

MATHÉMATIQUES POUR L'INFORMATIQUE 2

LES COURS DU MODULE " MPI " DU SEMESTRE 3

KILLIAN REINE

*Licence 2
Orientation Informatique*

RESSOURCES UTILISÉES :

- SUPPORTS DE COURS, CHRISTOPHE DUHAMEL
- SUPPORTS DE COURS, SAMUEL CITEAU
- SUPPORTS TUTORAT MPI 2023-2024, KILLIAN REINE

TABLE DES MATIÈRES

0 Notions préliminaires	4
0.1 Rappels et généralités sur les ensembles	4
0.2 Rappel sur le produit cartésien	8
0.3 Ensembles disjoints	8
1 Relations binaires	9
1.1 Rappels et généralités	9
1.2 Propriété des relations binaires	10
1.3 Relation d'équivalence	11
1.4 Partition d'un ensemble	13
1.5 Relation d'ordre	14
1.6 Diagramme de Hasse	15
1.7 Extrema d'un ensemble ordonné	16
1.8 Morphisme d'ordre	17
2 Graphes	18
2.1 Quelques généralités sur les graphes	18
2.2 Graphes particuliers	21
2.3 Parcours de graphe	24
2.4 Retour sur les graphes particuliers	25
2.4.1 Arbre et forêts	25
2.4.2 Graphe bipartis	26
2.4.3 Graphe planaire	27
2.4.4 Arbres couvrants	29
2.5 Graphe pondéré	29
2.6 Coloration de graphe	30
2.6.1 L'Heuristique de Welsh et Powell	31
3 Algèbre de Boole	32
3.1 Bases et généralités	32
3.2 Atomes	34
3.3 Théorème de Stone	36
3.4 Algèbre de Boole engendrée	37
4 Théorie des codes	39
4.1 Le codage de l'information	39
4.2 Code détecteur, code correcteur	41

4.3 Différents codages possibles	41
4.4 Représentation du code	42

CHAPITRE 0

NOTIONS PRÉLIMINAIRES

0.1) Rappels et généralités sur les ensembles

DÉFINITION (ensemble)

En mathématiques **un ensemble** est une collections d'objets distincts. Chacun des objet est appelé "élément" de l'ensemble.

D'une manière plus simple, un ensemble peut être vu comme une boîte contenant des formes toutes différentes les unes que les autres.

- L'ordre des éléments n'a pas d'importance
- Chaque élément de l'ensemble est unique, il ne peut donc pas y avoir de doublons.

Remarque

Généralement, un ensemble peut être définit de deux manières :

- En extension**, on donne la liste des éléments
- En compréhension**, on donne une propriété
Les éléments de l'ensembles doivent donc respecter la propriété.

Rappel de cours

Par conventions :

- Les ensembles sont notés avec une majuscule.
- Les éléments d'un ensembles sont entre accolades $\{\dots\}$ et séparés par des virgules.

Exemples, Différentes définition d'un ensembles

Type d'ensemble	Exemple	Nombre d'éléments
Ensemble fini	$E = \{1, 2, 3, 4, 5, 6\}$	x
Ensemble infini	$E = \mathbb{R}$	∞
Ensemble vide	$E = \{\}$ ou $E = \emptyset$	0
Singleton	$E = \{\text{juste_moi}\}$	1
Ensemble pair	$E = \{\text{toi, moi}\}$	2

- Remarque** || Il existe d'autres types d'ensembles :
- L'ensemble booléen $\{0, 1\}$
 - L'ensemble en compréhension : $E = \{x \in E \mid \mathcal{P}(x)\}$

DÉFINITION (L'inclusion)

Soient A et B deux parties de E

On dit qu'un ensemble A **est inclus dans** un ensemble B si tous les éléments de A sont aussi éléments de B .

Il faut que tous les éléments de A appartiennent aussi à B .

On note :

$$A \subset B \iff \forall x \in A, x \in B$$

Si $A \subset B$ alors on dit que A **est une partie de** B . Ou alors que A **est un sous-ensemble** de B .

Exemple

$$\{-1, 0, 1, 2\} \not\subset \mathbb{N} \text{ mais par contre, } \{-1, 0, 1, 2\} \subset \mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$$

DÉFINITION (L'égalité)

Soient A et B deux parties de E

Les ensembles A et B sont **égaux** s'ils ont exactement les mêmes éléments.

On note :

$$\forall x, (x \in A \iff x \in B)$$

Remarque

Pour montrer que deux ensembles sont égaux, il suffit de montrer l'inclusion des ensembles dans les deux sens.

Soient E un ensemble et A, B deux parties de E

$$A = B \iff A \subset B \wedge B \subset A$$

Rappel de cours

Le symbole \wedge signifie "et". Tandis que le symbole \vee signifie "ou".

Exemple d'application

Montrer que les ensembles suivants sont égaux.

$$A = \{x^2 - 4x + 3 = 0\} \text{ et } B = \{x = 1 \vee x = 3\}$$

Pour montrer que $A \subset B$, nous devons résoudre l'équation de degré 2.

$$\Delta = b^2 - 4ac = (-4)^2 - 4 \times 1 \times 3 = 16 - 12 = 4$$

Les racines réelles sont donc :

$$x_1 = \frac{4 + \sqrt{4}}{2} = \frac{6}{2} = 3 \text{ et } x_2 = \frac{4 - \sqrt{4}}{2} = \frac{2}{2} = 1$$

Les solutions de l'équation sont donc $x = 1$ et $x = 3$, exactement le contenu de l'ensemble B ainsi, $A \subset B$.

Pour montrer que $B \subset A$.

relérons chaque élément de B et montrons qu'il respecte la condition pour appartenir à A .

Soit $x = 1$ alors $1^2 - 4 \times 1 + 3 = 0$ d'où $1 \in A$

Soit $x = 3$ alors $3^2 - 4 \times 3 + 3 = 9 - 12 + 3 = 0$ d'où $3 \in A$

Ainsi A contient 1 et 3 donc $B \subset A$.

Ainsi les deux inclusions montrent que $A = B$.

DÉFINITION (L'union)

Soient A et B deux parties de E .

L'**union** notée $A \cup B$ de deux ensemble représente l'ensemble des éléments présents dans A ou dans B .

Autrement dit, faire l'union de deux ensembles revient à créer un ensemble contenant à la fois les éléments de A puis ceux de B .

On note :

$$A \cup B = \{x \in E \mid x \in A \vee x \in B\}$$

DÉFINITION (L'intersection)

Soient A et B deux parties de E .

L'**intersection** notée $A \cap B$ de deux ensemble représente l'ensemble des éléments présents à la fois dans A et aussi dans B .

Autrement dit, l'intersection de deux ensemble revient à créer un ensemble contenant les éléments communs à A et B .

On note :

$$A \cap B = \{x \in E \mid x \in A \wedge x \in B\}$$

DÉFINITION (La différence)

Soient A et B deux parties de E .

La **différence** notée $A \setminus B$ de deux ensemble représente l'ensemble des éléments qui appartiennent à A mais pas à B . On lit aussi " A privé de B ".

Autrement dit, la différence de A par B revient à créer un ensemble qui contiendra les éléments présent uniquement dans A .

On note :

$$A \setminus B = \{x \in A \mid x \notin B\}$$

DÉFINITION (Le complémentaire)

Soient A une partie de E .

Le **complémentaire**, noté $C_E(A)$ représente l'ensemble des éléments de E n'appartenant pas à A . Le complémentaire peut aussi être noté A^c , \overline{A} ou encore $E \setminus A$.

On note :

$$C_E(A) = \{x \in E \mid x \notin A\}$$

Propriétés

□ Propriété sur les ensembles

Soient E, F et G trois ensembles.

- $\emptyset \subset E$ (resp. F , resp. G).

L'ensemble vide est inclu dans tout ensemble.

- **Réflexivité** $E \subset E$, un ensemble est inclu dans lui-même.

- **Antisymétrie** $E \subset F$ et $F \subset E \iff E = F$

Lorsque deux ensembles sont inclu l'un dans l'autre, cela implique forcément l'égalité.

- **Transitivité** $E \subset F$ et $F \subset G \implies E \subset G$

□ Le complémentaire \complement est prioritaire sur l'union \cup et sur l'intersection \cap .

□ L'union \cup et l'intersection \cap sont prioritaire sur l'égalité $=$ et sur l'inclusion \subset .

□ Soient E une ensemble et A, B, C trois parties de E .

1. Propriété de l'union \cup et de l'intersection \cap

(a) **Associativité :**

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

(b) **Commutativité**

$$A \cap B = B \cap A \quad A \cup B = B \cup A$$

(c) **Distributivité**

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

2. Propriété du complémentaire \complement

(a) $\complement_E(E) = \emptyset$, si on prive un ensemble de lui-même, il ne reste rien.

(b) $\complement_E(\emptyset) = E$, si je prive E de rien, il me reste E .

(c) $\complement_E(\complement_E(A)) = A$, le complémentaire s'annule.

(d) $\complement_E(A) \cup A = E$, on prive A pour ensuite faire l'union de E et A .

(e) $\complement_E(A) \cap A = \emptyset$, on prive A pour ensuite faire l'intersection de ce que l'on vient de priver.

(f) **Distributivité** du complémentaire

$$\complement_E(A \cup B) = \complement_E(A) \cap \complement_E(B) \quad \complement_E(A \cap B) = \complement_E(A) \cup \complement_E(B)$$

Remarque

Les propriétés du complémentaires et celles qui sont censées être connues permettent de déterminer les égalités suivantes :

$$A \setminus B = A \cup \complement_E(B) = A \setminus (A \cap B) \quad A = (A \cap B) \cup (A \cap \complement_E(B))$$

0.2) Rappel sur le produit cartésien

DÉFINITION (*n-uplet & produit cartésien*)

Soient $n \geq 2 \in \mathbb{N}^*$ et E_1, E_2, \dots, E_n n ensembles.

- $\forall x_1 \in E_1, \dots, x_n \in E_n$, (x_1, \dots, x_n) est un objet mathématique ordonné à n élément et est aussi appelé n -uplet. $\forall i \in [1; n]$, l'élément x_i est la i -ième composante du n -uplet.
- Le produit cartésien des ensembles E_1, \dots, E_n est l'ensemble noté $E_1 \times \dots \times E_n$ défini par :

$$E_1 \times \dots \times E_n = \{(x_1, \dots, x_n) \mid x_1 \in E_1, \dots, x_n \in E_n\}$$

On note aussi $\prod_{i=1}^n E_i$

Exemple

Soient $A = \{1, 2, 3\}$ et $B = \{1, 7, 8, 9\}$ deux ensembles alors le produit cartésien AB est données par :

$$AB = \{(1, 1), (1, 7), (1, 8), (1, 9), (2, 1), (2, 7), (2, 8), (2, 9), (3, 1), (3, 7), (3, 8), (3, 9)\}$$

0.3) Ensembles disjoints

DÉFINITION (*ensemble disjoint*)

En théorie des ensemble,

Soit E un ensemble et A, B deux parties de E . On dit que " A et B sont disjoints " lorsque :

$$A \cap B = \emptyset$$

En d'autre termes deux ensembles sont disjoints **si ils n'ont aucun élément en commun**.

Exemple

Soient $A = \{1, 8, 4, 5, 7\}$, $B = \{9, 10, 0, 2\}$ et $C = \{1, 84, 7\}$

- $A \cap B = \{x \in A \wedge x \in B\} = \emptyset$, A et B sont disjoints.
- $A \cap C = \{x \in A \wedge x \in C\} = \{1, 7\}$, A et C ne sont pas disjoints.
- $B \cap C = \{x \in B \wedge x \in C\} = \emptyset$, B et C sont disjoints.

CHAPITRE 1

RELATIONS BINAIRES

1.1) Rappels et généralités

DÉFINITION (*relation binaire*)

Soit A, B deux ensembles.

Une **relation binaire** sur A et B est une partie $\mathcal{R} \subseteq A \times B$. Deux éléments $a \in A, b \in B$ sont en relation si et seulement si $(a, b) \in \mathcal{R}$. On note alors $a \mathcal{R} b$.

Cas particulier, $a = b$ alors \mathcal{R} est "une relation binaire sur A ".

Exemples, représentation d'une relation binaire

1. Représentation ensembliste

En donnant l'ensemble des paires d'éléments en relation.

$$\mathcal{R} = \{(0, 7), (1, 7), (8, 2)\}$$

2. Représentation matricielle

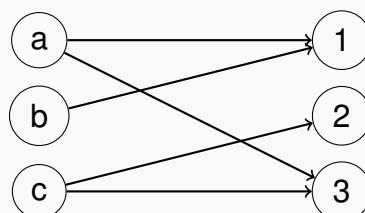
Une matrice \mathcal{M} de A vers B $\mathcal{M}_{ij} = 1 \leftrightarrow i \mathcal{R} j$ avec i les lignes et j les colonnes de la matrice.

$$\mathcal{M} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

3. Représentation avec un graphe

Les sommets représentent les éléments de A puis de B . La présence d'un arc entre un élément $a \in A$ et un élément de $b \in B$ signifie que $a \mathcal{R} b$.

Diagramme sagittal



Exemples, représentation d'une relation binaire sur A

1. Représentation ensembliste

Ici, les éléments de l'ensembles appartiennent à l'ensemble $A \times A$.

Soit $A = \{a, b, c\}$

On a la relation \mathcal{R} quelconque suivante :

$$\mathcal{R} = \{(a, a), (a, b), (a, c), (b, a), (b, c), (c, a), (c, b)\}$$

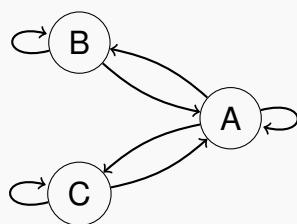
2. Représentation matricielle

Ici, puisque la relation se fait sur le même ensemble alors, la matrice sera carrée ($i = j$ même nombre de ligne et de colonne).

Considérons $\mathcal{R} = \{(a, a), (b, a), (c, a), (c, c)\}$

$$\mathcal{M} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

3. Représentation à l'aide d'un graphe



1.2) Propriété des relations binaires

Propriétés

Voici les propriétés fondamentales

Soit E une ensemble non vide et \mathcal{R} une relation.

La relation \mathcal{R} est dite :

- **Réfléxive** si $\forall x \in E, x \mathcal{R} x$
- **Symétrique** si $\forall (x, y) \in E^2, x \mathcal{R} y \Leftrightarrow y \mathcal{R} x$
- **Antisymétrique** si $\forall (x, y) \in E^2$ on a $(x \mathcal{R} y \wedge y \mathcal{R} x) \Rightarrow x = y$
- **Transitive** si $\forall (x, y, z) \in E^3$ on a $(x \mathcal{R} y \wedge y \mathcal{R} z) \Rightarrow x \mathcal{R} z$

Exemple

Soit $x, y \in E$ et \mathcal{R} la relation $x < y$.

Si $x < y$ alors $y \not< x$ cela impliquerait que $x = y$ donc la relation "inférieur strict" n'est pas antisymétrique.

1.3) Relation d'équivalence

DÉFINITION (*relation d'équivalence*)

Soit \mathcal{R} une relation sur un ensemble non vide A . La relation \mathcal{R} est dite d'équivalence si et seulement si \mathcal{R} est :

- Réflexive Symétrique Transitive

Remarque || Ainsi, pour montrer que \mathcal{R} est une relation d'équivalence, il suffira de montrer que les trois propriétés sont vérifiées.

DÉFINITION (*classe d'équivalence*)

Soit \mathcal{R} une relation d'équivalence sur un ensemble non vide A et $x \in A$. La classe d'équivalence notée $\mathcal{R}(x)$ représente l'ensemble des $y \in A$ tel que $x\mathcal{R}y$.

$$\mathcal{R}(x) = \{y \in A \mid x\mathcal{R}y\}$$

Autrement dit, la classe d'équivalence c'est en fait l'ensemble des éléments y de A qui sont en relation avec x .

Remarque || Chaque élément possède sa propre classe d'équivalence.
 Une classe d'équivalence contient entre 0 et $|A|$ éléments.

Rappel de cours

Soit A un ensemble. On note $|A|$ la cardinalité de l'ensemble, c'est à dire le nombre d'éléments que contient l'ensemble.

DÉFINITION (*Ensemble quotient*)

Soit \mathcal{R} une relation d'équivalence sur un ensemble non vide A et $x \in A$. L'ensemble quotient $A\backslash\mathcal{R}$ représente l'ensemble des classes d'équivalences distinctes de \mathcal{R} .

$$A\backslash\mathcal{R} = \{\mathcal{R}(x) \mid x \in A\}$$

Remarque || Il peut y avoir entre 1 et $|A|$ classes d'équivalences distinctes.

Propriétés

Soit \mathcal{R} une relation d'équivalence sur un ensemble non vide A . Alors les propriétés suivantes sont vérifiées :

- $\mathcal{R}(x) \neq \emptyset, \forall x \in A$
- Si $\mathcal{R}(x)$ et $\mathcal{R}(y)$ deux classes d'équivalences distinctes de $A \setminus \mathcal{R}$ alors :

$$\forall x, y \in A \quad \mathcal{R}(x) \neq \mathcal{R}(y), \quad \mathcal{R}(x) \cap \mathcal{R}(y) = \emptyset$$

$$\square A = \bigcup_{x \in A} \mathcal{R}(x)$$

Preuves / Démonstrations

1. $\mathcal{R}(x) \neq \emptyset, \forall x \in A$

Soit $x \in A$.

Puisque par définition d'une relation d'équivalence, \mathcal{R} est réfléxive alors $x \mathcal{R} x$ d'où $x \in \mathcal{R}(x)$ ainsi $\mathcal{R}(x) \neq \emptyset$.

2. $\forall x, y \in A \quad \mathcal{R}(x) \neq \mathcal{R}(y), \quad \mathcal{R}(x) \cap \mathcal{R}(y) = \emptyset$

Soit $x, y \in A$ avec $\mathcal{R}(x) \neq \mathcal{R}(y)$

Alors

$$\exists k \in A \mid k \in \mathcal{R}(x) \text{ et } k \notin \mathcal{R}(y) \text{ ou } \exists k \in A \mid k \notin \mathcal{R}(x) \text{ et } k \in \mathcal{R}(y)$$

Supposons qu'il existe un $k \in A$ tel que $k \in \mathcal{R}(x)$

Alors par définition de relation d'équivalence, \mathcal{R} est symétrique et puisque $k \in \mathcal{R}(x)$

Alors on a $x \mathcal{R} k$ et $k \mathcal{R} x$

Supposons que $\mathcal{R}(x) \cap \mathcal{R}(y) \neq \emptyset$

Alors cela voudrait dire que $\exists l \in A \mid l \in \mathcal{R}(x) \cap \mathcal{R}(y)$

Donc on a $x \mathcal{R} l$ et $y \mathcal{R} l$ puis par symétrie $l \mathcal{R} x$ et $l \mathcal{R} y$

Puis $k \mathcal{R} x$, $x \mathcal{R} l$ et $l \mathcal{R} y$ par transitivité $k \mathcal{R} y$ puis $y \mathcal{R} k$ par symétrie

Ce qui signifie que $k \in \mathcal{R}(y)$, ce qui contredit notre hypothèse

Ainsi, $\mathcal{R}(x) \cap \mathcal{R}(y) = \emptyset$

3. $A = \bigcup_{x \in A} \mathcal{R}(x)$

Soit $x \in A$

Alors $x \in \mathcal{R}(x)$ d'après 1.

Ducoup, par l'union $A \subset \bigcup_{x \in A} \mathcal{R}(x)$

De plus, $\mathcal{R}(x) \subset A$ par définition $\forall x \in A$

Alors, par l'union $\bigcup_{x \in A} \mathcal{R}(x) \subset A$

Ainsi $A = \bigcup_{x \in A} \mathcal{R}(x)$

1.4) Partition d'un ensemble

DÉFINITION (*partition*)

Soit $A \neq \emptyset$ et I un ensemble d'indice. Une famille $(P_i)_{i \in I}$ de parties de A est une partition de A si :

$$\square \forall i \in I, P_i \neq \emptyset \quad \square \forall i \neq j \in I, P_i \cap P_j = \emptyset \quad \square \bigcup_{i \in I} P_i = A$$

Proposition

Soit A un ensemble non-vide.

- Soit \mathcal{R} une relation sur A alors les classes d'équivalences distinctes forment une partition de A .
- Soit $(P_i)_{i \in I}$ une partition de A . Alors la relation \mathcal{R} définie sur A par :

$$\forall x, y \in A \quad x \mathcal{R} y \Leftrightarrow \exists \alpha \in I \mid x, y \in P_\alpha$$

est une relation d'équivalence sur A .

Exemple

La relation suivante est-elle une relation d'équivalence ?

$$\forall x, y \in \mathbb{N} \quad x \mathcal{R} y \Leftrightarrow |x - y| \leq 2$$

1. Réfléxivité

Soit $x \in \mathbb{N}$

Alors on a $x \mathcal{R} x = |x - x| = |0| = 0 < 2$ alors \mathcal{R} est réfléxive.

2. Symétrie

Soit $x, y \in \mathbb{N}$

Alors on a $|b - a| \leq 2 \Rightarrow x \mathcal{R} y = |a - b| = |b - a| \leq 2 \Leftrightarrow y \mathcal{R} x$

Ainsi, \mathcal{R} est symétrique.

3. Transitivité

Soit $x, y, z \in \mathbb{N}$

On a $x = 2, y = 4$ et $z = 5$

Alors :

$$|2 - 4| = |-2| = 2 \leq 2 \text{ d'où } x \mathcal{R} y$$

$$|4 - 5| = |-1| = 1 \leq 2 \text{ d'où } y \mathcal{R} z$$

Et $|2 - 5| = |-3| = 3 > 2$ alors la transitivité n'est pas respectée.

\mathcal{R} n'est donc pas transitive, la relation n'est donc pas une relation d'équivalence.

Exercice

Pour chacune des relations binaires \mathcal{R} suivantes, déterminer si elles sont réflexives, symétriques ou transitives.

1. $\forall a, b \in \mathbb{Q}^*, a \mathcal{R} b \Leftrightarrow a \cdot b > 0$
2. $\forall a, b \in \mathbb{Q}^*, a \mathcal{R} b \Leftrightarrow \frac{a}{b} \in \mathbb{N}^*$
3. $\forall a, b \in \mathbb{R}, a \mathcal{R} b \Leftrightarrow a - b = a^2 - b^2$

1.5) Relation d'ordre

DÉFINITION (*relation d'ordre*)

Soit \mathcal{R} une relation sur un ensemble A non-vide. La relation \mathcal{R} est **une relation d'ordre** sur A si elle est :

- Réflexive Antisymétrique Transitive

On parle **d'ordre partiel** sur A .

Remarque || Une relation d'ordre est le plus souvent noté \leq ou $<$.

DÉFINITION (*relation d'ordre total*)

Soit \mathcal{R} une relation d'ordre sur un ensemble A . On parle de **relation d'ordre total** lorsque

$$\forall x, y \in A \quad x \mathcal{R} y \text{ ou } y \mathcal{R} x$$

Autrement dit, si tout les éléments sont en relation entre eux alors on parle d'ordre partiel.
On parle aussi **d'ordre total** sur A .

Remarque

Si un ensemble A est doté d'une relation d'ordre est appelé **ensemble ordonné** on note (A, \mathcal{R}) et si A est doté d'une relation d'ordre total on parlera donc **d'ensemble totalement ordonné**.

DÉFINITION (*ordre produit*)

Soient (A, \mathcal{R}) et (B, \mathcal{S}) deux relations d'ordre. Alors la relation \mathcal{T} définie par :

$$\forall (a, b), (c, d) \in A \times B, \quad (a, b) \mathcal{T} (c, d) \Leftrightarrow a \mathcal{R} c \text{ et } b \mathcal{S} d$$

est une relation d'ordre partielle sur $A \times B$. On l'appelle **la relation d'ordre produit** sur $A \times B$.

DÉFINITION (*ordre lexicographique*)

Soient (A, \mathcal{R}) et (B, \mathcal{S}) deux relations d'ordre. Alors la relation \mathcal{L} définie par :

$$\forall (a, b), (c, d) \in A \times B, \quad (a, b) \mathcal{L} (c, d) \Leftrightarrow (a \neq c, a \mathcal{R} c) \text{ ou } (a = c, b \mathcal{S} d)$$

est une relation d'ordre sur $A \times B$. On l'appelle aussi **ordre lexicographique** sur $A \times B$.

1.6) Diagramme de Hasse

DÉFINITION (prédécesseur, successeur)

Soit (A, \leq) un ensemble ordonné, et soient $x, y \in A$ deux éléments tels que $x \leq y$, $x \neq y$. On suppose de plus qu'il n'existe aucun élément $k \in A$ distinct de x et y tel que $x \leq k \leq y$. Alors :

- x est appelé **prédécesseur** de y .
- y est appelé **successeur** de x .

Remarque

- La condition imposée sur l'existence de k sert à empêcher l'application de la transitivité de la relation \leq entre x et y .
- Ainsi, les notions de prédécesseur et successeur sont définies de manière indépendante de la propriété de transitivité de la relation .

Tout ensemble ordonné **fini** (A, \leq) peut être représenté à l'aide d'un diagramme dit "de Hasse" construit comme suit :

- Chaque point du graphe représente un élément de A
- La position de chaque point suit les conditions suivantes
 - $x, y \in A$, $x < y$ selon la relation \leq , le point représentant x est placé en dessous de celui représentant y .
 - Dans le cas contraire le point x sera au dessus du point y .
- Deux points x et y correspondant aux sommets et sont reliés par un segment allant de x à y .

Exemple (1)

On considère le graphe suivant

Graphe de la relation

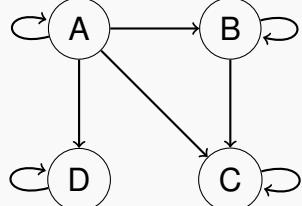
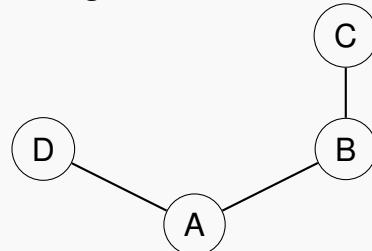


Diagramme de Hasse



- On enlève les boucles qui n'apparaissent pas sur le diagramme de Hasse
- On enlève les "arcs de transitivité"
- Ici on a $A \mathcal{R} B$ et $B \mathcal{R} C$ on enlève donc l'arc $A \mathcal{R} C$

Exemple (2)

On considère le graphe suivant.

Graphe de la relation

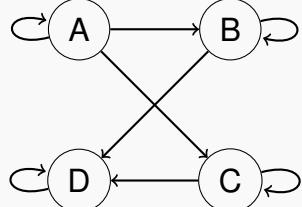
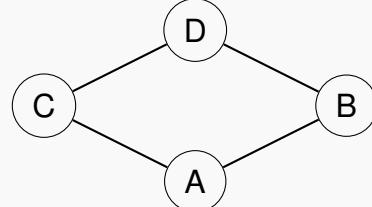


Diagramme de Hasse



- On enlève les "arcs de transitivité" (ici il n'y en a pas)
- On enlève les boucles

1.7) Extrema d'un ensemble ordonné

DÉFINITION (*maximum, minimum, maximal, minimal*)

Soit (A, \leq) un ensemble ordonné fini et $B \subseteq A$ un sous ensemble.

- $b \in B$ est appelé **minimum** de B si $\forall b' \in B$, on a $b' \leq b$
- $b \in B$ est appelé **maximum** de B si $\forall b' \in B$, on a $b' \geq b$
- $b \in B$ est appelé **minimal** de B si $\forall b' \in B$, on a $b' \leq b \Rightarrow b' = b$
- $b \in B$ est appelé **maximal** de B si $\forall b' \in B$, on a $b' \geq b \Rightarrow b' = b$

Remarque

à ne pas confondre

- Le minimum est le plus petit élément de B au sens de \leq , c'est à dire qu'il est plus petit que tous les éléments de B . De plus il est unique.
Sur le diagramme de Hasse, le minimum b est une racine unique
- La minimal lui, il n'y a aucun élément qui peut être plus petit que lui, sinon $b' = b$ au sens de \leq .
Dans le diagramme de Hasse, toutes les racines sont minimales.

Proposition

Soit (A, \leq) un ensemble ordonné fini et $B \subseteq A$ un sous-ensemble de A .

Alors si B admet un minimum (resp. maximum) alors il est **unique**.

Remarque

La maximum est noté $\max(B)$, le minimum $\min(B)$, si ils existent bien sur.

DÉFINITION (*majorant, minorant*)

Soit (A, \leq) un ensemble ordonné fini et $B \subseteq A$ un sous-ensemble de A .

- Le réel $\alpha \in A$ est appelé **majorant** de B si : $\forall b \in B, b \leq \alpha$
- Le réel $\alpha \in A$ est appelé **minorant** de B si : $\forall b \in B, b \geq \alpha$

Remarque

- Si il existe, le plus grand des minorants est appelé **Borne inférieure** de B et est noté $\inf(B)$
- Si il existe, le plus petit des majorants est appelé **Borne supérieure** de B et est noté $\sup(B)$
- Le minimum de B est la borne inférieure de B .
- Le maximum de B est la borne supérieure de B .
- En somme le maximal (resp. minimal) n'est pas nécessairement une borne de B .

1.8) Morphisme d'ordre

DÉFINITION (*morphisme d'ordre, isomorphisme d'ordre*)

Soient (A, \leq_A) et (B, \leq_B) deux ensembles ordonnés et $f : A \rightarrow B$ une application de A à valeurs dans B .

- On appelle **morphisme d'ordre** de A vers B toute application de A à valeurs dans B tel que :

$$\forall x, y \in A \quad x \leq_A y \Rightarrow f(x) \leq_B f(y)$$

- On appelle **isomorphisme d'ordre** de A vers B toute application bijective de A à valeurs dans B tel que :

$$\forall x, y \in A \quad x \leq_A y \Leftrightarrow f(x) \leq_B f(y)$$

CHAPITRE 2

GRAPHES

2.1) Quelques généralités sur les graphes

DÉFINITION *(graphe)*

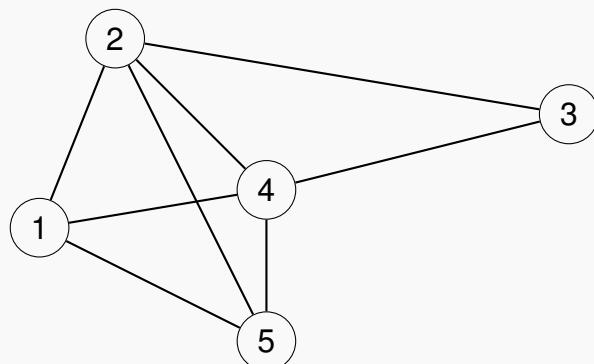
Un **graphe** $G = (\mathcal{S}, A, \phi)$ est un triplet avec :

- \mathcal{S}** l'**ensemble des sommets** du graphe
- A** l'**ensemble des arêtes** du graphes
- ϕ une **application** qui vas de A dans $\{\mathcal{S}' \subset \mathcal{S} \mid |\mathcal{S}'| = 2\}$ qui à chaque arrête $a \in A$ associe une paire $\{s_1, s_2\}$ de sommets, avec $s_1, s_2 \in \mathcal{S}$.

Vocabulaire supplémentaire :

- Les sommets qui définissent une arête sont appelés **extrémités**.
- Deux sommets sont **adjacents** s'ils sont extrémités d'une même arrête.
- Un sommet est **incident** à une arête a si et seulement si, il est une extrémité de a .

Exemple



- Le sommet 1 et le sommet 5 sont adjacents, ce sont les extrémités d'une même arrête.
- 2 est incidente à l'arrête $a = \{2, 5\}$.
- Les extrémités de $a = \{2, 5\}$ sont les sommets 2 et 5.

Remarque

On peut simplifier la définition d'un graphe.

Soit $G = (\mathcal{S}, A)$ en spécifiant l'ensemble des pairs de sommets mis en relation :

$$A = \{\{s_1, s_2\} \mid s_1, s_2 \in \mathcal{S}\}$$

A est l'ensemble des arrêtes.

DÉFINITION (degré)

Soit $G = (\mathcal{S}, A, \phi)$ un graphe, le **degré** d'un sommet $s \in \mathcal{S}$ est le nombre d'arrêtes incidents à ce sommet s .

Un **sommet isolé** si son degré est nul.

Exemple

En reprenant l'exemple ci-dessus, nous allons créer l'ensemble $\mathcal{D} = \{(s, d) \mid s \in \mathcal{S}, d \in \mathbb{N}\}$ où s est un sommet du graphe et d est le degré du sommet :

$$\mathcal{D} = \{(1, 3), (2, 4), (3, 2), (4, 3), (5, 3)\}$$

DÉFINITION (vocabulaire supplémentaire)

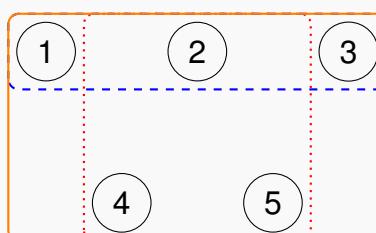
Soit $G = (\mathcal{S}, A, \phi)$ un graphe,

- On appelle **boucle** une arrête où ses extrémités désignent le même sommet.
- Deux arrêtes sont dites **parallèles** (= multiple) si leurs extrémités sont les mêmes.
- Un graphe est dit **simple** si il ne possède aucune arrête multiple.
- Tandis qu'un graphe G est dit **multiple** si il possède au moins une arrête multiple.

Remarque

Lorsque la cardinalité de deux éléments de l'application ϕ n'est pas limitée à 2 on parle alors d'**hypergraphe**, les éléments de l'ensemble A sont donc des hyperarêtes.

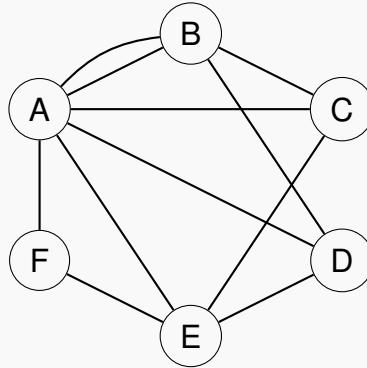
Un arrête multiple est une arrête qui relie plus de deux sommets.

Exemple d'hypergraphe

Ici, on a 3 hyperarêtes :

- $a_1 = \{1, 2, 3\}$ en bleu
- $a_2 = \{1, 2, 3, 4, 5\}$ en orange
- $a_3 = \{2, 4, 5\}$ en rouge

Exemple de graphe multiple



Ici, G est un egraphe multiple car il possède une arrête multiple entre A et B .

DÉFINITION (s)

Soit $G = (\mathcal{S}, A)$ un graphe simple,

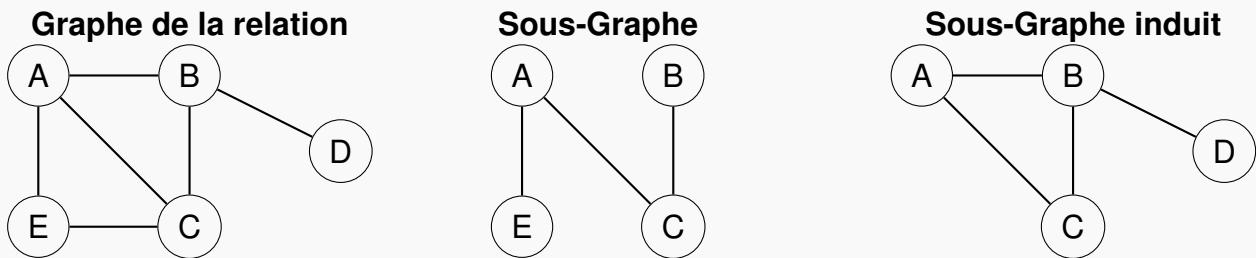
- On appelle **sous-graphe** de G un graphe $G' = (\mathcal{S}', A')$ tel que :

$$\mathcal{S}' \subset \mathcal{S}, A' \subset A \text{ et } \forall \{s_1, s_2\} \in A \Rightarrow \{s_1, s_2\} \in A'$$
 Toutes les arrêtes A entre les sommets de \mathcal{S}' ne sont pas conservées.
- On appelle **sous-graphe induit** de G le sous-graphe $G' = (\mathcal{S}', A')$ tel que :

$$\mathcal{S}' \subset \mathcal{S} \text{ et } \forall s_1, s_2 \in \mathcal{S}', \{s_1, s_2\} \in A \Rightarrow \{s_1, s_2\} \in A'$$
 Ici toutes les arrêtes entre les sommets de \mathcal{S}' sont conservées.

Exemple

Soit le graphe suivant :



DÉFINITION (isomorphisme de graphe)

Soient $G = (\mathcal{S}, A)$ et $G' = (\mathcal{S}', A')$ deux graphes simples.

On dit que les graphes G et G' sont **isomorphes** s'il existe une bijection $\phi : \mathcal{S} \rightarrow \mathcal{S}'$ telle que :

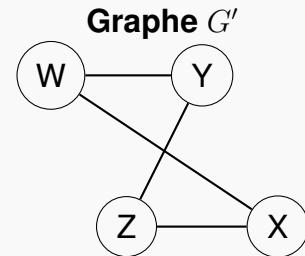
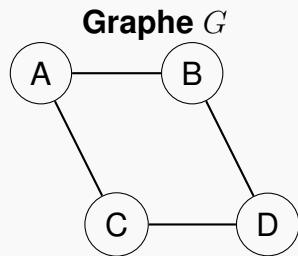
$$\forall s_1, s_2 \in \mathcal{S}, \quad \{s_1, s_2\} \in A \Leftrightarrow \{\phi(s_1), \phi(s_2)\} \in A'$$

Remarque

- En pratique, G' est un graphe dans lequel les sommets de A sont relabelisés par une application bijective.
- Les sommets sont éventuellement positionnés différemment sur le plan.

Exemple (1)

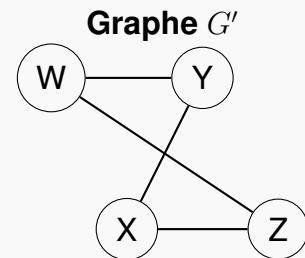
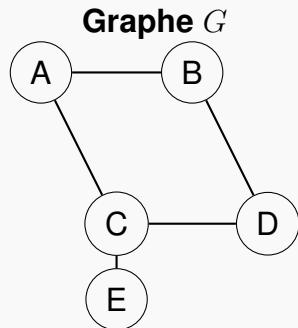
On considère les graphes suivants.



Dans notre cas, les deux graphes ci-dessus sont considérés comme différemment étiquetés. Mais structurellement ce sont les mêmes graphes. Si dans le graphe G' , on change la place de X et Z , on obtient G .

Exemple (2)

On considère les graphes suivants.



Dans notre cas, les deux graphes ci-dessus ne sont pas isomorphes.

Le graphe G contient un sommet supplémentaire E , tandis que le graphe G' ne contient que quatre sommets.

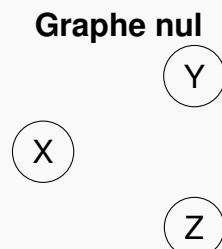
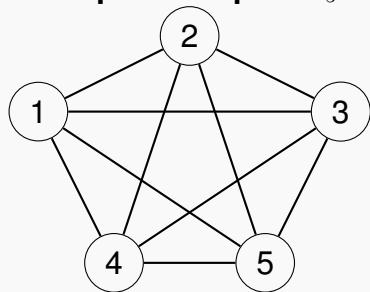
La structure des connexions diffère également, rendant les graphes non équivalents.

2.2) Graphes particuliers

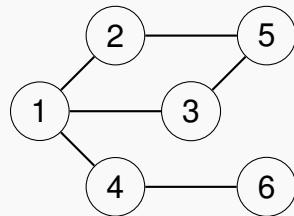
DÉFINITION (vocabulaire supplémentaire)

- Un graphe est dit **nul** lorsqu'il ne possède aucune arête.
- Un graphe est dit **complet** lorsqu'il existe une arête entre chaque paires de sommets. On note K_n le graphe complet à n sommets.
- On appelle **chaîne** une suite finie de sommets $(s_0, s_1, \dots, s_{k-1}, s_k)$ telle que $\forall i \in [1, k-1]$ les sommets s_i et s_{i+1} sont adjacents.
- Un **cycle** est un chemin reliant un sommet à lui-même, on note $s_0 = s_k$.

Remarque || k est la longueur de la chaîne, du cycle.

Exemple**Graphe Complet K_5** **Exemple**

Une chaîne puis un cycle

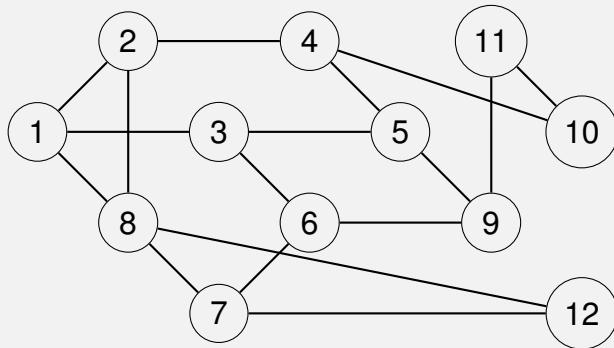


- 5 – 2 – 1 – 4 – 6 est une chaîne simple de longueur 5
- 1 – 3 – 5 – 2 est un cycle de longueur 4

Exercice

On considère le graphe suivant.

Déterminer si il existe des cycles, des chaînes du graphe.

**DÉFINITION** (*chaîne simple, élémentaire*)

Soit $G = (S, A)$ un graphe.

- Une **chaîne simple** est une chaîne sans répétition d'arête.
- Une **chaîne élémentaire** est une chaîne sans répétition de sommet.
- Un **cycle simple** est un cycle sans répétition d'arête.
- Un **cycle élémentaire** est un cycle sans répétition de sommet.

Remarque || Une chaîne élémentaire est forcément une chaîne simple (resp. pour les cycles).

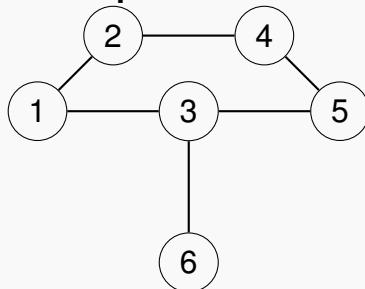
DÉFINITION (*Graphe connexe*)

On dit qu'un graphe G est **connexe** si il existe un chemin entre toute paire de sommets.

Exemple

On considère les graphes suivants.

Graphe Connexe



Graphe Non Connexe



- Le graphe de droite n'est pas connexe car il n'existe pas de chemin entre les arêtes 3 – 4.

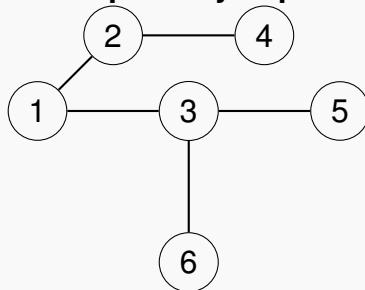
DÉFINITION (*Graphe acyclique*)

Un graphe G est dit **acyclique** si il ne possède aucun cycle.

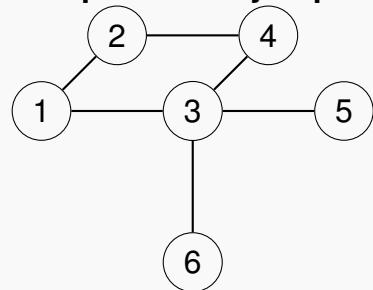
Exemple

On considère les graphes suivants.

Graphe Acyclique



Graphe non acyclique



- Le graphe de gauche est acyclique car il ne contient pas de cycles, ce qui en fait un arbre.
- Le graphe de droite contient un cycle entre les sommets 1, 3, 4, et 2.

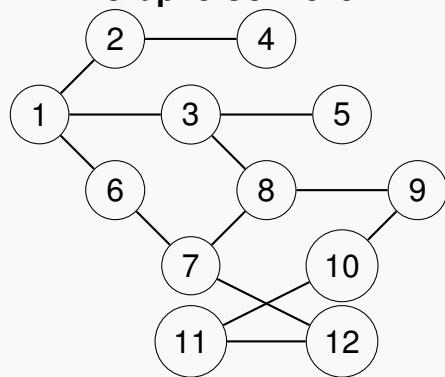
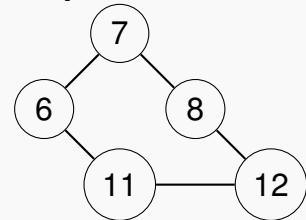
DÉFINITION (*composante connexe*)

Soit G un graphe simple.

Tout sous-graphe G' connexe et maximal de G est une **composante connexe** de G .

Exemple

On considère les graphes suivants.

Graphe Connexe**Composante Connexe**

- Le graphe de gauche est connexe car tous les sommets sont reliés entre eux par des chemins.
- La composante connexe à droite est un sous-graphe de celui de gauche qui est également connecté. Elle contient les sommets 6, 7, 8, 11, et 12.

2.3) Parcours de graphe

Soit $G = (\mathcal{S}, A)$ un graphe.

On part d'un sommet initial $s \in \mathcal{S}$, on souhaite visiter l'ensemble des sommets.

On définit une marque de visite $marqued_i \in \{\text{vrai}, \text{faux}\}$, $\forall i \in \mathcal{S}$.

On va utiliser une structure de donnée (SDD) pour stocker les sommets à visiter.

La complexité de cet algorithme est généralement $o(n + m)$

Cet algorithme permet de tester la connexité du graphe et les composantes connexes.

```

1  procédure parcours(G, s)
2      mettre marked_i ← faux, pour tout i dans S
3      poser SDD ← {s} et marked_s ← vrai
4      tant que SDD n'est pas vide
5          prendre i ← SDD.extraire()
6          afficher i
7          pour tout les voisins j de i dans le graphe G
8              si marked_j = faux
9                  SDD.inserer(j)
10                 marked_j ← vrai

```

Remarque

Le parcours dépend du type de la structure de donnée :

- File parcours en largeur
- Pile parcours en profondeur

2.4) Retour sur les graphes particuliers

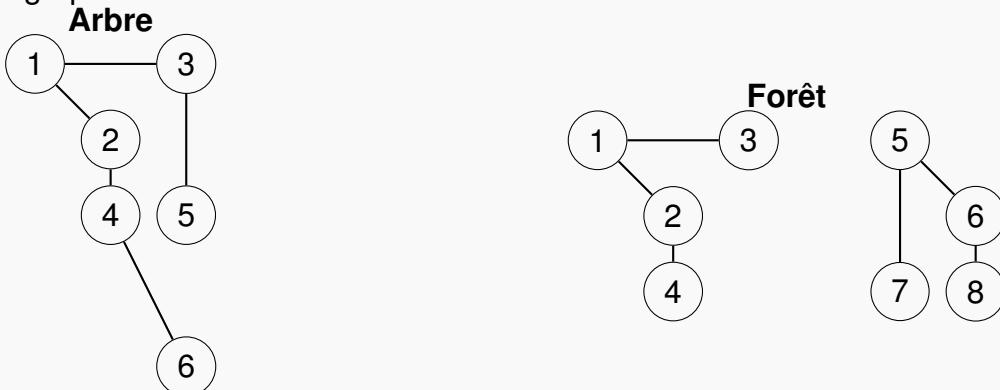
2.4.1) Arbre et forêts

DÉFINITION (arbre, forêt)

- Un **Arbre** est un graphe connexe sans cycle.
- Une **forêt** est un graphe acyclique.

Exemple

On considère les graphes suivants.



- Le graphe de gauche est un arbre car il est acyclique et connecté.
- Le graphe de droite est une forêt, car il contient plusieurs arbres (ici, deux arbres) et est acyclique.

DÉFINITION (vocabulaire supplémentaire)

- Les sommets d'un arbre sont des **noeuds**.
- Les arêtes d'un arbre sont des **branches**.
- Les noeuds de degré 1 sont des **feuilles**.

Proposition

Soit $T = (N, B)$ un arbre avec $|N| \geq 2$ (au moins 2 noeuds).

Alors T vérifie les propositions suivantes :

- Pour toute paire s_1, s_2 de noeuds avec $s_1 \neq s_2 \in N$, il existe un unique chemin entre s_1 et s_2
- Si on enlève une branche à T , on obtient deux composantes connexes qui sont des arbres
- Si on ajoute une branche à T , alors on crée un cycle
- On a $|B| = |N| - 1$

Proposition

Soit $G = (S, A)$ un graphe, c'est un arbre si il vérifie les propriétés suivantes :

- G est connexe
- G est acyclique
- $|A| = |S| - 1$

2.4.2) Graphe bipartis

DÉFINITION (graphe biparti)

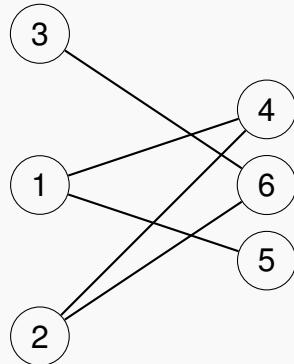
Soit $G = (\mathcal{S}, A)$ un graphe, on dit que G est **biparti** si il existe une bipartition $(\mathcal{S}_1, \mathcal{S}_2)$ de \mathcal{S} telle que :

$$A = \{\{i, j\} \mid i \in \mathcal{S}_1, j \in \mathcal{S}_2\}$$

On note le graphe biparti $G = (\mathcal{S}_1, \mathcal{S}_2, A)$

Exemple

On considère le graphe biparti suivant.



- Le graphe ci-dessus est biparti car il peut être divisé en deux ensembles :
 - Ensemble $U = \{1, 2, 3\}$
 - Ensemble $V = \{4, 5, 6\}$
- Les arêtes relient uniquement les sommets de U aux sommets de V , et il n'y a aucune arête entre les sommets de U ou entre les sommets de V .

Remarque || On note $K_{i,j}$ le graphe biparti complet tel que $|\mathcal{S}_1| = i$ et $|\mathcal{S}_2| = j$

Proposition

Un graphe est biparti si il ne contient aucun cycle simple de longueur impaire.

Remarque || **conclusion de la proposition**

Les arbres et les graphes de cycle de longueur paire sont donc bipartis.

2.4.3) Graphe planaire

DÉFINITION (graphe planaire)

Un graphe G est dit **planaire** si il est isomorphe à un graphe tracé sur un plan sans que ses arêtes se croisent en dehors des sommets.

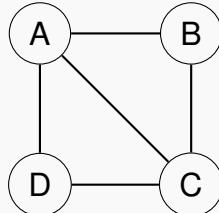
Autrement dit,

Un graphe G est appelé planaire s'il peut être dessiné sur un plan de manière à ce que ses arêtes ne se croisent pas, sauf aux sommets.

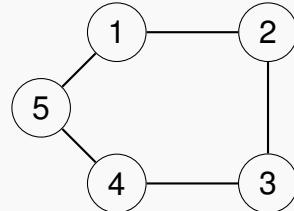
Exemple

On considère les graphes planaires suivants.

Graphe Planaire A



Graphe Planaire B (Cycle à 5 sommets)



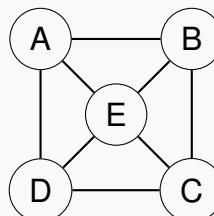
DÉFINITION (vocabulaire)

Soit G un graphe planaire.

- Toute représentation dans \mathbb{R}^2 de G sans croisement d'arêtes en dehors des sommets est appelée **représentation planaire** de G .
- Soit une représentation planaire de G . On appelle **régiion planaire** ou **face** de G toute partie maximale F de \mathbb{R}^2 possédant la propriété suivante :
 - Pour tous points $p_1, p_2 \in F$, il est possible de tracer une courbe entre p_1 et p_2 sans traverser une arête de G .
- La face non bornée du plan est appellée **face externe** ou **infinie**.
- Toute arête de G telle que tout segment qui la traverse contient ces points dans au moins deux faces différentes de G est appelé **face frontière**.

Exemple de Graphe Planar

On considère le graphe suivant représenté dans le plan sans croisement d'arêtes en dehors des sommets. Cela en fait une représentation planaire de ce graphe.



- **Représentation Planaire de G** : Ici, le graphe est dessiné dans le plan sans croisement d'arêtes en dehors des sommets, ce qui constitue une *représentation planaire* de G .

- **Régions Planaire ou Faces** : Dans cette représentation, on observe quatre régions planaires :
 - Trois faces internes : les triangles ABE , BCE , et CDE .
 - Une face externe : la région entourant entièrement le graphe, appelée *face infinie*.
- **Face Externe** : La face qui s'étend à l'infini autour du graphe est appelée la *face externe ou infinie*.
- **Arêtes Frontières** : Une *arête frontière* est une arête qui sépare deux faces. Dans ce graphe, les arêtes AB , BC , CD , et DA sont des arêtes frontières car elles séparent la face externe des différentes faces internes.

Proposition

Soit $G = (\mathcal{S}, A)$ un graphe planaire connexe avec n sommets, m arêtes et f faces. Alors toute représentation planaire vérifie la **relation d'Euler** :

$$f = m - n + 2$$

Condition des propositions

Remarque

- K_5 est le graphe complet à 5 sommets, est non planaire.
- $K_{3,3}$ est le graphe bipartis complet, est non planaire.

Remarque

|| Preuve du théorème d'Euler, vue en TD.

Proposition

Soit $G = (\mathcal{S}, A)$ un graphe simple, planaire et connexe avec $n \geq 3$ sommets, m arêtes et f faces. Alors :

$$m \leq 3n - 6$$

Preuve

Soit f_i le nombre de face de longueur i .

On remarque que $\sum_i i \times f(i) = 2m$ et $\sum_i f_i = f$

Comme G est simple, $n \geq 3$ et $f_1 = f_2 = 0$

Alors :

$$2 = \sum_i i \times f(i) \geq \sum_i 3f_i = 3\sum_i f_i = 3f$$

d'où $f = \frac{2}{3}m$

Puisque G est planaire et connexe. Il vérifie donc la formule d'Euler : $f = m - n + 2$
donc $m - n + 2 \leq \frac{2}{3}m \Leftrightarrow m \leq 3n + 6$

2.4.4) Arbres couvrants

DÉFINITION (arbre couvrant)

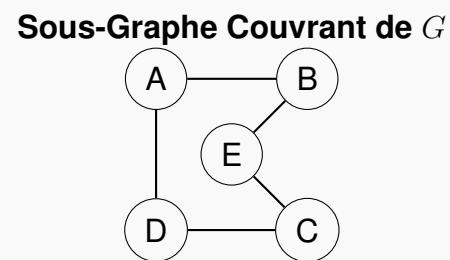
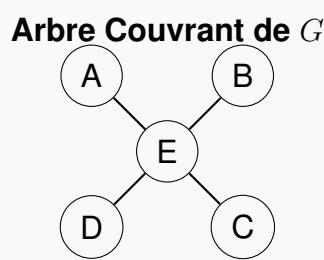
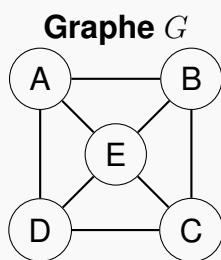
Soit $G = (\mathcal{S}, A)$ un graphe simple.

- Un **arbre couvrant** de G est un sous-graphe couvrant de T de G qui est un arbre.
- Un **sous-graphe couvrant** de G est un sous-graphe $G' = (\mathcal{S}', A')$ telle que $\mathcal{S} = \mathcal{S}'$

Exemple de Graphe, Arbre Couvrant, et Sous-Graphe Couvrant

On considère le graphe G suivant.

Un arbre couvrant de ce graphe est un sous-graphe qui relie tous les sommets sans former de cycles. Un sous-graphe couvrant est un sous-graphe qui inclut tous les sommets mais peut contenir des cycles.



- **Arbre Couvrant** : L'arbre couvrant de G est un sous-graphe qui relie tous les sommets de G sans former de cycles. Ici, l'arbre couvrant est constitué des arêtes AE, BE, CE , et DE , reliant tous les sommets via le sommet E sans boucle.
- **Sous-Graphe Couvrant** : Le sous-graphe couvrant inclut tous les sommets de G mais conserve des cycles. Dans cet exemple, le sous-graphe couvrant contient un cycle formé par les sommets A, B, E, C , et D .

2.5) Graphe pondéré

DÉFINITION (graphe pondéré)

Soit $G = (\mathcal{S}, A)$ un graphe simple et $p : A \rightarrow \mathbb{R}$ une application appelée pondération sur les arêtes de G .

- Le couple (G, p) est appelé **graphe pondéré**, il peut aussi être noté $G = (\mathcal{S}, A, p)$
- $p(a)$ est le poid de l'arête $a \in A$.
- Pour tout sous-graphe $G' = (\mathcal{S}', A')$ de G , le réel $p(G') = \sum_{a \in A'} p(a)$ est appelé **poid du graphe** G .
- Un **arbre couvrant de poids minimum** du graphe pondéré (G, p) est un arbre couvrant T^* dont le poids $p(T^*)$ est minimum parmi l'ensemble des poids de tous les arbres couvrants de (G, p) .

Algorithme de Prim

```

1 Input : Graphe pondéré (G, p)
2 Output : Un arbre couvrant T = (N, B) de poids minimum
3
4 Prim(G)
5     Choisir un sommet s dans S
6     poser N ← {s} et B ← ∅
7     tant que les sommets ne sont pas couverts pas T
8         Choisir a = {i, j} dans A et i dans N, j pas dans N et p(a) minimal
9         si a existe
10            faire N ← N ∪ {j} et B ← B ∪ {a}
11         sinon
12             retourner vide
13         retourner T = (N, B)

```

Complément

- La complexité de la version naïve est $O(nm)$
- La complexité dépend de la File en priorité
 - Liste, tableau : $O(n^2)$
 - Tas minimum : $O(m \log(n))$
 - Tas de fibonacci : $O(m + n \log(n))$

Remarque

Il y a aussi l'algorithme de Kruskal, qui ne sera pas ajouté à ce cours.

Soit $G = (S, A, p)$ un graphe pondéré, il peut exister plusieurs arbres couvrant $T = (N, B)$ de poids minimal.

Comment identifier les arbres couvrants

Remarque

- Soit $a \notin B$ une arête de poids $p(a)$ hors de l'arbre
- Son ajout dans B induit un cycle γ
- Pour toute arêtes $a \in \gamma$, le poids $p(a') \geq p(a)$
- Si il existe une arête arêtes $a' \in \gamma$ de poids $p(a') = p(a)$, alors $T' = (N, B \cup \{a\} \setminus \{a'\})$ est un autre arbre couvrant de poids minimal.

2.6) Coloration de graphe

DÉFINITION (coloration, k -coloration, nombre chromatique)

- On appelle **coloration** d'un graphe $G = (S, A)$ la donnée d'une application $c : S \rightarrow \mathbb{N}$ telle que $\forall \{i, j\} \in A, c(i) \neq c(j)$.
En gros l'action de colorer un graphe c'est le fait d'associer un entier (qui sera la couleur) à chaque sommet tel que deux sommets adjacents n'ont pas la même couleur.
- Un graphe $G = (S, A)$ est dit **k -colorable** si il existe une coloration $c : S \rightarrow \{1 \dots k\}$ valide.
- On appelle **nombre chromatique** noté $\chi(G)$ le plus petit entier k tel que G est colorable.
Ducoup c'est le nombre de couleur minimale valide pour colorer un graphe.
- Une **clique** représente un ensemble de sommets ayant chacun une couleur différente.
- Un **stable** est un ensemble de sommets ayant la même couleur.

Remarque

- Soit K_n un graphe complet, alors $\chi(K_n) = n$
- Pour les cycles pairs $\chi(G) = 2$
- Pour les cycles impairs $\chi(G) = 3$
- Arbres et graphe bipartis $\chi(G) = 2$

2.6.1) L'Heuristique de Welsh et Powell

L'algorithme de Welsh et Powell permet de résoudre les problèmes de coloration de graphe. Ceci consiste à attribuer une couleur à chaque sommet d'un graphe de manière à ce que deux sommets adjacents (reliés par une arête) n'aient pas la même couleur. L'objectif est de minimiser le nombre total de couleurs utilisées.

1. Les sommets sont trié par ordre de degré décroissant
2. Si deux sommets ont le même degré, leur ordre est quelconque
3. Le premier sommet de la liste prend une couleur
4. Pour chaque sommet restant :
 - Attribuer la plus petite couleur disponible si les sommets adjacents ne l'utilisent pas.
 - Sinon donner une nouvelle couleur
5. On retourne le nombre de couleurs utilisées.

CHAPITRE 3

ALGÈBRE DE BOOLE

3.1) Bases et généralités

L'**algèbre de Boole** est une branche des mathématiques proposée par *Georges Boole* en 1854 qui traite des variables logiques et des opérations logiques. Elle constitue la base des circuits numériques et de la logique informatique.

N'empêche c'est déjà pas mal vieux quand même

DÉFINITION (*Algèbre de Boole*)

Un **Algèbre de Boole** est un ensemble B muni de lois de compositions internes + l'addition et · la multiplication et d'une application $\bar{}$: $B \rightarrow B$ appelée "complémentation".
L'ensemble B contient au moins deux éléments notés 1 et 0.
Ainsi on note la structure d'un algèbre de Boole

$$(B, +, \cdot, \bar{})$$

B possède une structure d'Algèbre de Boole si :

- Les lois + et · sont :
 - ⇒ **Associatives**
 $\forall a, b, c \in B$ on a $a + (b + c) = (a + b) + c$ et $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
 - ⇒ **Commutatives**
 $\forall a, b \in B$ on a $a + b = b + a$ et $a \cdot b = b \cdot a$
- 1 est l'élément neutre pour ·
- 0 est l'élément neutre pour +
- et + sont distributives l'une par rapport à l'autre
$$a \cdot (b + c) = a \cdot b + a \cdot c \quad a + (b \cdot c) = a \cdot b + a \cdot c$$
- Chaque $a \in B$ possède un complémentaire \bar{a} tel que :

$$a + \bar{a} = 1 \quad a \cdot \bar{a} = 0$$

Remarque

Rappel de cours

(1) Éléments de base

L'ensemble $B = \{0, 1\}$ dans le cas où l'Algèbre de Boole possède deux éléments. Les éléments de B représentent respectivement les valeurs *faux* et *vrai*.

Notation ensembliste

- $a + b \iff a \vee b$ le OU
- $a \cdot b \iff a \wedge b$ le ET

$a + b$	b	
	0	1
a	0	0
	1	1

$a \cdot b$	b	
	0	1
a	0	0
	1	1

(2) Loi d'identité

- $a + 0 = a$
- $a \cdot 1 = a$

(3) L'application \neg est le NOT

Proposition

Soit $(B, +, \cdot, \neg)$ une algèbre de Boole.

Alors $\forall a \in B, \exists a' \in B$ tel que $a + a' = 1$ et $a \cdot a' = 0$. Si a' vérifie ces conditions alors a' est le **complémentaire de a** que l'on noté généralement \bar{a} .

D'ailleurs $\bar{0} = 1$ et $\bar{1} = 0$.

Et $\forall a \in B$ on a $\bar{\bar{a}} = a$.

Remarque || D'après la définition d'une algèbre de Boole, les deux Ici et les éléments neutres, jouent un rôle symétrique.

Proposition, à retenir absolument

Soit $(B, +, \cdot, \neg)$ une algèbre de Boole et $a, b, c \in B$.

Les propriétés suivantes sont vérifiées :

- **Indempotence** $a + a = a$ et $a \cdot a = a$
- **Élément absorbant** $1 + a = 1$ et $0 \cdot a = 0$
- **Absorption** $a \cdot (a + b) = a$ et $a + (a \cdot b) = a$
- **Redondance** $a \cdot b + \bar{a} \cdot c = a \cdot b + \bar{a} \cdot c + b \cdot c$
- **Loi de Morgan** $\bar{a + b} = \bar{a} \cdot \bar{b}$ et $\bar{a \cdot b} = \bar{a} + \bar{b}$

Preuves

Nous utiliserons donc les **notation ensembliste** :

$$\bullet + \iff \cup$$

$$\bullet \cdot \iff \cap$$

- $a + a = a$

Par définition de l'algèbre de Boole, $+$ signifie l'union. Ainsi l'union d'un élément avec lui-même donne lui-même.

D'où $a + a = a$

- $a \cdot a = a$ Par définition de l'algèbre de Boole, \cdot signifie l'intersection. Ainsi l'intersection d'un élément avec lui-même donne lui-même.

D'où $a \cdot a = a$

1 + a = 1

Dans l'algèbre de Boole, 1 est considéré comme élément absorbant dans l'union.

Ainsi, peu importe a , 1 reste absorbant avec l'union, d'où $1 + a = 1$.

 0 · a = 0

0 est l'élément absorbant pour l'intersection.

Peu importe a , l'intersection avec 0 donne toujours 0, donc $0 \cdot a = 0$.

 $a \cdot (a + b) = a$

Par distributivité, on a : $a \cdot (a + b) = a \cdot a + a \cdot b$.

Par idempotence, $a \cdot a = a$, donc $a + a \cdot b$.

Par absorption, $a + a \cdot b = a$, car a "absorbe" $a \cdot b$.

 $a + (a \cdot b) = a$

On a démontré ci-dessus que cette propriété découle de la loi d'absorption.

 $a + \bar{a} \cdot b = a + b$

Par distributivité, $a + \bar{a} \cdot b = (a + \bar{a}) \cdot (a + b)$.

Par la loi du complément, $a + \bar{a} = 1$.

Donc, $1 \cdot (a + b) = a + b$.

 $a \cdot \bar{a} + b = a \cdot b$

Par la loi du complément, $a \cdot \bar{a} = 0$.

Donc, $a \cdot \bar{a} + b = 0 + b = b$.

Ainsi, l'expression se réduit à $a \cdot b$.

3.2) Atomes

Théorème, relation d'ordre

Soit $(B, +, \cdot, \bar{\cdot})$ une algèbre de Boole. La relation \leq définie sur B par :

$$\forall a, b \in B \quad a \leq b \iff a \cdot b = a$$

est une relation d'ordre sur B compatible avec ses deux lois. En plus, cette relation est stable avec les opérations $+$ et \cdot .

$$\forall a, b, c \in B \mid a \leq b \quad c \cdot a \leq c \cdot b \text{ et } c + a \leq c + b$$

Autrement dit

On dit que $a \leq b$ si et seulement si $a \cdot b = a$. On dira alors que " a est une partie de b ".

Remarque

- Dans une algèbre de Boole, 0 est le minimum, 1 le maximum.
- Si $|B| \geq 2$ alors l'ordre n'est pas total
- La relation d'ordre est aussi définie par $a \leq b \iff a + b = b$
- L'inégalité suivante est vérifiée :

$$\forall a, b \in B \quad a \cdot b \leq a \text{ et } b \leq a + b$$

DÉFINITION (atome)

Soit $(B, +, \cdot, \bar{\cdot})$ une algèbre de Boole **finie**. Alors $x \in B$ est un **atome** de B si :

 $x \neq 0$ **x possède deux minorants : 0 et lui-même**

Proposition

Soit $(B, +, \cdot, \bar{\cdot})$ une algèbre de Boole finie, et $a \neq 0$ avec $a \in B$. L'ensemble des minorants de a contient au moins un atome de B .

Rappel de cours**Minorant**

Soit E un ensemble ordonné et $m \in E$. On dit alors que m est un **minorant** de E si :

$$m \leq e \quad \forall e \in E$$

En d'autres termes, le minorant est un élément qui est plus petit ou égal à tous les éléments de E selon la relation d'ordre.

Chaque élément de B est décrit par les atomes.

Un atome est un élément minimal non nul de B .

Autrement dit $x \in B$ avec $x \neq 0$ et $\exists y \in B$ avec $y \neq 0$ et $y \neq a$ tel que $y \leq x$.

En gros chaque élément de B peut être décrit comme une somme (= union) logique d'atomes de manière unique.

Exemple

Soit $B = \{0, a, b, a + b, 1\}$ une algèbre de Boole avec 0 le plus petit élément et 1 le plus grand.

Les atomes de B sont a et b car ils sont non-nuls et il n'y a aucun élément entre 0 et a ou entre 0 et b .

Description de chaque éléments :

- $0 = \emptyset$ (aucun atome)
- $a = a$ et $b = b$ décrit par eu même
- $a + b$ c'est l'union des deux atomes
- $1 = a + b$ c'est le plus grand élément qui correspond à l'union de tous les atomes.

Remarque**Théorème description**

Soit $(B, +, \cdot, \bar{\cdot})$ une algèbre de Boole finie contenant p atomes. Alors :

- Soit x et y deux atomes de B différents alors $x \cdot y = 0$
- $\sum p = 1$, la somme de tous les atomes de B donne 1.
- Soit $a \in B$ alors il s'écrit comme une somme d'atomes et \bar{a} s'écrit sous la forme d'une somme des atomes restant.
- $|B| = 2^p$, le nombre d'éléments de B .

3.3) Théorème de Stone

DÉFINITION (*isomorphisme d'algèbre de Boole*)

Soit $(B, +, \cdot, \bar{})$ et $(\tilde{B}, +, \cdot, \bar{})$ deux algèbres de Boole.

Toute application $f : B \rightarrow \tilde{B}$ est un **isomorphe d'algèbre de Boole** si $\forall a, b \in B :$

- $f(a + b) = f(a) + f(b)$
- $f(a \cdot b) = f(a) \cdot f(b)$
- $f(\bar{a}) = \bar{f(a)}$

Remarque

On a obligatoirement :

- $f(0) = 0$ et $f(1) = 1$
- Si f est un isomorphe d'algèbres de Boole alors f un un isomorphe d'ordre.

Théorème de Stone

Soit $(B, +, \cdot, \bar{})$ une algèbre de Boole finie.

Alors on dit qu'il est isomorphe à l'algèbre de Boole $(P([1, p]), \cup, \cap, \complement)$ où p est le nombre d'atomes de B .

Preuve

Soit $(B, +, \cdot, \bar{})$ une algèbre de Boole.

D'après la caractérisation des éléments de B , $\forall a \in B$, $\exists I_a \subset [1; p]$ unique tel que $a = \sum_{k=1}^p a_k$

Soit f une application définie par :

$$\begin{aligned} f : B &\rightarrow P([1, p]) \\ a &\mapsto I_a \end{aligned}$$

Alors f est bijective et vérifie les propriétés suivantes :

- $f(a + b) = f(a) \cup f(b)$
- $f(a \cdot b) = f(a) \cap f(b)$
- $f(\bar{a}) = \complement_{[1, p]} f(a)$

3.4) Algèbre de Boole engendrée

DÉFINITION (*expression booléenne, littéral, ...*)

Soit $(B, +, \cdot, \bar{\cdot})$ une algèbre de Boole, a_1, \dots, a_n n éléments de B . Alors :

- Tout élément de B obtenu en combinant des éléments de B à l'aide d'un nombre fini d'opération est appelée **expression booléenne** des éléments a_1, \dots, a_n .
- On appelle **littéral** une expression booléenne d'un élément composé uniquement de ce même élément ou de son complément.
- Un **monôme** est un produit d'un ou de plusieurs littéraux.
- Un **monal** est une somme d'un ou de plusieurs littéraux.
- Un **minterme** de n éléments a_1, \dots, a_n est un monôme à n littéraux où chaque littéral en position i est choisi en a_i et \bar{a}_i et présent une seule fois.
- Un **maxterme** de n éléments a_1, \dots, a_n est un monal à n littéraux où chaque littéral en position i est choisi en a_i et \bar{a}_i et présent une seule fois.

Remarque || L'ensemble des expression booléenne constructible à partir des éléments a_1, \dots, a_n est noté $G(a_1, \dots, a_n)$.

DÉFINITION (*algèbre de Boole engendrée*)

Soit $(B, +, \cdot, \bar{\cdot})$ une algèbre de Boole et $A \neq \emptyset$ une partie de B . L'ensemble A est appelée **sous-algèbre de Boole** de B si la restriction des opérations de B aux éléments de A confère à A une structure d'algèbre de Boole :

$$\forall a, b \in B \quad a + b \in A \quad a \cdot b \in A \quad \bar{a} \in A$$

Proposition

Soit $(B, +, \cdot, \bar{\cdot})$ une algèbre de Boole et $a_1, \dots, a_n \in B$ alors l'ensemble des expression booléenne $G = (a_1, \dots, a_n)$ est un sous algèbre de Boole de B .

Il est appelé **algèbre de Boole engendré par les éléments** a_1, \dots, a_n .

Remarque ||

- D'après la **loi de Morgan**, et la **propriété de distributivité**, tout élément de $G = (a_1, \dots, a_n)$ peut s'exprimer comme une somme de monômes.
- Tout atôme de $G = (a_1, \dots, a_n)$ est un monôme.

Théorème

Soit $(B, +, \cdot, \bar{\cdot})$ une algèbre de Boole et soient $a_1, \dots, a_n \in B$. Les atomes de $G = (a_1, \dots, a_n)$ sont les mintermes **non nuls** des éléments a_1, \dots, a_n .

Caractérisation

Soit $(B, +, \cdot, \bar{\cdot})$ une algèbre de Boole et a_1, \dots, a_n n éléments de B . Soit $a \in G(a_1, \dots, a_n)$.

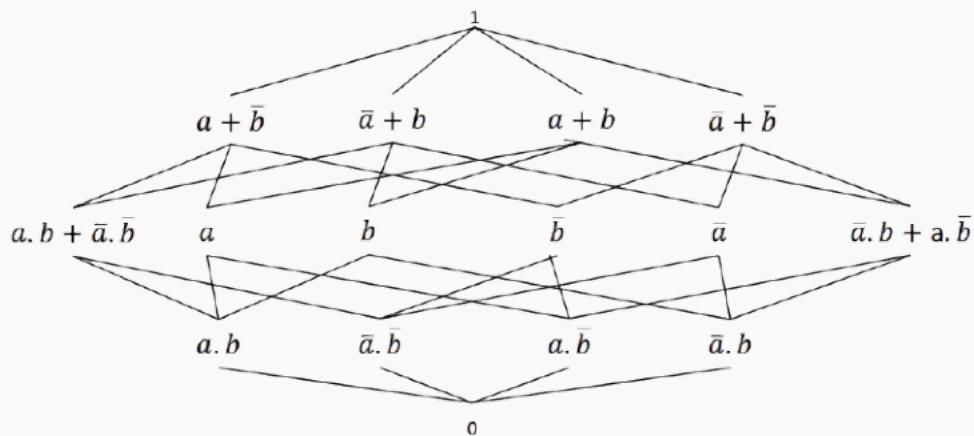
Alors :

- ⇒ Le produit de deux mintermes est nul.
- ⇒ La somme de tous les mintermes est 1.
- ⇒ La somme de deux maxtermes distincts est 1.

- ⇒ Le produit de tous les maxtermes est 0.
- ⇒ $\forall a \in G(a_1, \dots, a_n)$ peut s'écrire sous la forme d'une somme de mintermes distincts non nuls.
- ⇒ $\forall a \in G(a_1, \dots, a_n)$ peut s'écrire sous la forme d'un produit de mintermes distincts différents de 1.
- ⇒ Lorsqu'un élément $a \in G(a_1, \dots, a_n)$ est écrit sous la forme de somme de mintermes distincts, alors son complément noté \bar{a} est quant à lui écrit avec la somme des mintermes restant.
- ⇒ Lorsqu'un élément $a \in G(a_1, \dots, a_n)$ est écrit sous la forme de produits de maxtermes distincts son complément noté \bar{a} est quant à lui écrit avec le produit des maxtermes restant.
- ⇒ Le nombre d'éléments de $G(a_1, \dots, a_n)$ est 2^p où p peut être :
 - Le nombre de mintermes non nul de $G(a_1, \dots, a_n)$
 - Le nombre de maxtermes différents de 1 de $G(a_1, \dots, a_n)$

Exemple

Soit $(B, +, \cdot, \bar{})$ une algèbre de Boole et $a, b \in B$ si les mintermes de a et de b sont non nuls alors le diagramme de Hasse de $G(a, b)$ est donné par :



DÉFINITION (décomposition canonique)

Soient a_1, \dots, a_n, n éléments d'une algèbre de Boole B et $a \in G(a_1, \dots, a_n)$. Alors

- La somme des mintermes distincts et non nuls de a_1, \dots, a_n servant à décrire a est appelée **décomposition canonique disjonctive** de l'élément a .
- Le produit des maxtermes distincts et non nuls de a_1, \dots, a_n servant à décrire a est appelé **décomposition canonique conjonctive** de l'élément a .

CHAPITRE 4

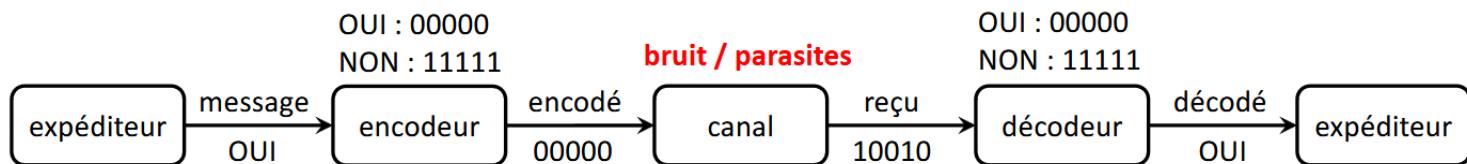
THÉORIE DES CODES

4.1) Le codage de l'information

DÉFINITION (*codage de l'information*)

Le **codage de l'information** désigne l'étude de la façon de coder un message afin de le transmettre d'un expéditeur vers un destinataire via un dispositif de transmission.

Schéma de M.Duhamel



Explications :

L'image illustre un processus de communication numérique avec un système de codage et de décodage destiné à gérer les erreurs causées par le bruit ou les parasites dans un canal de transmission. Voici une explication détaillée des différentes étapes :

- **L'expéditeur** c'est l'origine du message, la personne qui souhaite communiquer. Dans l'exemple, le message qu'il envoie est une simple réponse "oui" ou "non".
- **Le message** est ensuite envoyé sous forme de texte. Ici "OUI".
- **L'encodeur** convertit le message en code binaire pour être transmis. Dans notre cas, OUI = 00000 et NON = 11111.
- Le codage répétitif permet de détecter et corriger les erreurs si des bits sont "faussés"
- Le message traverse un **canal** de communication où il peut être exposé à des perturbations qui peuvent alterner les bits.
- A la sortie du canal, le mot est 10010.
- Le **décodeur** lui possède le codage de base des mots du code OUI et NON puis le message reçu.
- Dans notre cas il regarde la distance entre le mot reçu et les mots possibles afin de détecter le ou les erreurs puis de les corriger si possible.
- Dans notre exemple le mot est corrigé et le destinataire reçoit bien OUI.

Théorie de l'information développée par Claude Shannon en 1948. Les 4 branches concernées sont codage de l'information, compression de données, Transmission de message et cryptographie.

DÉFINITION (code & cie.)

- Un **Alphabet** est un ensemble A **fini** non vide et ses éléments sont appelés *lettres*.
- Un **mot** de longueur $n \in \mathbb{N}$ est un n -uplet $(x_1, \dots, x_n) \in A^n$ de lettres.
Il se note aussi x_1, \dots, x_n où x_i avec $i \in \mathbb{N}^*$ est le i -ième bit du mot.
- Le **mot vide** noté ϵ est de longueur nulle, $n = 0$.
- L'ensemble de tous les mots est notée $A^* = \bigcup_{k \in \mathbb{N}} A^k$
- Un **code** sur A est une partie $C \subseteq A^*$. Ses éléments sont des mots de code.
- Un **code de longueur n** est un code où tous les mots sont de longueur n .

Remarque || Le **code binaire** repose alors sur l'alphabet $A = \{0, 1\}$.

DÉFINITION (erreur de transmission)

Soit m_{envoye} et m_{recu} deux messages.

On dit qu'une **erreur de transmission** est survenue si le message reçu est différent du message envoyé.

$$m_{envoye} \neq m_{recu}$$

Remarque || Dans le cours de L2, on ne prend en compte que le cas où un bit a été alteré.

Théorème

Soit $n \in \mathbb{N}$ et $p \in [0; 1]$ la **probabilité d'une erreur** de transmission sur 1 bit. Alors la probabilité $\mathbb{P}(k)$ qu'un mot de n bits soit transmit avec $k \in [0; n]$ erreur est donnée par :

$$\mathbb{P}(k) = \binom{n}{k} p^k (1-p)^{n-k}$$

DÉFINITION (distance de Hamming)

Soit $n \in \mathbb{N}$ et A un alphabet. La **distance de Hamming** est l'application :

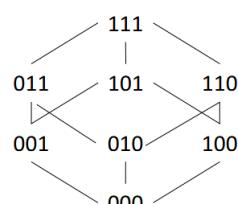
$$\begin{aligned} d : A^n \times A^n &\rightarrow \mathbb{N} \\ (u, v) &\mapsto d(u, v) = \text{card}(\{i \in [1; n] \mid a_i \neq b_i\}) \end{aligned}$$

où $u = (a_1, \dots, a_n)$ et $v = (b_1, \dots, b_n)$ deux mots.

En gros la distance de Hamming représente le nombre de bits différents entre deux mots u et v .

Remarque

Lien avec le Diagramme de Hasse
La distance de Hamming correspond au plus petit chemin entre deux mots dans le diagramme de Hasse.



DÉFINITION (*Distance du code*)

Soit C un code de longueur n . La **distance du code** est donnée par :

$$d(C) = \min\{d(u, b) \mid u, b \in C \wedge u \neq b\}$$

Règle du plus proche voisin

Soit C le code de longueur n et $u \in A^n$ un mot reçu. Le *plus proche voisin* est le mot de code $c \in C$ minimisant la distance $d(u, c)$.

4.2) Code détecteur, code correcteur**DÉFINITION** (*k-détecteur, k-correcteur*)

- Le code C est dit **k-correcteur** si il permet de corriger un mot avec au plus k erreurs, à l'aide de la règle du plus proche voisin **sans se tromper**.
- Le code C est dit **k-détecteur** si il permet de détecter k erreurs sur un mot reçu.

Remarque

- Si le mot reçu est un mot du code alors il n'y a aucune erreur.
- Un mot avec erreur ne peut pas toujours être corrigé si il existe plusieurs mots du code à la même distance minimale. On ne peut donc pas choisir la solution donc corriger le mot.

Théorème

Soit C un code de longueur n et $k \in [1; n]$.

- Le code est dit *k-détecteur* si $k \leq d(C) - 1$
 $d(C) - 1$ est le nombre d'erreurs détectées du code C
- Le code C est dit *k-correcteur* si $k \leq \frac{d(C) - 1}{2}$
 $\left\lfloor \frac{d(C) - 1}{2} \right\rfloor$ est le nombre d'erreurs corrigées du code C

4.3) Différents codages possibles

Pour augmenter la distance d'un code,

- **Codage par répétition** on duplique f -fois chaque bit
- **Codage par ajout de bit de parité**
 On ajoute un bit à la fin du mot en faisant en sorte que le nombre de bits à 1 soit pair.

Remarque || Il existe évidemment de multiples autres codages possibles.

DÉFINITION (n, M, D)

Un (n, M, D) -code est un **code binaire** tel que :

- n est la longueur du code (= longueur des mots du code)
- M le nombre de mots du code
- d la distance du code

Remarque || étant donné n et d , on cherche à maximiser le nombre de mots que l'on peut contruire.

DÉFINITION $(sphère)$

On appelle **sphère** de centre $u \in \{0, 1\}^n$ le rayon $r \in \mathbb{N}$ l'ensemble défini par :

$$S(u, r) = \{v \in \{0, 1\}^n \mid d(u, v) \leq r\}$$

Remarque || Pour toute sphères de rayon r composée de mots dans $\{0, 1\}^n$ contient alors $\sum_{i=0}^r \binom{n}{i}$ mots.

4.4) Représentation du code

Tout code binaire C peut être représenté par une matrice notée C de M lignes et de n colonnes dont chaque ligne représente un mot du code.

DÉFINITION $(code équivalents)$

Deux codes binaires sont dits **équivalents** si l'on peut obtenir l'un de ces codes à partir de l'autre en combinant les opérations suivantes :

- Permutation des positions des lettres dans tous les mots du code
- Permutation des symboles $(0, 1)$ apparaissant dans une position donnée des mots du code

Remarque || Tout (n, M, D) -code binaire est équivalent à un (n, M, D) -code binaire contenant le mot $000\dots 0$.