Les fondements du binaire : l'algèbre de Boole

M. Combacau
combacau@laas.fr

November 3, 2024

Objectif

Connaître l'outil mathématique de DDP

Algèbre de Boole : définitions (1)

Ensemble de définition, axiome 1, variable scalaire et vectorielle

- Ensemble de définition : $B_2 = \{0, 1\}$ $(\{\text{faux}, \text{vrai}\})$
- Variable booléenne scalaire : symbole (x) prenant valeur dans B_2
- **Axiome 1** : $(x = 0 \Leftrightarrow x \neq 1)$ et $(x = 1 \Leftrightarrow x \neq 0)$
- Variable booléenne vectorielle à n composantes :
  $X = (x_{n-1}, \ldots, x_1, x_0)$ prenant sa valeur dans B_2^n
- B_2^n comporte 2^n éléments appelés :
  - combinaison (de 1 et de 0)
  - point (ses coordonnées) dans un espace binaire à n dimensions
- $X = Y \Leftrightarrow \forall i \in [0, n-1], x_i = y_i$

Algèbre de Boole : définitions (2)

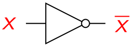
Opérateur unaire

- Complément (Non)
- Ensembles de définition : $B_2 \longrightarrow B_2$
- **Axiome 2** (définition des valeurs de la fonction)

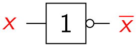
$$\begin{array}{ccc} 0 & \rightarrow & 1 \\ 1 & \rightarrow & 0 \end{array}$$

- Notations
  - Complement $(x) = \overline{x}$ ("x barre", utilisée dans ce cours)
  - Complement $(x) = \neg x$ ("Non x" utilisée en logique)
- Logigramme (représentation schématique)

MIL STD806



IEC 617



Algèbre de Boole : définitions (3)

Opérateur binaire (1)

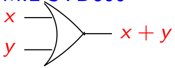
- OU (disjonction)
- Ensembles de définition : $B_2^2 \longrightarrow B_2$
- **Axiome 3** (définition des valeurs de la fonction)

0	0	$\rightarrow$	0
0	1	$\rightarrow$	1
1	0	$\rightarrow$	1
1	1	$\rightarrow$	1

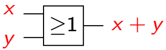
$$OU(x, y) = 0 \Leftrightarrow (x = 0) \text{ et } (y = 0)$$

- Notations
  - OU $(x, y) = x + y$ (“x ou y”, utilisée dans ce cours)
  - OU $(x, y) = x \vee y$ (“x ou y” utilisée en logique)
- Logigramme (représentation schématique)

MIL STD806



IEC 617



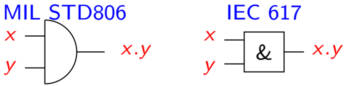
Algèbre de Boole : définitions (4)

Opérateur binaire (2)

- ET (conjonction)
- Ensemble de définition : $B_2^2 \longrightarrow B_2$
- **Axiome 4** (définition des valeurs de la fonction)

$$\begin{array}{cccc} 0 & 0 & \rightarrow & 0 \\ 0 & 1 & \rightarrow & 0 \\ 1 & 0 & \rightarrow & 0 \\ 1 & 1 & \rightarrow & 1 \end{array} \qquad ET(x,y) = 1 \Leftrightarrow (x = 1) \text{ et } (y = 1)$$

- Notations
  - ET $(x, y) = x.y$ (“x et y”, utilisée dans ce cours)
  - ET $(x, y) = x \wedge y$ (“x et y” utilisée en logique)
- Logigramme (représentation schématique)



Algèbre de Boole : propriétés des opérateurs (1)

Propriétés démontrées par induction

- involution : $\bar{\bar{x}} = x$ $\quad \begin{cases} 0 \longrightarrow & \bar{0} = 1 \longrightarrow \bar{1} = 0 \\ 1 \longrightarrow & \bar{1} = 0 \longrightarrow \bar{0} = 1 \end{cases}$
- idempotence :
  - $x + x = x$ $\quad \begin{cases} 0 + 0 = 0 \\ 1 + 1 = 1 \end{cases}$
  - $x.x = x$ $\quad \begin{cases} 0.0 = 0 \\ 1.1 = 1 \end{cases}$
- Eléments neutres et absorbants : (démo au tableau)
  - $x + 0 = x$ et $x.1 = x$
  - $x + 1 = 1$ et $x.0 = 0$

Algèbre de Boole : propriétés des opérateurs (2)

Propriétés démontrées par induction

- Complémentarité :
  - $x + \overline{x} = 1$ $\quad \begin{cases} 0 + 1 = 1 \\ 1 + 0 = 1 \end{cases}$
  - $x.\overline{x} = 0$ $\quad \begin{cases} 0.1 = 0 \\ 1.0 = 0 \end{cases}$
- Commutativité
  - $x + y = y + x$
  - $x.y = y.x$
- associativité (démo au tableau)
  - $(x + y) + z = x + (y + z)$
  - $(x.y).z = x.(y.z)$

Algèbre de Boole : propriétés des opérateurs (3)

Propriétés démontrées par induction

- Inclusion :
  - Absorption
    - # $x + x.y = x$ $\begin{cases} \dots \\ \dots \end{cases}$
    - # $x.(x + y) = x$ $\begin{cases} \dots \\ \dots \end{cases}$
  - Simplification
    - # $x + \overline{x}.y = x + y$ $\begin{cases} \dots \\ \dots \end{cases}$
    - # $x.(\overline{x} + y) = x.y$ $\begin{cases} \dots \\ \dots \end{cases}$
- Distributivité
  - $x.(y + z) = x.y + x.z$
  - $x + y.z = (x + y).(x + z)$

Algèbre de Boole : propriétés des opérateurs (4)

Propriétés démontrées par induction

- Théorème de DE MORGAN
  - $\overline{x+y} = \overline{x}.\overline{y}$ $\left\{ \begin{array}{l} \dots \\ \dots \end{array} \right.$
  - $\overline{x.y} = \overline{x} + \overline{y}$ $\left\{ \begin{array}{l} \dots \\ \dots \end{array} \right.$
- Règle du consensus
  - $x.y + \overline{x}.z + y.z = x.y + \overline{x}.z$ $\left\{ \begin{array}{l} \dots \\ \dots \end{array} \right.$
  - $(x+y).(\overline{x}+z).(y+z) = (x+y).(\overline{x}+z)$ $\left\{ \begin{array}{l} \dots \\ \dots \end{array} \right.$

Algèbre de Boole : particularités

Distributivité OU sur ET, pas d'inverse pour les opérateurs binaires

- $x + y.z = (x + y).(x + z)$ (lié à l'élément absorbant 1 pour $+$)
- Pas de soustraction : $x + y = x + z \nRightarrow y = z$
  contre-exemple: $x = 1$ et $y = 0$ et $z = 1$
- Pas de division : $x.y = x.z \nRightarrow y = z$
  contre-exemple: $x = 0$ et $y = 1$ et $z = 0$
- existence d'opérateurs dérivés (cas spéciaux)
  - XOR (OU exclusif) : $(XOR(x, y) = 1) \Leftrightarrow (x \neq y)$
  - NAND (ET NON) : $(NAND(x, y) = 0) \Leftrightarrow (x = y = 1)$
  - NOR (OU NON) : $(NOR(x, y) = 1) \Leftrightarrow (x = y = 0)$

Nous verrons l'intérêt de ces opérateurs au long de ce cours

Expressions algébriques (Ea): définition

Définition récurrente pour le formalisme

Une expression algébrique prend une valeur dans B_2

- Soit $x_1 \ldots x_n$ des variables booléennes scalaires
  alors 0,1,x $\overline{x} \ldots$ $x_n, \overline{x_n}$ sont des Ea (atomiques)
- Si Ea1 et Ea2 sont des Ea alors
  - (Ea1) et (Ea2) sont des Ea
  - $\overline{\text{Ea1}}$ et $\overline{\text{Ea2}}$ et sont des Ea
  - Ea1+Ea2 est une Ea
  - Ea1.Ea2 est une Ea

Les opérateurs NON, ET et OU s'expriment simplement par une Ea
$x + (\overline{y}.z).(y + z)$ est aussi une Ea
$x. + (y + z)$ n'est pas une Ea

Expressions algébriques remarquables

Très utiles au niveau de la terminologie en particulier

- Littéral : Ea composée d'une seule variable x ou $\overline{x}$
- monôme : ET (on dit "produit") de littéraux - Exemple : $x_2.x_1.\bar{x_0}$
- monal : OU (on dit "somme") de littéraux - Exemple : $x_2 + \overline{x_1} + x_0$
- Somme de Produits (forme $\sum\prod$) est une somme de monômes - Exemple : $x_1.x_0 + x_3.\overline{x_2}$
- Produit de Sommes (forme $\prod\sum$) est un produit de monals - Exemple : $(x_3 + x_2 + \overline{x_0}).(x_2 + x_0)$
- Diviseur : Un diviseur d'un monôme m est obtenu en supprimant un nombre quelconque de littéraux à ce monôme.
  Exemple : $m_1 = x_2.x_1.x_0$ admet l'ensemble de diviseurs $\{x_2.x_1,\ x_2.x_0,\ x_1.x_0,\ x_2,\ x_1,\ x_0\}$

Valeur d'une expression algébrique

EA comme une fonction d'une variable vectorielle booléenne

- Lorsqu'une expression algébrique Ea contient les littéraux $x_{n-1} \ldots x_1, x_0$ pouvant être considérés comme les composantes d'une variable vectorielle X, alors elle peut être vue comme l'expression d'une relation entre $B_2^n \longrightarrow B_2$.

  On dit alors que Ea est "formée" sur X.
- La valeur (l'image) par cette Ea d'une combinaison X_0 de la variable vectorielle $X = (x_{n-1} \ldots x_1, x_0)$ est calculée en remplaçant chaque littéral de Ea par la valeur qu'elle a dans la combinaison X_0
- Exemple : soit $X = (x_2, x_1, x_0)$ et $Ea = \overline{x_0} + x_1.x_2$

  Pour la combinaison $X_0 = (0, 0, 1)$ on a $Ea(X_0) = \overline{0} + 0.1 = 1$
- On dit que $(Ea1 = Ea2)$ si et seulement si $Ea1(X) = Ea2(X)$ ont des valeurs identiques quelle que soit la combinaison (valeur) de X

Expression algébriques : définitions complémentaires

Autres Expressions algébriques remarquables

Considérons une Ea formée sur le vecteur X

- un minterme est un monôme dans lequel toutes les composantes de X apparaissent exactement une fois dans Ea
- un maxterme est un monal dans lequel toutes les composantes de X apparaissent exactement une fois dans Ea
- Exemple :

  Soit $X = (x_2, x_1, x_0)$ et $Ea = \overline{x_0} + x_1.x_2$

  - $Ea1 = x_2.\overline{x_1}.x_0$ est un minterme
  - $Ea2 = x_2 + x_1 + \overline{x_0}$ est un maxterme
  - $Ea2 = \overline{x_2}.x_1 + \overline{x_0}$ n'est ni un maxterme, ni un minterme

Fonctions logiques simples

Définition et terminologie

- f fonction logique a pour ensemble de départ B_2^p
- f fonction logique a pour ensemble d'arrivée B_2
- f fonction logique partitionne l'ensemble de départ en
  - un ensemble de points vrais : ceux ayant 1 pour image
  - un ensemble de points faux : ceux ayant 0 pour image
- Le nombre de points de B_2^n est 2^n, à chacune de ces combinaisons une fonction donne pour image 0 ou 1:

  $\Rightarrow$ le nombre de fonctions simples de n variables est 2^{2^n}.

Fonctions logiques simples

Fonctions logiques simples d'une variable $(n = 1)$

$2^{2^1} = 2^2 = 4$ fonctions

x	U_0	U_1	U_2	U_3
0	0	0	1	1
1	0	1	0	1

- U_0 : la fonction constante 0
- U_1 : fonction identité
- U_2 : fonction complément (l'opérateur complément donc)
- U_3 : la fonction constante 1

Fonctions logiques simples

Fonctions logiques simples de deux variables ($n = 2$)

$2^{2^2} = 2^4 = 16$ fonctions

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

- f_0 : la fonction constante 0
- f_1 : l'opérateur ET
- f_6 : l'opérateur XOR
- f_7 : l'opérateur OU
- f_8 : l'opérateur NOR
- f_{13} : représente l'implication logique ($x \Rightarrow y$)
- f_{14} : l'opérateur NAND
- f_{15} : la fonction constante 1

Fonctions logiques simples

Fonction incomplètement spécifiée (notée f^*)

- Soit $B_2^* = \{0, *, 1\}$
- f^* est une fonction de B_2^n vers B_2^*
- f^* partitionne l'ensemble de départ B_2^n en
  - un ensemble de points vrais : ceux ayant 1 pour image
  - un ensemble de points faux : ceux ayant 0 pour image
  - un ensemble de point non spécifiés : ceux ayant $*$ pour image
- Un point non spécifié correspond en général
  - une combinaison ne pouvant se produire dans la réalité (ex ascenseur)
  - une combinaison pour laquelle la valeur de la fonction ne compte pas (ex monte-charge)
- Très utilisé en modélisation (cahier des charges $\rightarrow$ modèle binaire)

Fonctions logiques multiples

Juxtaposition de plusieurs fonctions logiques simples

- p fonctions logiques simples ayant même ensemble de départ B_2^n
- Ensemble d'arrivée B_2^p
- Simplement une simplification d'écriture, pas de spécificité
- Très courant en automatique, un système de contrôle-commande avec plusieurs sorties dépendant toutes de l'ensemble des entrées (penser à l'exemple de l'allumage des feux d'un véhicule)
- Concept utilisé dans la deuxième partie du cours (arithmétique et codes correcteurs d'erreurs)