Éléments de Logique Formelle et du Raisonnement Mathématique

Transformation d'une formule logique

Stéphane Devismes

Université de Picardie Jules Verne

29 janvier 2025

Lors du dernier cours

- Logique propositionnelle
- Syntaxe
- Sens des formules

Notre exemple avec une table de vérité

Hypothèses :

- (H1) : Si Pierre est grand, alors Jean n'est pas le fils de Pierre
- (H2) : Si Pierre n'est pas grand, alors Jean est le fils de Pierre
- (H3) : Si Jean est le fils de Pierre alors Marie est la soeur de Jean

Conclusion (C) : Marie est la soeur de Jean ou Pierre est grand ou les deux à la fois.

$$(p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m) \Rightarrow m \vee p$$

p	j	m	$A = p \Rightarrow \neg j$	$B = \neg p \Rightarrow j$	$C = j \Rightarrow m$	$A \wedge B \wedge C$	$m \vee p$	$A \wedge B \wedge C \Rightarrow m \vee p$
0	0	0	1	0	1	0	0	**1**
0	0	1	1	0	1	0	1	**1**
0	1	0	1	1	0	0	0	**1**
0	1	1	1	1	1	1	1	**1**
1	0	0	1	1	1	1	1	**1**
1	0	1	1	1	1	1	1	**1**
1	1	0	0	1	0	0	1	**1**
1	1	1	0	1	1	0	1	**1**

Préambule

Comment prouver qu'une formule est valide ?

- Table de vérité
  - Problème : pour une formule à 100 variables, la table de vérité aura 2^{100} lignes (non calculable même par un ordinateur !).
- Idée :
  - Simplifier la formule en utilisant les **substitutions**, les **remplacements**, ou encore les **transformations en formes normales** (disjonctives ou conjonctives)
  - Puis, résoudre la formule simplifiée en utilisant les tables de vérités ou un raisonnement logique (par exemple : équivalences remarquables)

Plan

1. Substitution et remplacement
2. Formes normales
3. Algèbre de Boole
4. Fonctions booléennes
5. Conclusion

Substitution à support fini

Définition 2.2

- **Support** d'une substitution σ : l'ensemble des variables x telles que $x\sigma \neq x$.
- Une substitution σ à **support fini** est notée $< x_1 := A_1, \ldots, x_n := A_n >$, où $x_1, \ldots, x_n$ sont des variables **distinctes**, $A_1 \neq x_1, \ldots, A_n \neq x_n$ sont des formules et la substitution vérifie :
  - $\forall i, i \in 1, \ldots n : x_i\sigma = A_i$
  - $\forall y, y \notin \{x_1, \ldots, x_n\} : y\sigma = y$

Exemple 2.1

$A = x \vee x \wedge y \Rightarrow z \wedge y$ et $\sigma =< x := a \vee b, z := b \wedge c >$

$A\sigma = (a \vee b) \vee (a \vee b) \wedge y \Rightarrow (b \wedge c) \wedge y$

Substitution

Définition 2.1

Une **substitution** σ est une application de l'ensemble des variables dans l'ensemble des formules.

$A\sigma$ = remplacer dans la formule toute variable x par la formule $\sigma(x)$.

Exemple : $A = \neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$

- Soit σ la substitution suivante : $\sigma(p) = (a \vee b), \sigma(q) = (c \wedge d)$
- $A\sigma = \neg((a \vee b) \wedge (c \wedge d)) \Leftrightarrow (\neg(a \vee b) \vee \neg(c \wedge d))$

Propriétés des substitutions

Propriété 2.1

Soit A une formule, v une assignation et σ une substitution, nous avons $[A\sigma]_v = [A]_w$ où pour toute variable x, $w(x) = [\sigma(x)]_v$.

Exemple 2.2

Soit $A = x \vee y \vee d$
Soit $\sigma =< x := a \vee b, y := b \wedge c >$
Soit v telle que $v(a) = 1$, $v(b) = 0$, $v(c) = 0$, $v(d) = 0$
$A\sigma = (a \vee b) \vee (b \wedge c) \vee d$
$[A\sigma]_v = (1 \vee 0) \vee (0 \wedge 0) \vee 0 = 1$
$w(x) = [\sigma(x)]_v = [a \vee b]_v = 1 \vee 0 = 1$
$w(y) = [\sigma(y)]_v = [b \wedge c]_v = 0 \wedge 0 = 0$
$w(d) = [\sigma(d)]_v = [d]_v = 0$
$[A]_w = 1 \vee 0 \vee 0 = 1$

Démonstration.

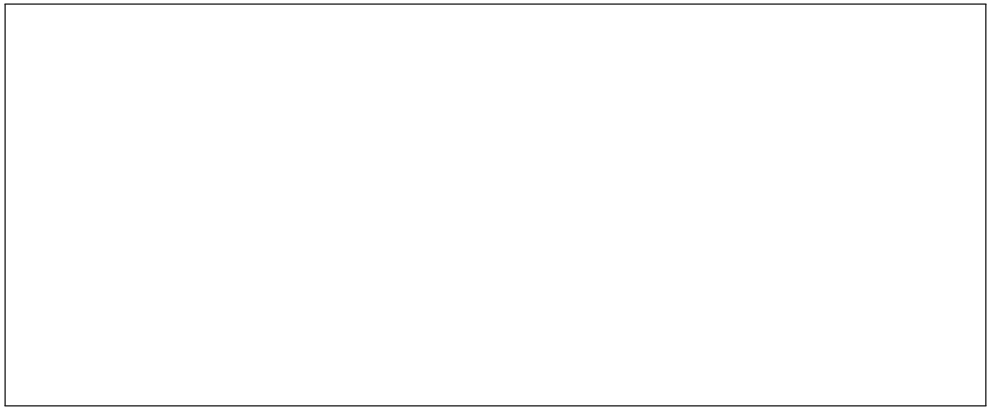
Soit A une formule, v une assignation et σ une substitution.
Preuve par récurrence sur la taille des formules. □

Cas de base : $|A| = 0$

Induction

Hypothèse : Supposons que la propriété soit vraie pour toute formule de taille inférieure ou égale à $n \geq 0$.

Soit A une formule de taille $n+1$, deux cas possibles :



Induction

Hypothèse : Supposons que la propriété soit vraie pour toute formule de taille inférieure ou égale à $n \geq 0$.

Soit A une formule de taille $n+1$, deux cas possibles :

Substitution d'une formule valide

Théorème 2.1

L'application d'une substitution à une formule valide donne une formule valide.

Démonstration.

Soit A une formule valide et σ une substitution.
Soit v une assignation quelconque.

Exemples

Exemple 2.3

Prouvons en utilisant les substitutions que $F = (a \wedge b) \vee \neg a \vee \neg b$ est valide.

Exemples

Exemple 2.4

Soit A la formule $\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$. Cette formule est valide, c'est une équivalence remarquable. Soit σ la substitution suivante :
$< p := (a \vee b), q := (c \wedge d) >$. La formule $A\sigma =$

Remplacement

Remplacer une formule par une formule.

Définition 2.3

Soient A, B, C, D des formules.
La formule D est obtenue en remplaçant dans C certaines occurrences de A par B
s'il existe une formule E et une variable x telles que, $C = E < x := A >$ et $D = E < x := B >$.

Exemples

Exemple 2.5

Considérons la formule $C = ((a \Rightarrow b) \vee \neg(a \Rightarrow b))$.

- La formule obtenue en remplaçant toutes les occurrences de $(a \Rightarrow b)$ par $(a \wedge b)$ dans C est

  C et D sont obtenues en considérant la formule $E = (x \vee \neg x)$ et les substitutions $< x := (a \Rightarrow b) >$ et $< x := (a \wedge b) >$.
- La formule obtenue en remplaçant la première occurrence de $(a \Rightarrow b)$ par $(a \wedge b)$ dans C est

  C et D sont obtenues en considérant la formule $E = (x \vee \neg(a \Rightarrow b))$ et les substitutions $< x := (a \Rightarrow b) >$ et $< x := (a \wedge b) >$.

Propriétés des remplacements (1/2)

Théorème 2.2

Soit C une formule et D la formule obtenue en remplaçant, dans C, des **occurrences** de la formule A par la formule B. Nous avons :
$(A \Leftrightarrow B) \models (C \Leftrightarrow D)$.

Démonstration.

Par définition du remplacement, il existe une formule E et une variable x telles que, $C = E < x := A >$ et $D = E < x := B >$. Supposons que v est une assignation modèle de $(A \Leftrightarrow B)$. Nous avons donc $[A]_v = [B]_v$. D'après la propriété 2.1 :

- $[C]_v = [E]_w$ où w est identique à v sauf que $w(x) = [A]_v$
- $[D]_v = [E]_{w'}$ où w' est identique à v sauf que $w'(x) = [B]_v$

Puisque $[A]_v = [B]_v$, les assignations w et w' sont identiques, donc $[C]_v = [D]_v$. Par suite v est modèle de $(C \Leftrightarrow D)$. □

Propriétés des remplacements (2/2)

Corollaire 2.1

Soit C une formule et D la formule obtenue en remplaçant, dans C, une **occurrence** de la formule A par la formule B. Nous avons : si $A \equiv B$ alors $C \equiv D$.

Démonstration.

Si $A \equiv B$, alors la formule $(A \Leftrightarrow B)$ est valide (propriété 1.1), donc la formule $(C \Leftrightarrow D)$ également puisqu'elle est, d'après le théorème 2.2, la conséquence de $(A \Leftrightarrow B)$. Par suite $C \equiv D$. □

Exemple 2.7

$(\neg(p \vee q) \Rightarrow (\boxed{\neg(p \vee q)} \vee r)) \equiv (\neg(p \vee q) \Rightarrow (\boxed{(\neg p \wedge \neg q)} \vee r))$, puisque $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$.

Application du théorème

Exemple 2.6

$p \Leftrightarrow q \models (p \vee (\boxed{p} \Rightarrow r)) \Leftrightarrow (p \vee (\boxed{q} \Rightarrow r))$.

Définitions

Définition 2.4

- Un **littéral** est une variable ou la négation d'une variable.
- Un **monôme** est une conjonction de littéraux.
- Une **clause** est une disjonction de littéraux.

Exemple

Exemple 2.8

Forme normale

Définition 2.5

Une formule est en **forme normale** si elle n'utilise que les opérateurs $\wedge, \vee, \neg$ et que les négations sont uniquement appliquées aux variables.

Exemple 2.9

La formule $\neg a \vee b$ est en forme normale, alors que la formule $a \Rightarrow b$ n'est pas en forme normale bien qu'elle soit équivalente à la première.

1. Élimination des équivalences
2. Élimination des implications
3. Déplacement des négations de sorte qu'elles ne portent que sur des variables

Éliminer une équivalence

Remplacer une occurrence de $A \Leftrightarrow B$ par l'une des sous-formules

(a) $(A \wedge B) \vee (\neg A \wedge \neg B)$

(b) $(\neg A \vee B) \wedge (\neg B \vee A)$

Éliminer une implication

Remplacer une occurrence de $A \Rightarrow B$ par $\neg A \vee B$

Déplacer les négations

Remplacer une occurrence de

(a) $\neg\neg A$ par A

(b) $\neg(A \vee B)$ par $\neg A \wedge \neg B$

(c) $\neg(A \wedge B)$ par $\neg A \vee \neg B$

Simplifications

Simplifier le plus tôt possible :

1. Remplacer une sous-formule de la forme $\neg(A \Rightarrow B)$ par $A \wedge \neg B$.
2. Remplacer une conjonction par 0 s'il comporte
   - soit une formule et sa négation,
   - soit un 0
3. Remplacer une disjonction par 1, si elle comporte
   - soit une formule et sa négation
   - soit un 1
4. Remplacer $\neg 1$ par 0 et $\neg 0$ par 1
5. Enlever les 0 des disjonctions et les 1 des conjonctions
6. Appliquer les simplifications :
   - $x \vee (x \wedge y) = x$,
   - $x \wedge (x \vee y) = x$,
   - $x \vee (\neg x \wedge y) = x \vee y$
7. Appliquer l'idempotence de la conjonction et de la disjonction.

Forme normale disjonctive

Définition 2.6

Une formule est une **forme normale disjonctive** (en bref **fnd**) si et seulement si elle est une disjonction (somme) de monômes.

Distribution des conjonctions sur les disjonctions
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
L'intérêt des fnd est de mettre en évidence ses modèles.

Exemple 2.10

$(x \wedge y) \vee (\neg x \wedge \neg y \wedge z)$ est une fnd, qui a deux modèles

Forme normale conjonctive

Définition 2.7

Une formule est une **forme normale conjonctive** (en bref **fnc**) si et seulement si elle est une conjonction (produit) de clauses.

Appliquer la distributivité (inhabituelle) de la disjonction sur la conjonction :

- $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$
- $(B \wedge C) \vee A = (B \vee A) \wedge (C \vee A)$.

L'intérêt des fnc est de mettre en évidence ses contre-modèles.

Exemple 2.11

$(x \vee y) \wedge (\neg x \vee \neg y \vee z)$ est une fnc, qui a deux contre-modèles

Remarque 2.1

Par convention, nous considérons que 0 et 1 sont des disjonctions de monômes et des conjonctions de clauses.

Exemple

Transformer $(a \Rightarrow b) \Leftrightarrow (\neg b \Rightarrow \neg a)$ en disjonctions de monôme (*fnd*) :

Autres exemples

Mise en **fnd** de :

$$(a \vee b) \wedge (c \vee d \vee e) \equiv$$

Mise en **fnc** de :

$$(a \wedge b) \vee (c \wedge d \wedge e) \equiv$$

Utilisation des disjonctions de monômes

BUT de transformer une formule en fnd

Déterminer si une formule est valide ou non.

Soit A une formule dont on souhaite déterminer la validité :

On transforme $\neg A$ en une disjonction de monômes **équivalente** B

- **Si** $B = 0$ alors $\neg A = 0$, donc $A = 1$, c'est-à-dire, A **est valide**
- **Sinon** B est égal à une disjonction de monômes non nuls équivalente à $\neg A$, qui nous donnent des modèles de $\neg A$, donc des contre-modèles de A.

Exemple

Soit $A = (p \Rightarrow (q \Rightarrow r)) \Rightarrow (p \wedge q \Rightarrow r)$

Déterminer si A est valide.

Autre exemple

Soit $A = (a \Rightarrow b) \wedge c \vee (a \wedge d)$.

Déterminer si A est valide.

La logique propositionnelle est une algèbre de Boole

Les axiomes se démontrent par tables de vérités.

notations logiques	notations booléennes
$\neg a$	$\overline{a}$
$a \wedge b$	$a.b$
$a \vee b$	$a+b$
$a \Rightarrow b$	$\overline{a}+b$
$a \Leftrightarrow b$	$a.b+(\overline{a}.\overline{b})$ ou $(a+\overline{b}).(\overline{a}+b)$

Figure 2.1 – Correspondances

Définition

Définition 2.8

Une **algèbre de Boole** est un ensemble d'au moins deux éléments, 0, 1, et trois opérations, complément ($\overline{x}$), somme (+) et produit (.), qui vérifient les axiomes suivants :

1. la somme est :
   - associative : $x+(y+z) = (x+y)+z$,
   - commutative : $x+y = y+x$,
   - 0 est élément neutre de la somme : $0+x = x$,
2. le produit est :
   - associatif : $x.(y.z) = (x.y).z$,
   - commutatif : $x.y = y.x$,
   - 1 est élément neutre du produit : $1.x = x$,
3. le produit est distributif sur la somme : $x.(y+z) = (x.y)+(x.z)$,
4. la somme est distributive sur le produit : $x+(y.z) = (x+y).(x+z)$,
5. les lois de la négation : $x+\overline{x} = 1$ et $x.\overline{x} = 0$.

Autre exemple d'algèbre de Boole

Algèbre de Boole	$\mathcal{P}(X)$
1	X
0	$\emptyset$
$\overline{p}$	$X-p$
$p+q$	$p \cup q$
$p.q$	$p \cap q$

Figure 2.2 – Ensemble des parties de l'ensemble X

Propriété d'une algèbre de Boole

Propriété 2.2

Pour tout x, il y a un et un seul y tel que $x + y = 1$ et $xy = 0$, autrement dit la négation est unique.
(preuve admise)

Propriété 2.3

1. $\overline{1} = 0$
2. $\overline{0} = 1$
3. $\bar{\bar{x}} = x$
4. Idempotence du produit : $x.x = x$
5. Idempotence de la somme : $x + x = x$
6. 1 est élément absorbant de la somme : $1 + x = 1$
7. 0 est élément absorbant du produit : $0.x = 0$
8. Lois de De Morgan : $\overline{xy} = \bar{x} + \bar{y}$ et $\overline{x + y} = \bar{x}.\bar{y}$

Preuve

1. $\overline{1} = 0$.
2. $\overline{0} = 1$.
3. $\bar{\bar{x}} = x$.

Preuve

- Idempotence du produit : $x.x = x$.

Preuve

- Idempotence de la somme : $x + x = x$.

Preuve

- 1 est élément absorbant de la somme : $1 + x = 1$.

- 0 est élément absorbant du produit : $0.x = 0$.

Preuve : Lois de De Morgan : $\overline{x+y} = \overline{x}.\overline{y}$

Preuve : Lois de De Morgan : $\overline{xy} = \overline{x} + \overline{y}$

Définition 2.9

Une **fonction booléenne** est une fonction dont les arguments et le résultat sont dans le domaine $\{0,1\}$.

Exemple 2.12

- La fonction $f : \mathbb{B} \to \mathbb{B} : f(x) = \overline{x}$
- La fonction $f : \mathbb{N} \to \mathbb{B} : f(x) = x \bmod 2$
- La fonction $f : \mathbb{B} \to \mathbb{N} : f(x) = x + 1$
- La fonction $f : \mathbb{B} \times \mathbb{B} \to \mathbb{B} : f(x,y) = \overline{x.y}$

Fonctions booléennes et somme de monômes

Théorème 2.3

Pour toute variable x, nous posons $x^0 = \overline{x}$ et $x^1 = x$.

Soit f une fonction booléenne à n arguments. Cette fonction est représentée à l'aide de n variables $x_1, \ldots, x_n$. Soit A la formule suivante :

$$A = \sum_{f(a_1,\ldots,a_n)=1} x_1^{a_1} \,.\, \cdots \,.\, x_n^{a_n}.$$

Les a_i sont des valeurs booléennes et A est la somme des monômes $x_1^{a_1} \,.\, \cdots \,.\, x_n^{a_n}$ tels que $f(a_1, \ldots, a_n) = 1$. Par convention, si la fonction f vaut toujours 0 alors $A = 0$.

Pour toute assignation v telle que $v(x_1) = a_1, \ldots, v(x_n) = a_n$, nous avons $f(a_1, \ldots, a_n) = [A]_v$.

Exemple

Exemple 2.13

La fonction *maj* à 3 arguments vaut 1 lorsqu'au moins 2 de ses arguments valent 1.

Définir la somme de monômes équivalente (théorème 2.3)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	**1**
1	0	0	0
1	0	1	**1**
1	1	0	**1**
1	1	1	**1**

$maj(x_1, x_2, x_3) = \overline{x_1} x_2 x_3 + x_1 \overline{x_2} x_3 + x_1 x_2 \overline{x_3} + x_1 x_2 x_3$

Vérifions le théorème 2.3 sur l'exemple 2.13

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$	$\overline{x_1} x_2 x_3$	$x_1 \overline{x_2} x_3$	$x_1 x_2 \overline{x_3}$	$x_1 x_2 x_3$	$\overline{x_1} x_2 x_3 + x_1 \overline{x_2} x_3 + x_1 x_2 \overline{x_3} + x_1 x_2 x_3$
0	0	0	**0**	0	0	0	0	**0**
0	0	1	**0**	0	0	0	0	**0**
0	1	0	**0**	0	0	0	0	**0**
0	1	1	**1**	1	0	0	0	**1**
1	0	0	**0**	0	0	0	0	**0**
1	0	1	**1**	0	1	0	0	**1**
1	1	0	**1**	0	0	1	0	**1**
1	1	1	**1**	0	0	0	1	**1**

Preuve du Théorème 2.3

Soit v une assignation quelconque. Notons que pour toute variable x, $[x^a]_v = 1$ si et seulement si $v(x) = a$. De cette remarque, nous déduisons la propriété suivante :

$$[x_1^{a_1} \,.\, \cdots \,.\, x_n^{a_n}]_v = 1 \text{ si et seulement si } v(x_1) = a_1, \ldots, v(x_n) = a_n. \qquad (1)$$

Soient $a_1, \ldots, a_n$ une liste de n valeurs booléennes et v une assignation telle que $v(x_1) = a_1, \ldots v(x_n) = a_n$. Considérons les deux cas suivants :

1. $f(a_1, \ldots, a_n) = 1$: Le monôme $x_1^{a_1} \,.\, \cdots \,.\, x_n^{a_n}$ est alors un des monômes de A.
   D'après (1), nous avons $[x_1^{a_1} \,.\, \cdots \,.\, x_n^{a_n}]_v = 1$.
   Puisque, par définition de A, ce monôme est élément de la somme A, nous avons $[A]_v = 1$.
2. $f(a_1, \ldots, a_n) = 0$: Supposons, par contradiction, que $[A]_v = 1$.
   Il existe alors un monôme de A, $x_1^{b_1} \,.\, \cdots \,.\, x_n^{b_n}$, tel que $[x_1^{b_1} \,.\, \cdots \,.\, x_n^{b_n}]_v = 1$.
   Par définition de A, nous avons $f(b_1, \ldots, b_n) = 1$.
   Or, d'après (1), nous avons $[x_1^{b_1} \,.\, \cdots \,.\, x_n^{b_n}]_v = 1$ si et seulement si $v(x_1) = b_1, \ldots, v(x_n) = b_n$, donc par définition de v, $a_1 = b_1, \ldots, a_n = b_n$.
   Nous obtenons donc une contradiction avec $f(a_1, \ldots, a_n) = 1$, par suite $[A]_v = 0$.

Fonctions booléennes et produit de clauses

Théorème 2.4

Pour toute variable x, nous posons $x^0 = \overline{x}$ et $x^1 = x$.

Soit f une fonction booléenne à n arguments. Cette fonction est représentée à l'aide de n variables $x_1, \ldots, x_n$. Soit A la formule suivante :

$$A = \prod_{f(a_1,\ldots,a_n)=0} x_1^{\overline{a_1}} + \ldots + x_n^{\overline{a_n}}.$$

Les a_i sont des valeurs booléennes et A est le produit des clauses $x_1^{\overline{a_1}} + \ldots + x_n^{\overline{a_n}}$ telles que $f(a_1, \ldots, a_n) = 0$. Par convention si la fonction f vaut toujours 1 alors $A = 1$.

Pour toute assignation v telle que $v(x_1) = a_1, \ldots, v(x_n) = a_n$, nous avons $f(a_1, \ldots, a_n) = [A]_v$.

Preuve du théorème 2.4

La preuve du théorème est à faire chez vous.

Soit v une assignation quelconque. Notons que pour toute variable x, $[x^a]_v = 0$ si et seulement si $v(x) \neq a$. De cette remarque, nous déduisons la propriété suivante :

$$[x_1^{\overline{a_1}} + \ldots + x_n^{\overline{a_n}}]_v = 0 \quad \Leftrightarrow \quad v(x_1) \neq \overline{a_1}, \ldots v(x_n) \neq \overline{a_n} \tag{1}$$
$$\Leftrightarrow \quad v(x_1) = a_1, \ldots v(x_n) = a_n. \tag{2}$$

Des propriétés ci-dessus, nous déduisons comme précédemment que $f(x_1, \ldots x_n) = A$.

Exemple

Exemple 2.14

La fonction *maj* à 3 arguments vaut 1 lorsqu'au moins 2 de ses arguments valent 1.

Définir le produit de clauses équivalent (théorème 2.4)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$
0	0	0	**0**
0	0	1	**0**
0	1	0	**0**
0	1	1	1
1	0	0	**0**
1	0	1	1
1	1	0	1
1	1	1	1

Vérifions le théorème 2.4 sur l'exemple 2.14

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$	$x_1+x_2+x_3$	$x_1+x_2+\overline{x_3}$	$x_1+\overline{x_2}+x_3$	$\overline{x_1}+x_2+x_3$	$(x_1+x_2+x_3)$ $(x_1+x_2+\overline{x_3})$ $(x_1+\overline{x_2}+x_3)$ $(\overline{x_1}+x_2+x_3)$
0	0	0	**0**	0	1	1	1	**0**
0	0	1	**0**	1	0	1	1	**0**
0	1	0	**0**	1	1	0	1	**0**
0	1	1	**1**	1	1	1	1	**1**
1	0	0	**0**	1	1	1	0	**0**
1	0	1	**1**	1	1	1	1	**1**
1	1	0	**1**	1	1	1	1	**1**
1	1	1	**1**	1	1	1	1	**1**

Aujourd'hui

- Substitutions et remplacements
- Formes normales
- Algèbre de Boole
- Fonctions booléennes

La prochaine fois

- Résolution

Merci de votre attention.