Informatique Générale

Guillaume Hutzler
Laboratoire IBISC
(Informatique Biologie Intégrative et Systèmes Complexes)
guillaume.hutzler@ibisc.univ-evry.fr
Cours Dokeos 625
http://www.ens.univ-evry.fr/modx/dokeos.html

Plan et objectifs du cours

- Objectifs du cours
  - Donner une vue d'ensemble de l'informatique
    - du point de vue **historique**
    - du point de vue des **concepts**
    - du point de vue des **techniques**
  - Donner un aperçu des métiers de l'informatique
- Séances
  - 1-2 : Histoire de l'informatique
  - 3-4 : Fondements mathématiques de l'informatique
  - 5-6 : Architecture des ordinateurs et des micro-processeurs
  - 7-8 : Systèmes d'exploitation
  - 9-10 : Langages de programmation
  - 11-12 : Réseaux

Informatique Générale
Logique des propositions
Algèbre de Boole

Guillaume Hutzler
Laboratoire IBISC
(Informatique Biologie Intégrative et Systèmes Complexes)
guillaume.hutzler@ibisc.univ-evry.fr

F. Bacon – le codage binaire (1623)

- But = crypter un texte pour qu'il ne puisse pas être déchiffré
  - lettres de l'alphabet remplacées par des séquences de 5 caractères `a` ou `b` (alphabet bilitère)

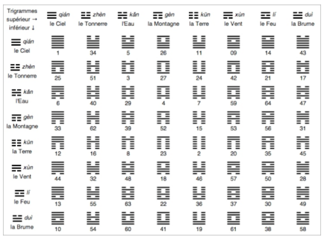
A	B	C	D	E	F
aaaaa	aaaab	aaaba	aaabb	aabaa	aabab
G	H	I	K	L	M
aabba	aabbb	abaaa	abaab	ababa	ababb
N	O	P	Q	R	S
abbaa	abbab	abbba	abbbb	baaaa	baaab
T	U	W	X	Y	Z
baaba	baabb	babaa	babab	babba	babbb

  - un texte de couverture quelconque est imprimé en utilisant deux styles typographiques distincts, l'un associé au `a`, l'autre associé au `b`
  - ex:

```
Nepar|tezsu|rtout|passa|nsmoi
aabab|baabb|babba|aabaa|babbb
  f  |  u  |  y  |  e  |  z
```


G. v. Leibniz – Numérotation binaire (1666)

- But = langage universel permettant une représentation exacte de toutes réalités ; réduire toutes les opérations logiques à un calcul
  - inspiré par le codage binaire de Bacon
  - inspiré par le Yi Jing (système de divination chinois – 3000 av. J. C.)



L'algèbre de Boole

- G. Boole
  - 1854 : restructure la logique en un système formel -> la logique devient une branche des mathématiques
- Algèbre de Boole
  - partie des mathématiques, de la logique et de l'électronique qui s'intéresse aux opérations et aux fonctions sur les variables logiques
  - permet d'utiliser des techniques algébriques pour traiter les expressions à deux valeurs de la logique des propositions
  - permet de modéliser des raisonnements logiques, en exprimant un "état" en fonction de conditions

L'expérience de Wason

- *Quatre cartes comportant un chiffre sur une face et une lettre sur l'autre, sont disposées à plat sur une table. Une seule face de chaque carte est visible. Les faces visibles sont les suivantes : D, 7, 5, K.*

D 7 5 K

  - *Quelle(s) carte(s) devez-vous retourner pour déterminer la ou les carte(s) qui ne respecte(nt) pas la règle suivante :* Si une carte a un D sur une face, alors elle porte un 5 sur l'autre face. *Il ne faut pas retourner de carte inutilement, ni oublier d'en retourner une.*

Réponse : D et 7

Vérification

- Si (valeur recto = D) alors (valeur verso = 5)
- Table de vérité

valeur recto = D	valeur verso = 5	Si (valeur recto = D) alors (valeur verso = 5)
V	V	V
V	F	F
F	V	V
F	F	V

K

La logique des propositions

- De manière informelle
  - les propositions sont des énoncés, phrases décrivant une situation, une propriété, une relation, un jugement, auxquels on serait susceptible d'associer dans des circonstances précises une valeur de vérité : elle est vrai (valeur V) ou fausse (valeur F)
  - la logique s'interdit la contradiction ⇒ pas de phrases autoréférentielles
    - « cette phrase est fausse »
      - cette proposition est-elle vraie ou fausse ?
    - le barbier annonce à l'entrée de sa boutique : « je rase tous ceux qui ne se rasent pas eux-mêmes »
      - le barbier se rase-t-il ?

La logique des propositions

- De manière formelle
  - Les énoncés élémentaires sont représentés par des variables dites variables propositionnelles
  - Les énoncés composés sont formés d'un ou de plusieurs énoncés (élémentaires ou composés) combinés par des connecteurs (∧, ∨, ¬, ⇒, ⇔)
  - Des combinaisons plus complexes peuvent être formées par parenthésage
    ((A ⇒ D) ⇒ (D ⇒ B)) ⇒ (A ⇒ B)

Exemples
- énoncés élémentaires
  - soit P la proposition « la terre est plate »
  - soit Q la proposition « 29 est un nombre premier »
- énoncés composés
  - (non P) et Q : « la terre n'est pas plate et 29 est un nombre premier »
  - (non P) et (non Q) : « la terre n'est pas plate et 29 n'est pas premier »
  - P ou Q : « la terre est plate ou 29 est un nombre premier »

Négation : ¬P

- si P est une proposition arbitraire, sa négation est la proposition (non P), également notée ¬P, dont la véracité est l'opposée de celle de P
- Table de vérité

P	¬P
V	F
F	V

Conjonction : P ∧ Q

- si P et Q sont deux propositions, leur conjonction est la proposition (P et Q), également notée (P ∧ Q)
  - elle n'est vraie que si P et Q sont toutes les deux vraies
  - « et » dans le sens ordinaire
  - la conjonction est réflexive et commutative
- Table de vérité

P	Q	P ∧ Q
V	V	V
V	F	F
F	V	F
F	F	F

Disjonction (ou adjonction) : P ∨ Q

- si P et Q sont deux propositions, leur disjonction est la proposition (P ou Q), également notée (P ∨ Q)
  - elle est vraie lorsque au moins l'une des deux propositions est vraie
  - « ou » dans un sens inclusif
  - « soit P, soit Q, soit les deux »
  - la disjonction est réflexive et commutative
- Table de vérité

P	Q	P ∨ Q
V	V	V
V	F	V
F	V	V
F	F	F

Equivalence : P ⇔ Q

- si P et Q sont deux propositions, leur équivalence se note (P ⇔ Q)
  - elle est vraie si P et Q ont la même valeur de vérité
  - l'équivalence est réflexive et commutative
- Table de vérité

P	Q	P ⇔ Q
V	V	V
V	F	F
F	V	F
F	F	V

Implication : P ⇒ Q

- si P et Q sont deux propositions, l'implication (P implique Q), notée également (P ⇒ Q) traduit la proposition conditionnelle « si P alors Q »
  - elle est définie comme fausse si l'hypothèse P est vraie et que la conclusion Q est fausse
  - elle est définie comme vraie dans tous les autres cas
- Table de vérité

P	Q	P ⇒ Q
V	V	V
V	F	F
F	V	V
F	F	V

Remarques sur l'implication

- si l'implication P ⇒ Q est vraie
  - P est une **condition suffisante** pour Q
  - Q est une **condition nécessaire** pour P
- une équivalence est une implication dans les deux sens
  - **condition nécessaire et suffisante**
- le faux implique n'importe quoi, y compris le vrai
  - A partir d'hypothèses fausses, on peut démontrer n'importe quoi
  - un journaliste a demandé à Hilbert de démontrer :
    - « si 1 + 1 = 3, alors Hilbert est le Pape »
  - démonstration
    - si 1 + 1 = 3 alors 1 = 2
    - soit l'ensemble {le Pape; David Hilbert}
    - il est de cardinal 2 donc de cardinal 1 puisque 1 = 2
    - c'est un singleton donc David Hilbert est le Pape

Tautologies (1)

- Une tautologie est une assertion qui dépend d'autres assertions mais qui est toujours vraie, quelles que soient les valeurs de vérité de ces dernières
- Exemple
  « A ∨ ¬A » est une tautologie
  « A ⇔ ¬¬A » est une tautologie

A	¬A	A ∨ ¬A	¬¬A	A ⇔ ¬¬A
V	F	V	V	V
F	V	V	F	V

Tautologies (2)

- Une tautologie de type A ⇔ B permet de dire qu'il est logiquement équivalent de démontrer A ou de démontrer B, quel que soit le contexte
  - on dit des propositions A et B qu'elles sont **logiquement équivalentes**
  - pour démontrer que deux propositions sont logiquement équivalentes, il suffit de montrer qu'elles ont la même table de vérité

Tautologies à connaître

1	A ⇔ ¬¬A	double négation
2	¬(A ∨ B) ⇔ ¬A ∧ ¬B	1ère loi de Morgan
3	¬(A ∧ B) ⇔ ¬A ∨ ¬B	2ème loi de Morgan
4	A ∨ ¬A	tiers exclus
5	(A ⇒ B) ⇔ ¬A ∨ B	
6	(A ⇒ B) ⇔ (¬B ⇒ ¬A)	contraposition
7	(A ⇔ B) ⇔ (A ⇒ B) ∧ (B ⇒ A)	
8	((A ⇒ B) ∧ (B ⇒ C)) ⇒ (A ⇒ C)	transitivité de l'implication
9	(A ∨ (B ∧ C)) ⇔ (A ∨ B) ∧ (A ∨ C)	distributivité
10	(A ∧ (B ∨ C)) ⇔ (A ∧ B) ∨ (A ∧ C)	distributivité

Démonstrations (1)

(2) ¬(A ∨ B) ⇔ ¬A ∧ ¬B

A	B	¬A	¬B	A ∨ B	¬(A ∨ B)	¬A ∧ ¬B
V	V	F	F	V	F	F
V	F	F	V	V	F	F
F	V	V	F	V	F	F
F	F	V	V	F	V	V

- Quel est le contraire de la phrase
  « cette voiture est verte ou blanche »

Démonstrations (2)

(3) ¬(A ∧ B) ⇔ ¬A ∨ ¬B

$\neg A \vee \neg B \overset{(1)}{\Leftrightarrow} \neg\neg(\neg A \vee \neg B)$

$\overset{(2)}{\Leftrightarrow} \neg(\neg\neg A \wedge \neg\neg B)$

$\overset{(1)}{\Leftrightarrow} \neg(A \wedge B)$

- Quel est le contraire de la phrase
  « j'aime le chocolat et la vanille »

Démonstrations (3)

(6) $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$

$(A \Rightarrow B) \overset{(5)}{\Leftrightarrow} (\neg A \vee B)$

$\overset{(1)}{\Leftrightarrow} (\neg A \vee \neg\neg B)$

(commutativité de $\vee$)
$\Leftrightarrow (\neg\neg B \vee \neg A)$

$\overset{(5)}{\Leftrightarrow} (\neg B \Rightarrow \neg A)$

Interprétation ensembliste

- soit
  - ε un ensemble qu'on appelle le contexte
  - $\alpha \subset \varepsilon$, $\beta \subset \varepsilon$
  - soit A l'assertion « $x \in \alpha$ »
  - soit B l'assertion « $x \in \beta$ »
- alors
  - $A \vee B \Leftrightarrow x \in \alpha \cup \beta$
  - $A \wedge B \Leftrightarrow x \in \alpha \cap \beta$
  - $(A \Rightarrow B) \Leftrightarrow \alpha \subset \beta$
  - $(A \Leftrightarrow B) \Leftrightarrow \alpha = \beta$
  - $\neg A \Leftrightarrow x \in \varepsilon \setminus \alpha$

Logique et raisonnement

- La logique est utilisée pour raisonner ou produire des démonstrations, c'est-à-dire, à partir d'énoncés de départ (les **germes**), aboutir à un ensemble de conclusions par l'application successives de **règles d'inférence**
- Différentes formes de raisonnement
  - le syllogisme
  - la contraposition
  - le raisonnement par l'absurde

Le syllogisme

- Forme la plus courante de raisonnement, identifiée par Aristote
  - « Socrate est un homme »
  - « Les hommes sont mortels »
  - « Donc Socrate est mortel »
- Raisonnement qui peut se ramener sous la forme

  Si A est vraie
  Et $A \Rightarrow B$ est vraie
  Alors B est vraie

La contraposition

Si $\neg B \Rightarrow \neg A$
Alors $A \Rightarrow B$
(en réalité, c'est une équivalence mais on l'utilise dans ce sens)

Quelle est la forme exacte du raisonnement suivant :
« $7^2 \neq 3^2 + 6^2$, donc le triangle de côtés 3, 6, 7 n'est pas rectangle »

- contraposée du sens direct du théorème de Pythagore

Le raisonnement par l'absurde

- Principe du tiers exclus
  - soit A vraie, soit $\neg$A vraie
  - il suffit de montrer que $\neg$A est fausse
  - on part de $\neg$A pour arriver à une assertion dont on sait qu'elle est fausse

  $\neg A \Rightarrow F$
  donc A vraie

Algèbre de Boole

- Constat
  - De nombreux dispositifs électronique, électromécanique, (mécanique, électrique, pneumatique, etc.) fonctionnement en TOUT ou RIEN
  - ils peuvent prendre 2 états
    - arrêt/marche
    - ouvert/fermé
    - enclenché/déclenché
    - avant/arrière
    - vrai/faux
    - conduction/blocage
  - avantageux d'employer un système mathématique n'utilisant que 2 valeurs numériques (exemple O ou 1) pour étudier les conditions de fonctionnement de ces dispositifs

Algèbre de Boole

- composée de
  - l'ensemble *B*={0,1}
  - les opérations
    - de **disjonction (+)** (équivalent du « ou » logique)
    - de **conjonction (.)** (équivalent du « et » logique)
    - de **négation (')** (équivalent du « non » logique)

+	0	1
0	0	1
1	1	1

.	0	1
0	0	0
1	0	1

'	0	1
	1	0

Propriétés de l'opérateur +

Propriétés	
associativité	(a + b) + c = a + (b + c)
élément neutre	a + 0 = a = 0 + a
élément absorbant	a + 1 = 1 = 1 + a
idempotence	a + a = a
commutativité	a + b = b + a
ordre préfixe	a ≤ a + b
réflexif	a ≤ a
transitif	a ≤ b, b ≤ c ⇒ a ≤ c
antisymétrique	a ≤ b, b ≤ a ⇒ a = b
treillis	sup(a, b) = a + b

Propriétés de l'opérateur .

Propriétés	
associativité	(a.b).c = a.(b.c)
élément neutre	a.1 = a = 1.a
élément absorbant	a.0 = 0 = 0.a
idempotence	a.a = a
commutativité	a.b = b.a
ordre préfixe	a ≥ a.b
réflexif	a ≥ a
transitif	a ≥ b, b ≥ c ⇒ a ≥ c
antisymétrique	a ≥ b, b ≥ a ⇒ a = b
treillis	inf(a, b) = a.b

Propriétés mutuelles des opérateurs + et .

Propriétés		
distributivité	a.(b + c) = a.b + a.c = b.a + c.a = (b + c).a	a + (b.c) = (a + b).(a + c) = (b + a).(c + a) = (b.c) + a
absorption	a + (a.b) = a	a.(a + b)=a

Propriétés du « non » dans *B*

Propriétés		
involution	a'' = a	
complémentarité	a + a' = 1	a.a' = 0
dualité	(a + b)' = a'.b'	(a.b)' = a' + b'
antitonie	a ≤ b ↔ a' ≥ b'	a ≥ b ↔ a' ≤ b'

Variable logique (ou variable binaire)

- Formellement
  - la variable logique est une grandeur qui peut prendre 2 valeurs qui sont représentées habituellement **0** ou **1**.Cette variable binaire se note par une lettre comme en algèbre (ex. a b x)
- Physiquement
  - cette variable peut correspondre à l'un des dispositifs cités dont les 2 états représentent les 2 valeurs possibles que peut prendre cette variable
  - ces 2 états sont repérés H et L et on attribue
    - à l'état **H** (high) la valeur **1**
    - à l'état **L** (low) la valeur **0**

On parle aussi de **variable booléenne**

Fonction logique

- Une fonction logique est le résultat de la combinaison (logique combinatoire) d'une ou plusieurs variables logiques reliées entre elles par des opérations mathématiques booléennes bien définies
  - la valeur résultante de cette fonction dépend de la valeur des variables logiques
  - de toute façon cette résultante ne peut être que **0** ou **1**
- Une fonction logique possède donc
  - une ou des **variables logiques d'entrée**
  - une **variable logique de sortie**
- Cette fonction logique se note par une lettre comme en algèbre (ex. A G Y B F X)

On parle aussi de **fonction booléenne**

Les fonctions booléennes de 2 variables

x	0011	
y	0101	
fonction	**vecteur**	**expression**
0	0000	0
1	0001	x.y (et)
2	0010	x.y'
3	0011	x
4	0100	x'.y
5	0101	y
6	0110	x ⊕ y (ou exclusif)
7	0111	x + y (ou)

x	0011	
y	0101	
fonction	**vecteur**	**expression**
8	1000	x ↑ y (nor = (x+y)')
9	1001	x ⊙ y = (x ⊕ y)'
10	1010	y'
11	1011	x' ↓ y
12	1100	x'
13	1101	x ↓ y'
14	1110	x ↓ y (nand = (x.y)')
15	1111	1

Représentation par table de vérité

- Soit la fonction booléenne F = (p.q) + (q'.r)
- Sa table de vérité est la suivante :

p	*q*	*r*	*F*
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Représentation canonique (forme normale disjonctive)

- Soit la fonction booléenne F = (p.q) + (q'.r)
- Sa forme canonique est la suivante :

p	*q*	*r*	*F*
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

F = (p'.q'.r) + (p.q'.r) + (p.q.r') + (p.q.r)

minterms

Simplification des expressions

- Exemple :

p'q'r + p'qr + pq'r'	= p'rq' + p'rq + pq'r'	(commutativité)
	= (p'rq' + p'rq) + pq'r'	(associativité)
	= p'r (q' + q) + pq'r'	(distributivité)
	= p'r + pq'r'	(q' + q) = 1

Diagramme de Karnaugh

p’q’r + p’qr + pq’r’

	pq	p’q	p’q’	pq’
r		1	1	
r’				1

Diagramme de Karnaugh

- inventé dans les années 50 pour simplifier la conception de circuits logiques
- représentation visuelle mettant en évidence les paires de minterms que l’on peut réunir et fusionner en une seule expression plus simple
- les lignes et les colonnes sont étiquetées de manière à ce qu’en se déplaçant de ligne en ligne ou de colonne en colonne, on observe exactement *un* changement dans l’étiquette
- pour une expression booléenne donnée sous forme normale disjonctive, on écrit un 1 dans chaque case représentant les minterms présents
- la simplification correspond aux groupes de 2^n cellules contiguës

Exemple de diagramme de Karnaugh (1)

- pqr + p’qr’ + pq’r

	pq	p’q	p’q’	pq’
r	1			1
r’		1		

- se simplifie en
  pr + p’qr’

Exemple de diagramme de Karnaugh (2)

- pqr + p'q'r' + p'qr + pqr' + p'qr'

	pq	p'q	p'q'	pq'
r	1	1		
r'	1	1	1	

- se simplifie en
  q + p'r'

Sources

- L. Frécon, *Eléments de mathématiques discrètes*, Presses polytechniques et universitaires romandes, Lausanne, 2002
- Rod Haggarty, *Mathématiques discrètes appliquées à l'informatique*, Pearson Education, collection Synthex, 2005
- http://fr.wikipedia.org