suggère le nom, elle est relié aux polynômes, un concept que nous allons brièvement revoir.

Le *corps fini à deux éléments* est l'ensemble $\{0,1\}$ munit des deux opérations "$\cdot$" (multiplication) et $\oplus$ (addition) défini par la table suivante :

$\cdot$	0	1
0	0	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	0

.

Comme il est facile de voir, l'opération "$\cdot$" est équivalente au "ET" ($\wedge$) et l'opération plus est la même que l'opération XOR vu plus haut. Dans le théorème 2.2(i) nous avons vu que ces deux opérations sont distributives. C'est à dire que si f, g, et h sont des fonctions booléennes, alors

$$f \cdot (g \oplus h) = f \cdot g \oplus f \cdot h.$$

Comme dans l'arithmétique standard, on omet souvent le "$\cdot$" des expressions. Par exemple, la formule ci-dessus est souvent écrite $f(g \oplus h) = fg \oplus fh$.

On écrit f^m pour la multiplication de m termes f entre eux et mf pour l'addition de m termes f entre eux. Un *monôme* M en les variables booléennes $x_1, \ldots, x_n$ est un produit de la forme $M = \prod_{i \in S} x_i$, où S est un sous-ensemble de $\underline{n}$. Nous écrirons aussi par simplicité 1 à la place de $\mathbf{1}_n$ quand n est évident d'après le contexte.

Proposition 2.12. *Soit f, g, h des fonctions booléennes en les variables $x_1, \ldots, x_n$, Soit $1 := \mathbf{1}_n$, et soit $0 = \neg \mathbf{1}_n$, c'est à dire la fonction de $\mathcal{H}_n \to \mathcal{H}_1$ qui vaut toujours 0.*

(a) *Pour tout $m \geq 1$ on a $f^m = f$.*

(b) *on a $mf = f$ si m est impair, et $mf = 0$ si m est pair.*

(c) *Soit S et T des sous-ensembles de $\underline{n}$ et $f = \prod_{i \in S} x_i$ et $g = \prod_{j \in T} x_j$ des monômes. Alors $fg = \prod_{k \in S \cup T} x_k$ est aussi un monôme.*

(d) *$f \vee g = fg \oplus f \oplus g$.*

(e) *Si f et g sont des sommes de monômes, il en est de même pour fg.*

(f) *Si f et g sont des sommes de monômes, il en est de même pour $f \vee g$.*

(g) *Soit $D = \lambda_1 \vee \ldots \vee \lambda_t$ une clause disjonctive. Ils existent des monômes $M_1, \ldots, M_m$ tels que $D = M_1 \oplus \cdots \oplus M_m$.*

Démonstration. (a) il suffit de remarquer que $f \wedge f = f$.

(b) Il suffit de remarquer que $f \oplus f = 0$ d'après la définition de $\oplus$.

(c) On a $fg = \prod_{i \in S \cap T} x_i^2 \prod_{i \in (S \cup T) \setminus (S \cap T)} x_i$. Et d'après (a) on sait que $x_i^2 = x_i$, d'où le résultat.

(d) On a

$$\begin{array}{rcll} 1 \oplus (f \vee g) & = & \neg(f \vee g) & \\ & = & (\neg f \wedge \neg g) & \text{(loi de De Morgan)} \\ & = & (1 \oplus f)(1 \oplus g) & \text{(théorème 2.2(b))} \\ & = & 1 \oplus f \oplus g \oplus fg & \text{(par distributivité)} . \end{array}$$

Ajouter 1 des deux côtés et appliquer (b) donne le résultat.

(e) Supposons que $f = M_1 \oplus \cdots \oplus M_\ell$ et $g = N_1 \oplus \cdots \oplus N_d$, ou les M_i et les N_j sont des monômes en $x_1, \ldots, x_n$. Par distributivité, $fg = \sum_{i=1}^{\ell} \sum_{j=1}^{d} M_i N_j$. Chacun des $M_i N_j$ est un monômes d'après (c) ce qui implique le résultat.

(f) Supposons que $f = M_1 \oplus \cdots \oplus M_\ell$ et $g = N_1 \oplus \cdots \oplus N_d$, ou les M_i et les N_j sont des monômes en $x_1, \ldots, x_n$. D'après la partie (d), on a $f \vee g = fg \oplus f \oplus g$. Comme fg est une somme de monôme d'après (e), et que f et g sont des sommes de monômes par hypothèse, on en déduit le résultat.

(g) Sans perte de généralité on suppose $\lambda_i \in \{x_i, \neg x_i\}$ pou $i = 1, \ldots, t$. Posons $\varepsilon_i \in \{0,1\}$ avec $\varepsilon_i = 1$ ssi $\lambda_i = \neg x_i$. Alors $\lambda_i = \varepsilon_i \oplus x_i$ ce qui montre que λ_i est une somme de monômes. Ainsi, D est bien une somme de monôme par (f) et par induction. □

Théoréme 2.13. *Soit $f \colon \mathcal{H}_n \to \mathcal{H}_1$ une fonction booléenne sur n variables. Il existe des monômes $M_1, \ldots, M_t$ tels que $f = M_1 \oplus \cdots \oplus M_t$.*

Démonstration. Soit $f = D_1 \wedge \cdots \wedge D_t$ une représentation sous forme CNF de f. Pour chaque clauses disjonctives D_i, soit P_i une représentation de D_i comme une somme de monômes (cf la proposition 2.12(e)). Alors $f = P_1 \cdot P_2 \cdots P_t$. □

Exemple 2.14. Considérons encore la fonction f à trois variables de l'exemple 2.7 :

$$f = (\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3).$$

On a

$$\begin{aligned} \mathbf{1}_3 \oplus f &= \neg\Big((\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)\Big) \\ &= \neg(\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \wedge \neg(\neg x_1 \wedge x_2 \wedge x_3) \wedge \neg(x_1 \wedge \neg x_2 \wedge x_3) \wedge \neg(x_1 \wedge x_2 \wedge \neg x_3). \end{aligned}$$

D'après la proposition 2.12(c) on a

$$\begin{aligned} \neg(\neg x_1 \wedge \neg x_2 \wedge \neg x_3) &= 1 \oplus (1 \oplus x_1)(1 \oplus x_2)(1 \oplus x_3) \\ &= x_1 \oplus x_2 \oplus x_3 \oplus x_2x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3 \\ \neg(\neg x_1 \wedge x_2 \wedge x_3) &= 1 \oplus (1 \oplus x_1)x_2x_3 = 1 \oplus x_2x_3 \oplus x_1x_2x_3 \\ \neg(x_1 \wedge \neg x_2 \wedge x_3) &= 1 \oplus x_1(1 \oplus x_2)x_3 = 1 \oplus x_1x_3 \oplus x_1x_2x_3 \\ \neg(x_1 \wedge x_2 \wedge \neg x_3) &= 1 \oplus x_1x_2(1 \oplus x_3) = 1 \oplus x_1x_2 \oplus x_1x_2x_3. \end{aligned} \tag{2.1}$$

Pour calculer le produit, on commence par celui des trois derniers termes. En utilisant la proposition 2.12(c) plusieurs fois :

$$\begin{aligned} (1 \oplus x_2x_3 \oplus x_1x_2x_3)(1 \oplus x_1x_3 \oplus x_1x_2x_3) &= 1 \oplus x_1x_3 \oplus x_1x_2x_3 \oplus \\ &\quad x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2x_3 \oplus \\ &\quad x_1x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2x_3 \\ &= 1 \oplus x_1x_3 \oplus x_2x_3, \end{aligned}$$

où pour la dernière égalité on utilise la proposition 2.12(b). De manière similaire,

$$\begin{aligned} (1 \oplus x_1x_3 \oplus x_2x_3)(1 \oplus x_1x_2 \oplus x_1x_2x_3) &= 1 \oplus x_1x_2 \oplus x_1x_2x_3 \oplus \\ &\quad x_1x_3 \oplus x_1x_2x_3 \oplus x_1x_2x_3 \oplus \\ &\quad x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2x_3 \\ &= 1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3. \end{aligned}$$

Notez maintenant que

$$\begin{aligned} x_2x_3(x_1 \oplus x_2 \oplus x_3 \oplus x_2x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3) &= x_1x_2x_3 \oplus x_2x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus \\ &\quad x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_2x_3 \\ &= x_2x_3 \end{aligned}$$

Et de manière similaire

$$T(x_1 \oplus x_2 \oplus x_3 \oplus x_2x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3) = T$$

pour tout $T \in \{x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\}$. Ainsi, le produit $1 \oplus f$ de tous les termes de gauche dans l'équation (2.1) devient :

$$\begin{aligned} 1 \oplus f &= (x_1 \oplus x_2 \oplus x_3 \oplus x_2x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3)(1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3) \\ &= x_1 \oplus x_2 \oplus x_3 \oplus x_2x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \\ &= x_1 \oplus x_2 \oplus x_3. \end{aligned}$$

Ajouter 1 aux deux côté de l'équation implique

$$f = 1 \oplus x_1 \oplus x_2 \oplus x_3.$$

◇

La simplification d'une fonction booléenne donnée (comme l'on vient de le faire) est une tache très difficile. Même s'il existe des outils pour faire de la simplification automatique, le problème est prouvé difficile (avec un sens précis dont on ne parlera pas ici).

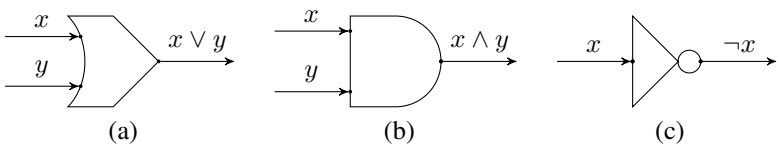


Figure 2.1 – Schémas des portes pour les opération OU, ET, et la Négation

2.5. Représentation d'une fonction booléenne par diagramme logique

Les fonctions booléennes sont au cœur des appareils électroniques modernes, comme les processeurs de nos ordinateurs. Le but principal de tels appareils peut se voir comme un calcul de certaines fonctions booléennes. Par exemple, regardons l'addition de deux entier sur un bits, c'est à dire l'addition de 0 et 1. Soit a et b deux entier sur 1 bit. Leur addition est un autre entier de la forme suivante :

$$a + b = 2c + d,$$

où c et d sont zéro ou un. En fait, c et d sont des fonctions booléennes en les variables a et b. On peut les définir comme suit :

$$d = a \oplus b, \quad c = a \wedge b = ab.$$

L'élément c est ce que nous connaissons depuis l'école primaire comme "retenue". Regardons maintenant l'addition d'entier de l'intervalle $\{0, 1, 2, 3\}$. De tels entiers peuvent se représenter de manière unique sous la forme $2x + y$ où x et y sont des entiers sur 1 bit. S'il on additionne deux entiers de cet intervalle, on obtient

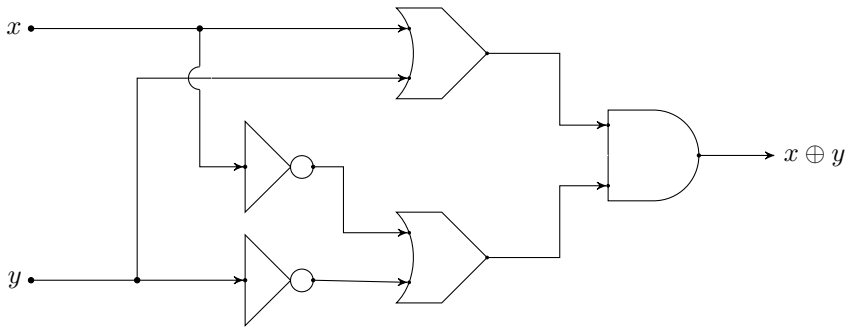
$$2x_1 + y_1 + 2x_2 + y_2 = 4z_3 + 2z_2 + z_1,$$

où encore une fois, z_1, z_2, z_3 sont des entiers du même intervalle. On aussi

$$z_1 = y_1 \oplus y_2, \quad z_2 = x_1 \oplus x_2 \oplus y_1 y_2, \quad z_3 = (x_1 \oplus x_2) y_1 y_2.$$

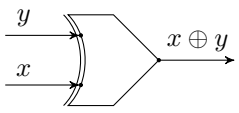
Ces formules s'obtiennent en examinant l'algorithme classique d'addition : $y_1 \oplus y_2$ est l'addition du premier chiffre de chaque nombre et $y_1 y_2$ est la retenue de cette opération. En continuant, $x_1 \oplus x_2 \oplus y_1 y_2$ est le deuxième chiffre du résultat. Finalement, $(x_1 \oplus x_2) y_1 y_2$ est la retenue de cette dernière opération.

Les fonctions booléennes sont souvent représentée sous forme de diagrammes logiques. De tels diagrammes considère certains éléments de bases comme donnés et les assembles en des structures plus compliquée. Par exemple, la figure 2.1 donne une description schématique des fonctions OU, ET et de la négation. Si l'on prend ces fonctions comme porte de base, une représentation possible de la fonction XOR est :

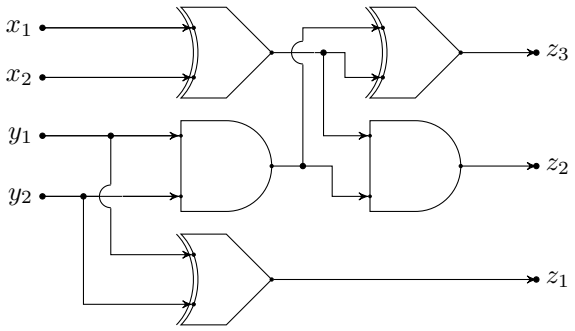


Les deux entrées x et y de la fonction sont dans un premier temps dupliquées. Les deux répliques du haut sont envoyées dans une porte OU pour produire $x \vee y$. Les deux répliques du bas sont d'abord inversées (négation) puis envoyées dans une porte OU pour produire $\neg x \vee \neg y$. Finalement, ces deux valeurs sont combinées par une porte ET pour produire $(x \vee y) \wedge (\neg x \vee \neg y)$ qui est la même chose que $x \oplus y$.

Supposons que le diagramme suivant correspond à la porte XOR :



Alors l'addition d'entiers de l'intervalle $\{0, 1, 2, 3\}$ est décrit par le diagramme suivant :



2.6. Exemple : Description booléenne des Sudokus 4×4 valides

Vous connaissez sûrement le jeu Sudoku, inventé par Howard Garns en 1979 : On vous donne une grille 9 formée de 9 sous-carré 3×3. Le but est de remplir la grille avec les chiffres de 1 à 9 de telle manière que sur chaque ligne, colonne et sous-carré 3×3 chaque chiffre apparaisse une et une seule fois.

On considère ici une version plus petite : à la place d'une grille 9×9, on considère une grille 4×4 formée de 4 grilles 2×2. Et on cherche a placer les chiffres de 1 à 4. Voici un exemple :

4	2	3	1
3	1	2	4
2	4	1	3
1	3	4	2

Dans cette section, nous allons construire des équations booléennes dont les solutions sont en bijection avec les grilles 4×4 valides.

Dans ce but, on introduit pour chaque position (i, j) de la grille 4 variables $p_{ij1}, p_{ij2}, p_{ij3}, p_{ij4}$. Leur significations est la suivante : La position (i, j) de la grille vaut ℓ ssi $p_{ij\ell} = 1$ (et les 3 autres variables sont à 0). Pour exprimer cette condition, on introduit la fonction booléenne suivante :

$$G(x_1, x_2, x_3, x_4) := (\neg x_1 \wedge x_2 \wedge x_3 \wedge x_4) \vee (x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4) \vee (x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \vee (x_1 \wedge x_2 \wedge x_3 \wedge \neg x_4).$$

Remarquez que $G(x_1, x_2, x_3, x_4) = 1$ ssi exactement l'un des x_i vaut 1 1. La condition sur les $p_{ij\ell}$ s'écrit ainsi :

$$\forall 1 \leq i, j \leq 4: \qquad G(p_{ij1}, p_{ij2}, p_{ij3}, p_{ij4}) = 1. \tag{2.2}$$

$$\forall 1 \leq i, \ell \leq 4: \qquad G(p_{i1\ell}, p_{i2\ell}, p_{i3\ell}, p_{i4\ell}) = 1. \tag{2.3}$$

$$\forall 1 \leq j, \ell \leq 4: \qquad G(p_{1j\ell}, p_{2j\ell}, p_{3j\ell}, p_{4j\ell}) = 1. \tag{2.4}$$

$$\forall 1 \leq i, j \leq 2, 1 \leq \ell \leq 4: \qquad G(p_{2i-1,2j-1,\ell}, p_{2i,2j-1,\ell}, p_{2i-1,2j,\ell}, p_{2i,2j,\ell}) = 1. \tag{2.5}$$

La dernière condition correspond au fait que chaque chiffre entre 1 et 4 apparaît exactement une fois dans une sous-grille 2×2. On a le résultat suivant :

Théoréme 2.15. *L'ensemble des grilles* 4×4 *valides est en bijection avec les valeurs possible des variables* $p_{ij\ell}$ *qui satisfont les conditions* (2.2) - (2.5).

Démonstration. On montre d'abord que n'importe quelle grille 4 valide conduit à un jeu de variables qui satisfait toutes les équations. Supposons donc que la position (i, j) du Sudoku contient la valeur t_{ij}. On veut montrer que si l'on pose $p_{ijt_{ij}} = 1$ et $p_{ijs} = 0$ pour $s \neq t$, alors les équations sont vérifiés. Regardons chaque ensemble d'équation indépendamment.

(2.2) : D'après la façons dont nous avons posé les $p_{ij\ell}$, il y a exactement des $p_{ij1}, \ldots, p_{ij4}$ qui vaut 1, $p_{ijt_{ij}}$; cet ensemble d'équations est donc valide.

(2.3) : Cet ensemble d'équations correspond au fait que chaque ligne du Sudoku contient tous les chiffres. Il est donc valide.

(2.4) : Même chose que ci-dessus pour les colonnes.

(2.5) : Même chose pour les sous-grilles 2×2.

Maintenant, supposons qu'on à une assignation des variables $p_{ij\ell}$ qui satisfait toutes les équations. (2.2) implique que pour chaque (i, j) il y a exactement 1 seule valeur telle que $p_{ij\ell} = 1$. Appelons la t_{ij}. Alors (2.3) implique que chaque ligne contient tous les chiffres, (2.4) implique que chaque colonne contient tous les chiffres et (2.5) implique que chaque sous-grille contient tous les chiffres. On a donc un Sudoku valide. □

En comptant le nombre de variables et le nombre d'équations, on peut voir que l'ensemble des grilles valides est décrit par 64 variables et 64 équations.

2.7. Exercises