Mathématiques Pour l'Informatique I : Théorie des Ensembles et Relations

Serge Iovleff

13 septembre 2004

Quelques références

- Ma Page http ://www.iut-info.univ-lille1.fr/˜iovleff
- Un Cours réalisé par des étudiants de deuxième année dans le cadre d'un projet
  http ://www.iut-info.univ-lille1.fr/projet2002/mathinfo/projet
- N. Permingeat et D. Glaudei, *« Algèbre de Boole : Théorie, Méthodes de Calcul, Applications »*, Masson, 1991.

Plan du Cours

1. Théorie des Ensembles
2. Relations Binaires
3. Arithmétique
   (a) Arithmétique Modulaire
   (b) Cryptographie
4. Algèbre De Boole
   (a) Algèbre de Boole et Fonctions Booléennes
   (b) Diagrammes de Karnaugh et Circuits
   (c) Fonctions Booléennes sur Variables Binaires
5. Logique
   (a) Techniques de Démonstration
   (b) Logique Propositionnelle
   (c) Logique des prédicats

Table des matières

Chapitre 1

Théorie des ensembles

Plan

1. Définition
2. Cardinal d'un ensemble
3. Représentation d'un ensemble
4. Relations entre ensemble
5. Ensemble des parties d'un ensemble
6. Opérations sur les ensembles
7. Propriétés des opérations sur les ensembles
8. Fonction caractéristique d'un ensemble

1.1 Définition

Définition 1.1.1 *Un ensemble est une collection non ambigu d'objets tous distincts, appelés éléments de l'ensemble.*

- Pour dire que a est élément d'un ensemble A, on écrit $a \in A$, dans le cas contraire, on écrit $a \notin A$.
- Un ensemble peut être écrit :
  - En extension : On donne la liste de ses éléments
  - En compréhension : On donne la ou les propriétés qui caractérisent ses éléments.
- L'ensemble vide noté $\emptyset$ où $\{\}$ est l'ensemble qui ne contient aucun élément.

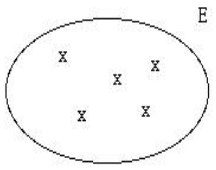
1.2 Cardinal d'un ensemble

Le Cardinal d'un ensemble E, noté Card(E) est le nombre d'éléments de E.

On le note aussi parfois $\#E$ ou $|E|$.

1.3 Représentation d'un ensemble

Un ensemble peut être représenté par un diagramme d'Euler-Venn comme illustré ci-dessous :



Les croix désignent les éléments de E.

1.4 Relations entre ensembles

On fixe un référentiel E.

1.4.1 L'inclusion

On dira qu'un ensemble A est inclus dans un ensemble B, où encore que A est un sous-ensemble ou une partie de B, si :

$$\forall x \in E, (x \in A) \Rightarrow (x \in B)$$

On écrit alors $A \subset B$.

1.4.2 L'égalité d'ensembles

Deux ensembles A et B qui contiennent les mêmes éléments sont dits égaux, et on écrit $A = B$.

1.5 Ensemble des parties d'un ensemble

Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble de toutes les parties de E.

Théorème 1.5.1 *Si* $\text{Card}(E) = n$ *alors* $\text{Card}\left(\mathcal{P}(E)\right) = 2^n$.

1.6 Opérations sur les ensembles

Soit E un référentiel et A, B deux parties de E. On définit dans $\mathcal{P}(E)$ les opérations suivantes :

1.6.1 La réunion

$$A \cup B = \{x \in E \text{ tels que } x \in A \underline{\text{ou}}\ x \in B\}$$

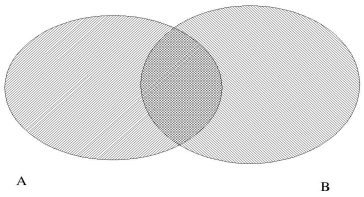


FIG. 1.1 – *La partie grisée représente l'union des ensembles A et B*

1.6.2 L'intersection

$$A \cap B = \{x \in E \text{ tels que } x \in A \underline{\text{et}}\ x \in B\}$$

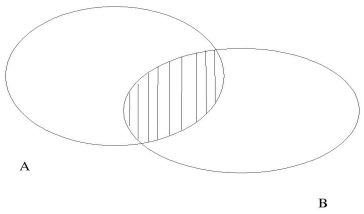


FIG. 1.2 – *La partie grisée représente l'intersection des ensembles A et B*

1.6.3 La différence d'ensemble

$$A \backslash B = \{x \in E \text{ tels que } x \in A \text{ et } x \notin B\}$$

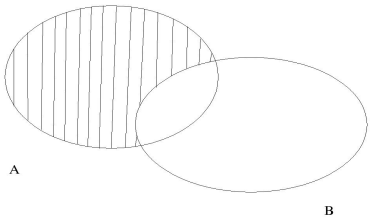


FIG. 1.3 – *La partie grisée représente la différence des ensembles A et B*

1.6.4 Cas particulier : la complémentation

$$\overline{A} = E \backslash A = \{x \in E \text{ tels que } x \notin A\}$$

La complémentation est une opération unaire.

1.7 Propriétés des opérations sur les ensembles

Soient, dans un référentiel E, trois ensembles A, B, et C.

1.7.1 Commutativité de la réunion et l'intersection

$$A \cup B = B \cup A \text{ et } A \cap B = B \cap A$$

1.7.2 Associativité de la réunion et l'intersection

$$(A \cup B) \cup C = A \cup (B \cup C) \text{ et } (A \cap B) \cap C = A \cap (B \cap C)$$

1.7.3 Idempotence

$$A \cup A = A \text{ et } A \cap A = A$$

1.7.4 Distributivité

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \text{ et } A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Attention : En général, on n'a pas

$$A \cup (B \cap C) = (A \cup B) \cap C$$

l'emploi des parenthèses est donc indispensable !

1.7.5 Dualité (Formules de De Morgan)

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \text{ et } \overline{A \cap B} = \overline{A} \cup \overline{B}$$

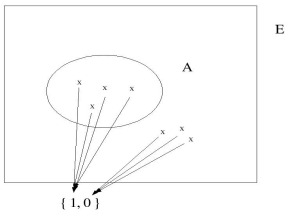
1.7.6 Absorption

$$\text{Si } B \subset A \text{ Alors } A \cap B = B \text{ et } A \cup B = A$$

1.8 Fonctions Caractéristiques

Soit dans un référentiel E, un sous-ensemble A. On définit la fonction caractéristique de A, notée $\mathbf{1}_A$ l'application définie par :

$$\begin{array}{rcl} \mathbf{1}_A : E & \longrightarrow & \{0,1\} \\ x & \mapsto & \begin{cases} 1 & \text{si} \quad x \in A \\ 0 & \text{si} \quad x \notin A \end{cases} \end{array}$$



On note $\chi(E)$ l'ensemble des applications caractéristiques.

Théorème 1.8.1 *$\chi(E)$ est en bijection avec $\mathcal{P}(E)$.*

Théorème 1.8.2 *Soit f une application de E dans $\{0,1\}$, alors $f \in \chi(E)$.*

1.8.1 Propriétés des Fonctions Caractéristiques

Soient A et B deux parties de E.

- $A \subset B \Leftrightarrow \mathbf{1}_A \leq \mathbf{1}_B$
- $A = B \Leftrightarrow \mathbf{1}_A = \mathbf{1}_B$
- $\mathbf{1}_{A \cap B} = \mathbf{1}_A \mathbf{1}_B$
- $\mathbf{1}_{A \cup B} = \mathbf{1}_A + \mathbf{1}_B - \mathbf{1}_A \mathbf{1}_B$
- $\mathbf{1}_{A \setminus B} = \mathbf{1}_A - \mathbf{1}_A \mathbf{1}_B$
- En particulier, $\mathbf{1}_{\overline{A}} = 1 - \mathbf{1}_A$

Chapitre 2

Relations binaires

Plan

1. Définitions, Exemples et Représentations
2. Compositions de Relations Binaires
3. Transposée d'une Relation Binaire
4. Relations Binaires sur un Ensemble
5. Relations d'équivalence
6. Relations d'Ordre Partiel
   (a) Diagrammes de Hasse
   (b) Eléments Particuliers

2.1 Définitions, Exemples et Représentations

2.1.1 Définition

Soient $A = \{a_1, a_2, \ldots, a_n\}$ et $B = \{b_1, b_2, \ldots, b_n\}$ (cas fini), ou $A = \{a_1, a_2, \ldots, a_n \ \ldots\}$ et $B = \{b_1, b_2, \ldots, b_n, \ldots\}$ (cas infini),

Définition 2.1.1 *Le produit cartésien de $A \times B$ est l'ensemble des paires ordonnées*

$$(a_i, b_j) \text{ où } a_i \in A \text{ et } b_j \in B.$$

Définition 2.1.2 *Une relation binaire $\mathcal{R}$ est un sous-ensemble de $A \times B$.*

On note $a\mathcal{R}b$ si $(a, b) \in \mathcal{R}$.

2.1.2 Exemples

Exemple 2.1.3 *Soient* $A = \{Albert,\ Bernard,\ Charles\}$, $B = \{Zoé,\ Yolande,\ Xavière,\ Wanda\}$ *et la relation* $a\mathcal{R}b$ *si et seulement si* a *est le mari de* b.

$$\mathcal{R} = \{(Albert, Zoé),\ (Bernard, Wanda),\ (Charles, Yolande)\}$$

Exemple 2.1.4 $A = \mathbb{Z}$ *et* $B = \mathbb{N}$ *et*

$$\begin{aligned} \mathcal{R} &= \{(0,0), (-1,1), (1,1), (-2,4), (2,4), \ldots\} \\ &= \{(x, x^2) : x \in \mathbb{Z}\} \end{aligned}$$

2.1.3 Représentation des Relations Binaires

On suppose que A et B sont des ensembles finis de cardinal respectif m et n.

2.1.3.1 Représentation matricielle

On peut représenter $\mathcal{R}$ par une matrice R comportant m lignes et n colonnes dont les coefficients sont 0 où 1. On définit les éléments de la matrice R de la manière suivante :

$$\begin{aligned} r_{ij} &= 1 \text{ si } a_i \mathcal{R} b_j \\ &= 0 \text{ sinon.} \end{aligned}$$

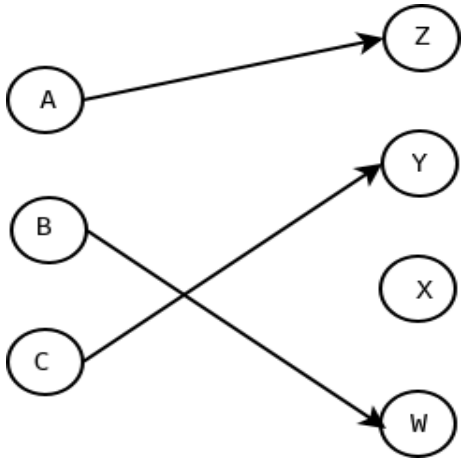
Exemple 2.1.5 *Reprenons l'exemple (2.1.3). La matrice* R *de la relation* $\mathcal{R}$ *est la suivante*

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

2.1.3.2 Représentation par un graphe

On peut représenter $\mathcal{R}$ par un graphe bipartite (c'est à dire qu'il y a une partition $A \cup B$ des sommets du graphe et que chaque arc va de A vers B)

$$G_{\mathcal{R}} = (A \cup B, \mathcal{R})$$



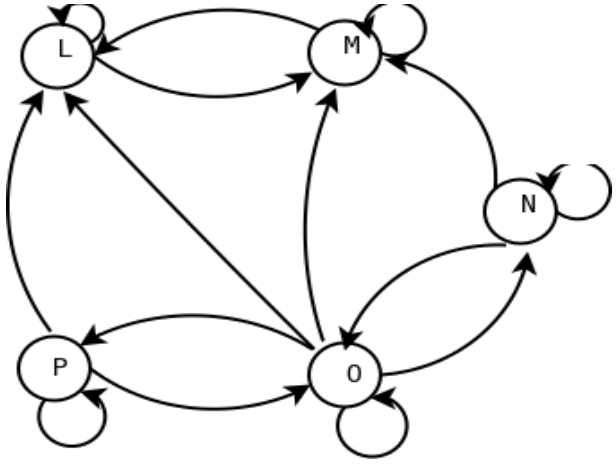
Les ensembles A et B ont été défini dans l'exemple (2.1.3). Chaque sommet contient l'initial d'un prénom.

Cas particulier : Relation sur un ensemble

Si $\mathcal{T} \subset (A \times A)$, on la représente à l'aide d'un graphe usuel. Soient, l'ensemble

$$C = \{\text{Léo}, \text{Mathieu}, \text{Nathalie}, \text{Ophélie}, \text{Patrick}\}$$

et la relation $\mathcal{T} \subset (A \times A)$ définie par $a\mathcal{T}b$ si et seulement si a connait b.



2.2 Compositions de relations

Soient $\mathcal{R} \subset (A \times B)$ et $\mathcal{S} \subset (B \times C)$ deux relations.

Définition 2.2.1 *La relation $\mathcal{R}\circ\mathcal{S}$ est une relation binaire sur $A\times C$ appelée* composée *de $\mathcal{R}$ et $\mathcal{S}$ telle que*

$$a(\mathcal{R}\circ\mathcal{S})c \Leftrightarrow \exists b \in B, (a\mathcal{R}b \wedge b\mathcal{S}c) \tag{2.1}$$

Proposition 2.2.2 *Soient $\mathcal{R} \subset (A \times B)$, $\mathcal{S} \subset (B \times C)$ et $\mathcal{T} \subset (C \times D)$, trois relations, alors*

$$(\mathcal{R} \circ \mathcal{S}) \circ \mathcal{T} = \mathcal{R} \circ (\mathcal{S} \circ \mathcal{T})$$

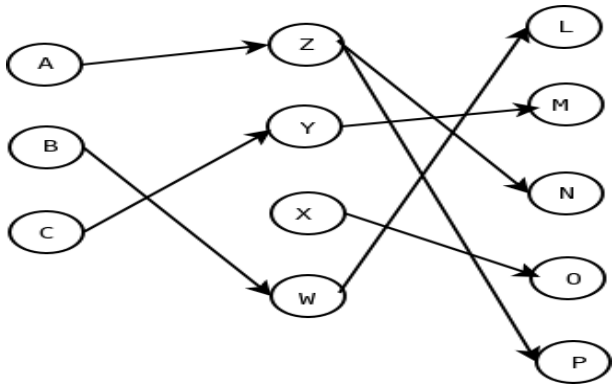
La composée de deux relations est associative.

Exemple 2.2.3 *Soient, l'ensemble*

$$C = \{Léo, Mathieu, Nathalie, Ophélie, Patrick\}$$

la relation $\mathcal{R} \subset (A \times B)$ vu à l'exemple (2.1.3) et la relation $\mathcal{S} \subset (B \times C)$ définie par $b\mathcal{S}c$ si et seulement si b est la mère de c :

$$\begin{aligned}\mathcal{S} \quad = \{ \quad & \textit{(Zoé, Nathalie)}, \textit{(Zoé, Patrick)}, \textit{(Yolande, Mathieu)}, \\ & \textit{(Xavière, Ophélie)}, \textit{(Wanda, Léo)}\}\end{aligned}$$



Alors

$$\begin{aligned}\mathcal{R}\circ\mathcal{S} \quad = \{ \quad & \textit{(Albert, Nathalie)}, \textit{(Albert, Patrick)}, \textit{(Bernard, Léo)}, \\ & \textit{(Charles, Mathieu)}\}\end{aligned}$$

Règle 1 *$a(\mathcal{R}\circ\mathcal{S})c$ si, et seulement si, il existe un chemin orienté dans le graphe de a vers c.*

Pour construire la matrice de la relation composée $\mathcal{T} = \mathcal{R}\circ\mathcal{S}$, il faut effectuer le produit booléen des matrices R et S défini par

$$t_{ij} = r_{i1}.s_{1j} + \ldots + r_{in}.s_{nj} = \sum_k r_{ik}s_{kj}$$

où les sommes et les produits sont définis au sens booléen.

2.3 Transposée d'une Relation Binaire

Définition 2.3.1 *Soit $\mathcal{R} \subset (A \times B)$ une relation. la* transposée *de $\mathcal{R}$ est la relation $\mathcal{R}^T \subset (B \times A)$ définie par :*

$$b\mathcal{R}^T a \Leftrightarrow a\mathcal{R}b$$

Pour représenter $\mathcal{R}^T$, il suffit d'inverser les flèches du graphe de $\mathcal{R}$ ou de transposer la matrice R.

2.4 Relations binaires sur un ensemble

Soit A un ensemble, et soit $\mathcal{R} \subset (A \times A)$ une relation sur cet ensemble. On dit que :

1. $\mathcal{R}$ est *réflexive* ssi $\forall a \in A, a\mathcal{R}a$
2. $\mathcal{R}$ est *symétrique* ssi $\forall a \in A, \forall b \in A, a\mathcal{R}b \Rightarrow b\mathcal{R}a$
3. $\mathcal{R}$ est *antisymétrique* ssi $\forall a \in A, \forall b \in A, a\mathcal{R}b \wedge b\mathcal{R}a \Rightarrow a = b$
4. $\mathcal{R}$ est *transitive* ssi $\forall a \in A, \forall b \in A, \forall c \in A, a\mathcal{R}b \wedge b\mathcal{R}c \Rightarrow a\mathcal{R}c$.

Exemple 2.4.1 *Soient $A = \mathbb{Z}$, et la relation $a\mathcal{R}b \Leftrightarrow a \geq b$, alors $\mathcal{R}$ est réflexive, non symétrique, antisymétrique, transitive.*

Exemple 2.4.2 *Soient $A = \mathbb{Z}$, et la relation $a\mathcal{R}b \Leftrightarrow a > b$, alors $\mathcal{R}$ est non réflexive, non symétrique, antisymétrique, transitive.*

Exemple 2.4.3 *Soient $A = \mathbb{Z}$, et la relation $a\mathcal{R}b \Leftrightarrow |x - y| \leq 1$, alors $\mathcal{R}$ est réflexive, symétrique, non antisymétrique, non transitive.*

2.5 Relations d'équivalence

Définition 2.5.1 *Une* relation d'équivalence *est une relation sur un ensemble A qui est réflexive, symétrique et transitive.*

Exemple 2.5.2 *Soient $A = \mathbb{Z}$, et la relation définie par :*

$$a\mathcal{R}b \Leftrightarrow \exists k \in A, x - y = 2.k$$

alors cette relation est

1. *réflexive car $x - x = 2.0$*

2. *symétrique car* $x - y = 2.k \Rightarrow y - x = 2.(-k)$
3. *transitive car si* $x - y = 2.k_1$ *et* $y - z = 2.k_2 \Rightarrow x - z = 2.(k_1 + k_2)$

Définition 2.5.3 *Soit x un élément de A, sa classe d'équivalence notée $\dot{x}$ est l'ensemble $\{y \in A : x\mathcal{R}y\}$.*

Exemple 2.5.4 *Dans l'exemple précédent, la classe d'quivalence de 4 est $\{0, 2, -2, 4, -4, \ldots, 2n, -2n, \ldots\}$, l'ensembles des entiers relatifs pairs. La classe d'équivalence de 3 est $\{1, -1, 3, -3, \ldots, 2n+1, -2n+1, \ldots\}$ l'ensemble des entiers relatifs impairs.*

Proposition 2.5.5 *Soit $\mathcal{R}$ une relation d'équivalence sur A. Tout élément de A appartient à une et une seule classe d'équivalence.*

La conséquence de cette proposition est que l'ensemble des classes d'équivalence définit une *partition* de A (c'est à dire des sous-ensembles non vides de A, disjoints 2 à 2, et dont l'union est A).

2.6 Relations d'Ordre Partiel

Définition 2.6.1 *Une relation $\mathcal{R}$ qui est réflexive, antisymétrique et transitive sur un ensemble A est appelé un* ordre partiel *sur A. On dit alors que $(A, \mathcal{R})$ est un ensemble partiellement ordonné.*

Les relations d'ordre partiel sont souvent notées $\preceq$.

Définition 2.6.2 *Si pour tout couple d'élément (a, b) de $A \times A$, on a $a\mathcal{R}b$ ou $b\mathcal{R}a$, alors on dit que $(A, \mathcal{R})$ est un ensemble totalement ordonné.*

Un ensemble est totalement ordonné si tous les éléments sont comparables entre eux.

2.6.1 Exemples

Exemple 2.6.3 *On prend $E = \mathcal{P}(A)$ (l'ensemble des parties de A) où E est un ensemble quelconque, la relation $X\mathcal{R}Y \Leftrightarrow X \subset Y$ est un ordre partiel.*

Exemple 2.6.4 *Soient $a, b \in \mathbb{N}$, on dit que a divise b et on écrit $a|b$ si et seulement si $\exists c \in \mathbb{N}$ tel que $b = a.c$.*

La relation $|$ est réflexive, antisymétrique et transitive.

L'ensemble $(\mathbb{N}, |)$ est donc partiellement ordonné.

Exemple 2.6.5 *Soit $(A, \preceq)$ un ensemble partiellement ordonné. On définit sur $A \times A$ une relation de la manière suivante : on dit que $(a_1, a_2) \preceq (b_1, b_2)$ si $a_1 \preceq b_1$ ou si $a_1 = b_1$ et si $a_2 \preceq b_2$.*

Cette relation s'appelle l'ordre lexicographique.

2.6.2 Diagramme de Hasse

Définition 2.6.6 *Les ordres partiels peuvent se représenter par un* diagramme de Hasse *en appliquant la règle suivante :*

- *Les éléments sont représentés par des sommets*
- *a et b sont joints par une arête si et seulement si*

$$a \preceq b \text{ et } \nexists z \in A, a \preceq z \text{ et } z \preceq b$$

En d'autre terme les raccourcis ne doivent pas figurer dans le graphe.

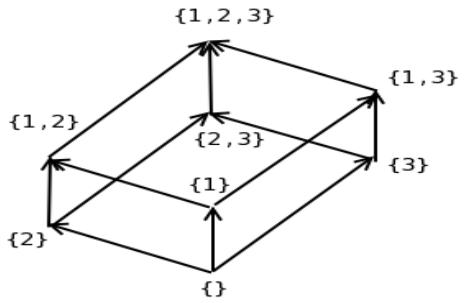


FIG. 2.1 – Diagramme de Hasse de $(\mathcal{P}(\{1,2,3\}), \subset)$.

2.6.3 Eléments Particuliers

Soit $(A, \preceq)$ un ensemble ordonné et soit $X \subset A$ un sous ensemble de A.

Définition 2.6.7 *Un élément $a \in A$ est un* majorant *de X si $\forall x \in X$ on a $x \preceq a$.*

Définition 2.6.8 *Un élément $a \in A$ est un* minorant *de X si $\forall x \in X$ on a $a \preceq x$.*

Définition 2.6.9 *Tout élément de $x \in X$ qui n'est majoré que par lui même dans X est appelé un élément* maximal *de X.*

Définition 2.6.10 *Tout élément de $x \in X$ qui n'est minoré que par lui même dans X est appelé un élément* minimal *de X.*

Remarque 1 *Il n'existe pas nécessairement de majorant ou de minorant, par contre il existe nécessairement au moins un élément maximal et un élément minimal.*

Définition 2.6.11 *On appelle* maximum *(plus grand élément) de X, s'il existe, un élément de X qui est un majorant de X.*

Définition 2.6.12 *On appelle* minimum *(plus petit élément) de X, s'il existe, un élément de X qui est un minorant de X.*

Définition 2.6.13 *On appelle* borne supérieure *de X, s'il existe, le minimum des majorants de X.*

Définition 2.6.14 *On appelle* borne inférieure *de X, s'il existe, le maximum des minorants de X.*

Définition 2.6.15 *On appelle* élément universel *de A, s'il existe, le maximum de A. On le note en général* 1*, et vérifie donc la propriété :*

$$\forall x \in A, \qquad x \preceq 1$$

Définition 2.6.16 *On appelle* élément nul *de A, s'il existe, le maximum de A. On le note en général* 0*, et vérifie donc la propriété :*

$$\forall x \in A, \qquad 0 \preceq x$$