

# Automates et circuits : Ordres, treillis et algèbre de Boole

Arnaud Labourel  
Courriel : [arnaud.labourel@lif.univ-mrs.fr](mailto:arnaud.labourel@lif.univ-mrs.fr)

Aix-Marseille Université

# Imaginons une hiérarchie

## Hiérarchie et précédence

Soit un ensemble  $E$  : avoir une *hiérarchie* sur  $E$  permet de définir une relation de précédence sur  $E$  :

$a$  est en relation avec  $b$  si  $a$  précède  $b$  dans la hiérarchie

## Exemples

- Les employés d'une société et la relation est-responsable-de
- Les livres et la relation a-autant-ou-plus-de-pages-que
- ... Les entiers naturels et la relation  $\leq$

# Propriétés de la précédence

## Antisymétrique

Si  $a$  et  $b$  sont différents, et si  $a$  précède  $b$ , alors  $b$  ne peut pas précéder  $a$   
(sinon ce n'est plus une hiérarchie...)

## Transitive

Si  $a$  précède  $b$  et si  $b$  précède  $c$  alors  $a$  précède  $c$   
(en principe !)

## Réflexive

Le chef de service est responsable de lui-même, chaque livre a autant de pages que lui-même,  $12 \leq 12$

# Relation d'ordre : définition

## Définition

Une relation *réflexive*, *antisymétrique* et *transitive*, s'appelle une relation d'ordre.

Un ensemble muni d'une relation d'ordre est un *ensemble ordonné*

## Exemples

- Les relations  $\leq$  et  $\geq$  sur  $\mathbb{N}$  sont des relations d'ordre
- Les relations  $<$  et  $>$  sur  $\mathbb{N}$  n'en sont pas
- sur  $\mathbb{N}^*$ , la relation  $a$  divise  $b$ , notée  $a \mid b$  est une relation d'ordre ( $a$  divise  $b$  s'il existe  $k \in \mathbb{N}^*$  tel que  $b = ka$ ). Par exemple,  $3 \mid 24$ .

# Ordre lexicographique

Soit  $\mathbb{B}^*$  les mots binaires, avec l'ordre  $0 < 1$

Soit  $\epsilon$  le mot de longueur nulle

Soit  $m \in \mathbb{B}^*$ ,  $m = m_1 m_2 m_3 \cdots m_p$  et  $w \in \mathbb{B}^*$ ,  $w = w_1 w_2 w_3 \cdots w_q$

## Ordre lexicographique $\preceq$

- $\forall m \in \mathbb{B}^*$ ,  $\epsilon \preceq m$
- $m \preceq w$  si :  $p = q$  et  $\forall i, m_i = w_i$  (011  $\preceq$  011)
- $m \preceq w$  si :  $m_1 = w_1, m_2 = w_2 \cdots m_{s-1} = w_{s-1}$  et  $m_s < w_s$  avec  $1 \leq s \leq p$  et  $s \leq q$  (101  $\preceq$  11)

100100  $\preceq$  100100**1**, 01000111  $\preceq$  **1**100, 01101  $\preceq$  01101, 101  $\preceq$  **1**10  
fa  $\preceq$  fa, poule  $\preceq$  poulet, avion  $\preceq$  train, livraison  $\preceq$  livre, foot  $\preceq$  fort

# Notations et vocabulaire

## Notations conventionnelles

- Relations d'ordre fréquentes :  
 $\leq, \geq, \preceq, \succeq, \sqsubseteq, \sqsupseteq, \subseteq, \supseteq, |$  etc.
- Notation générale :  $\ll$  et  $\gg$

## Vocabulaire conventionnel

Si  $x \ll y$ , on dit que :

$x$  est un minorant de  $y$  ( $x$  minore  $y$ )

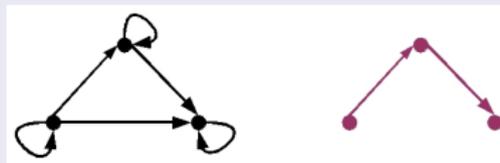
$y$  est un majorant de  $x$  ( $y$  majore  $x$ )

Par exemple, soit  $\geq$ , on a  $5 \geq 2$ , donc 5 minore 2...

# Diagramme de Hasse : intuitivement

## Version simplifiée du diagramme sagittal

Plus de boucles (réflexivité) et plus de flèche déductible par transitivité



## Successesseur immédiat

$y$  est un successeur immédiat de  $x$  si :

- 1  $x \ll y$
- 2  $x \neq y$
- 3 il n'existe pas  $z$  tel que  $x \ll z \ll y$

# Diagramme de Hasse : un exemple

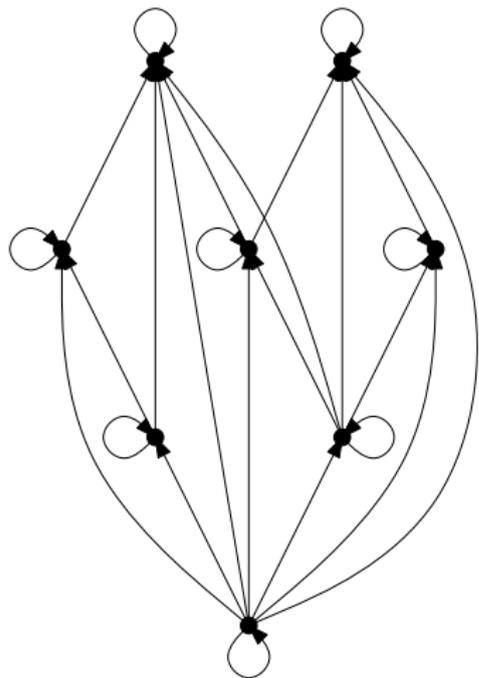


diagramme sagittal

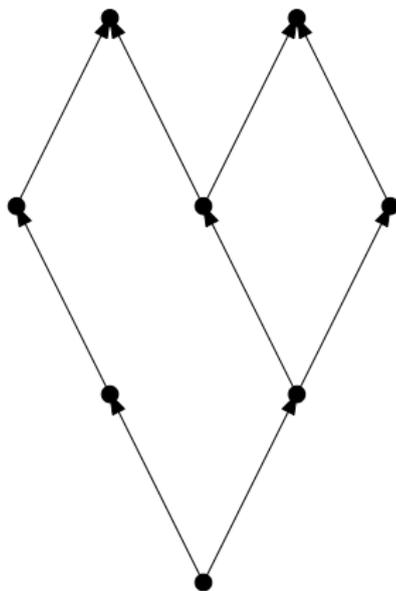


diagramme de Hasse

# Exemples

## Relation d'infériorité large $\preceq$ chez $\mathbb{N}^+$

Chaque élément n'a qu'un seul successeur immédiat, par exemple 3 est le seul successeur immédiat de 2

## Relation de divisibilité $|$

Il existe une infinité de successeurs immédiats de 2

4, 6, 10, 14, 22, 26, 34, 36, etc.

## Ordre lexicographique

Le successeur immédiat de 100 est 1000 (et non pas 101 car  $1000 \preceq 101$ )

# Théorème

## Théorème

L'élément  $x$  minore  $y$  ( $x \ll y$ ) si et seulement si on peut passer du point qui représente  $x$  au point qui représente  $y$  en suivant les flèches du diagramme de Hasse.

## Intérêt

- Comment le diagramme de Hasse permet de visualiser la relation d'ordre.
- Topologie du diagramme

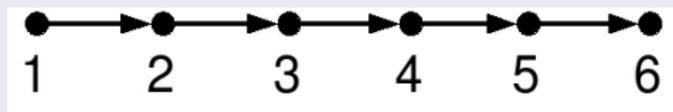
# Ordre total (ou linéaire)

## Définition

Une relation d'ordre  $\ll$  sur  $A$  est un ordre total si et seulement si  $\forall x, y \in A$ , on a  $x \ll y$  ou  $y \ll x$ .  
Autrement dit, tout élément se compare à tout autre.

## Exemple de $\leq$

L'ordre de large infériorité  $\leq$  sur  $\mathbb{N}_6^*$  est un ordre total.



# Ordre total (cont'd)

## Ensemble totalement ordonné

Un ensemble totalement ordonné est un ensemble muni d'une relation d'ordre total

## Diagramme de Hasse d'un ordre total

C'est une *Chaîne* (qui peut-être infinie)

## Ordre partiel

Pour souligner qu'un ordre n'est pas total (par exemple la responsabilité entre employés), on dit qu'il s'agit d'un *ordre partiel* : certains éléments sont incomparables dans un tel ordre

# Élément maximal

## Définition

Un élément  $x$  d'un ensemble ordonné est *maximal* s'il ne possède pas d'autre majorant que lui-même.

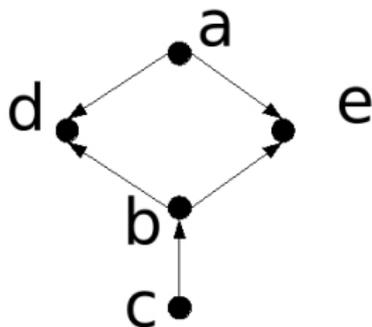
## Sur les diagrammes

- Diagramme de Hasse : un sommet duquel ne part aucune flèche
- Diagramme cartésien : sur sa ligne, aucune autre case noircie que celle de la diagonale (donc sur la matrice, cette ligne n'a qu'une valeur à 1)

# Exemple d'éléments maximaux

Ici,  $d$  et  $e$  sont maximaux

	a	b	c	d	e
a	■			■	■
b		■		■	■
c		■	■	■	■
d				■	
e					■



# Élément minimal

## Définition

Un élément  $x$  d'un ensemble ordonné est *minimal* s'il ne possède pas d'autre minorant que lui-même.

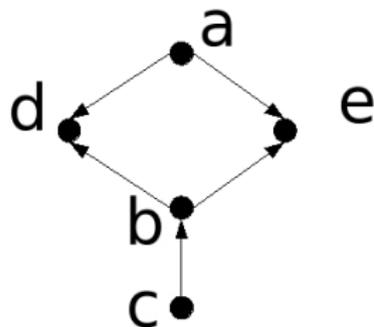
## Sur les diagrammes

- Diagramme de Hasse : un sommet vers lequel n'arrive aucune flèche
- Diagramme cartésien : sur sa colonne, aucune autre case noircie que celle de la diagonale (donc sur la matrice, cette colonne n'a qu'une valeur à 1)

# Exemple d'éléments minimaux

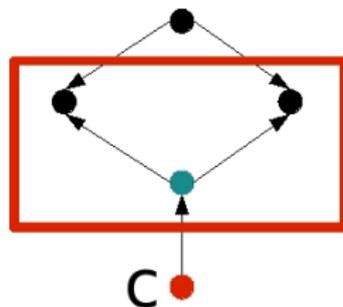
Ici,  $a$  et  $c$  sont minimaux

	a	b	c	d	e
a	■			■	■
b		■		■	■
c		■	■	■	■
d				■	
e					■



# Notes sur les éléments maximaux et minimaux

- Ils existent toujours dans les ensembles ordonnés finis, mais pas toujours chez les infinis (ex :  $\mathbb{Z}$ )
- Les successeurs immédiats d'un élément  $x$  sont les éléments minimaux de l'ensemble formé par les majorants de  $x$  différents de  $x$



# Plus grand élément

## Définition

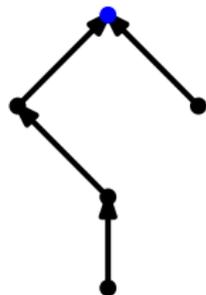
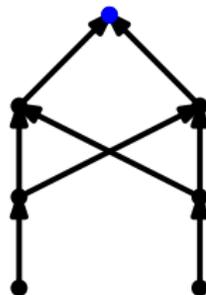
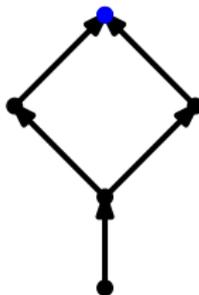
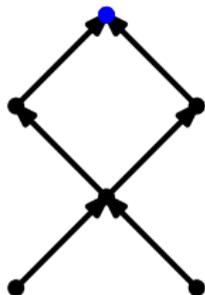
Un élément  $x$  est **le** plus grand élément d'un ensemble ordonné  $A$  s'il majore **tous** les éléments de  $A$ .

## Sur les diagrammes

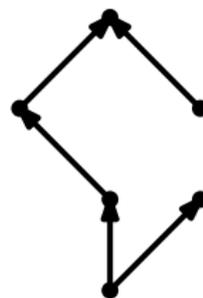
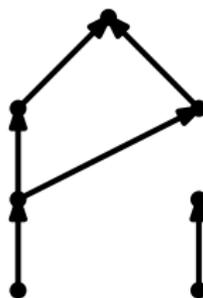
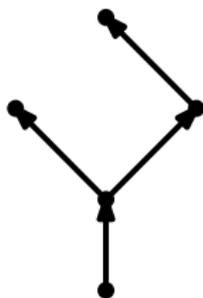
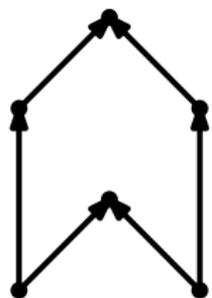
- Diagramme cartésien : la colonne qui lui correspond est complètement noircie
- Diagramme de Hasse : il existe un chemin (en parcourant les flèches) qui va de n'importe quel élément de  $A$  vers le plus grand

# Exemples de plus grands éléments

plus grand élément



# Exemples d'ensemble **sans** plus grands éléments



# Plus petit élément

## Définition

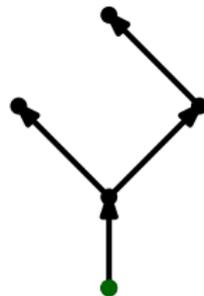
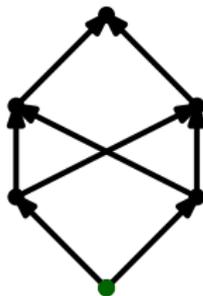
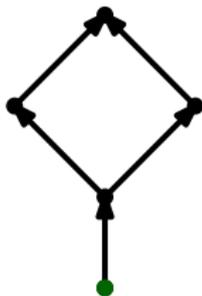
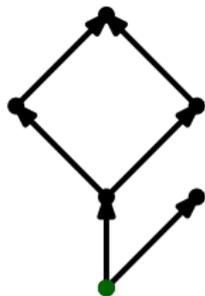
Un élément  $x$  est **le** plus petit élément d'un ensemble ordonné  $A$  s'il minore **tous** les éléments de  $A$ .

## Sur les diagrammes

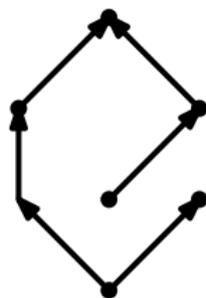
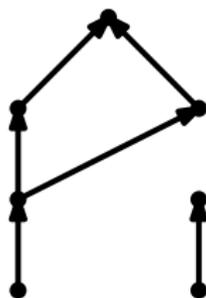
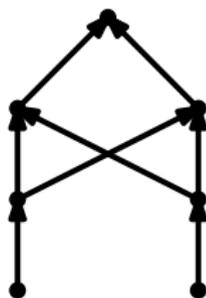
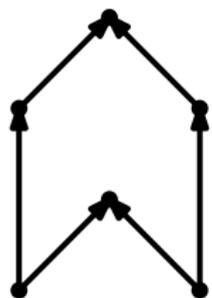
- Diagramme cartésien : la ligne qui lui correspond est complètement noircie
- Diagramme de Hasse : il existe un chemin (en parcourant les flèches) du plus petit élément vers tous les autres éléments de  $A$

# Exemples de plus petits éléments

plus petit élément



# Exemples d'ensemble **sans** plus petits éléments



# Notes sur les plus petits et plus grand éléments

Ils n'existent pas toujours

## Théorème

Soit  $A$  un ensemble ordonné

- 1 Si  $A$  possède un plus grand élément, celui-ci est unique ; c'est un élément maximal de  $A$ , et c'est le seul : on le note  $\sup(A)$
- 2 Si  $A$  possède un plus petit élément, celui-ci est unique ; c'est un élément minimal de  $A$ , et c'est le seul : on le note  $\inf(A)$

# Plus petit, plus grand, maximaux

## Théorème (réciproque du précédent)

Soit  $A$  un ensemble ordonné fini

- 1 Tout élément de  $A$  est majoré par au moins un élément maximal, et minoré par au moins un élément minimal
- 2 Si  $A$  possède un seul élément maximal, c'est  $\sup(A)$
- 3 Si  $A$  possède un seul élément minimal, c'est  $\inf(A)$

# Treillis : introduction

## Motivations

- Propriétés remarquables des treillis
- Représentation des algèbres de Boole en dimension  $n$
- Théorème de Stone
- Structure de données élaborée (treillis de Galois, cubes en fouille de données, etc.)

## Autres appellations

- En anglais : lattice
- En mathématiques : espace réticulé

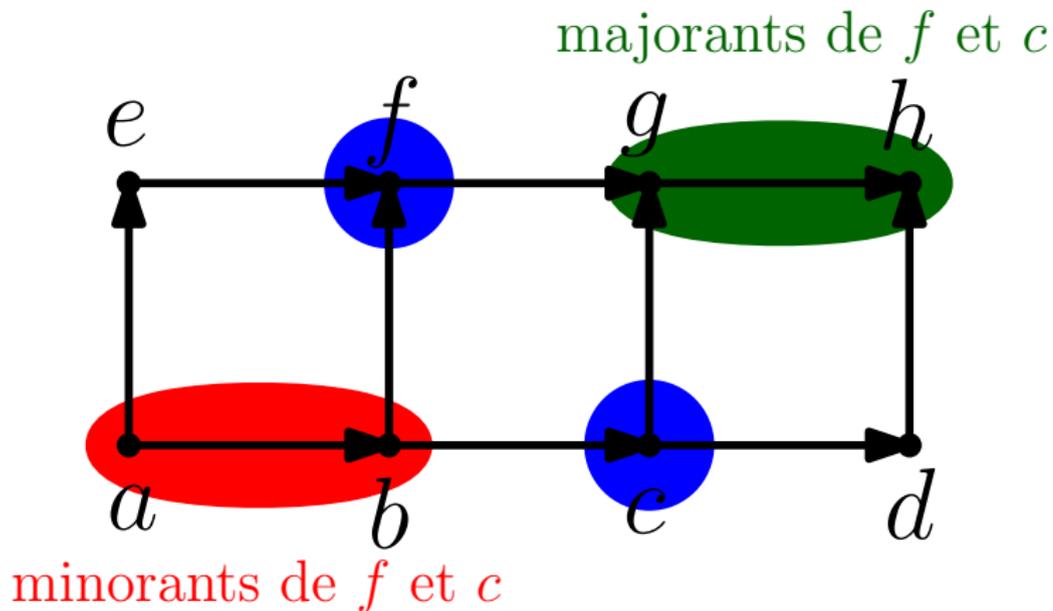
# Treillis : histoires de majorants et de minorants

## Théorème (preuve sur transitivité de l'ordre)

Soit  $A$  un ensemble ordonné,  $x$  et  $y$  deux éléments quelconques de  $A$ .

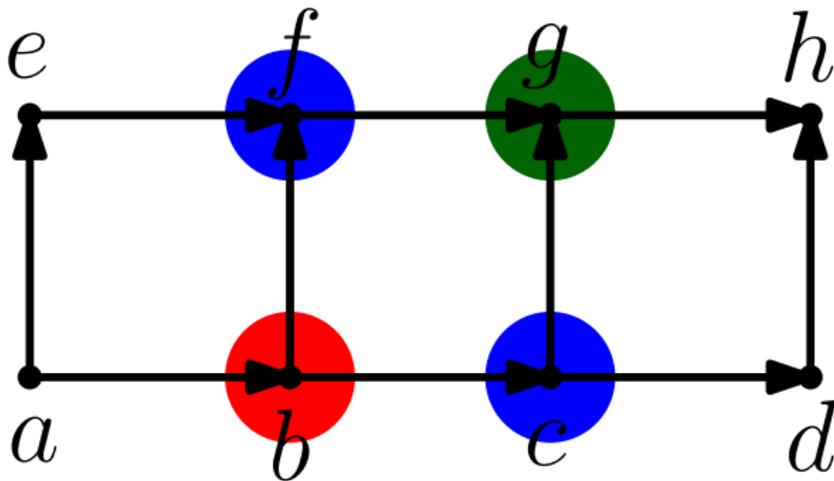
- 1 Si l'ensemble  $M(x, y)$  des majorants communs à  $x$  et  $y$  admet un plus petit élément  $z$ , alors  $M(x, y)$  coïncide avec l'ensemble des majorants de  $z$ .
- 2 Si l'ensemble  $m(x, y)$  des minorants communs à  $x$  et  $y$  admet un plus grand élément  $t$ , alors  $m(x, y)$  coïncide avec l'ensemble des minorants de  $t$ .

# Exemple de treillis



# Exemple de treillis

plus petit majorant  
commun à  $f$  et  $c$



plus grand minorant  
commun à  $f$  et  $c$

# Définitions préalables

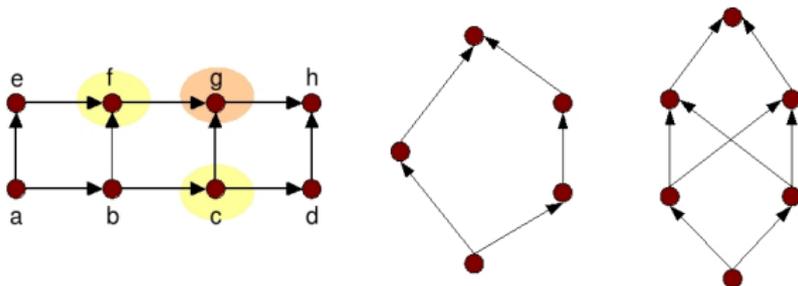
Soit  $A$  un ensemble ordonné, et  $x, y$  des éléments qcq de  $A$ .

## Borne supérieure de $x$ et de $y$

Quand l'ensemble des majorants communs à  $x$  et  $y$  possède un plus petit élément : on le note  $\sup(x, y)$  ou encore  $x \vee y$ .

## Borne inférieure de $x$ et de $y$

Quand l'ensemble des minorants communs à  $x$  et  $y$  possède un plus grand élément : on le note  $\inf(x, y)$  ou encore  $x \wedge y$ .



# Définitions préalables

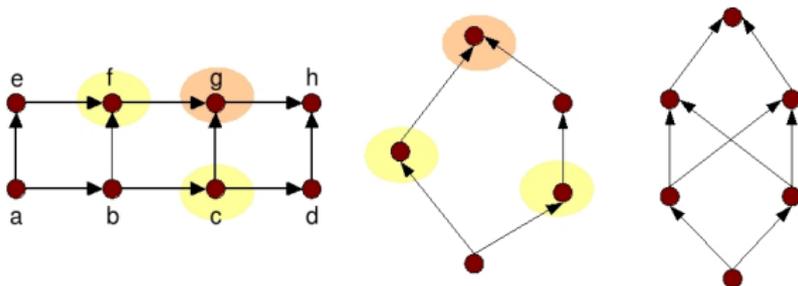
Soit  $A$  un ensemble ordonné, et  $x, y$  des éléments qcq de  $A$ .

## Borne supérieure de $x$ et de $y$

Quand l'ensemble des majorants communs à  $x$  et  $y$  possède un plus petit élément : on le note  $\sup(x, y)$  ou encore  $x \vee y$ .

## Borne inférieure de $x$ et de $y$

Quand l'ensemble des minorants communs à  $x$  et  $y$  possède un plus grand élément : on le note  $\inf(x, y)$  ou encore  $x \wedge y$ .



# Définitions préalables

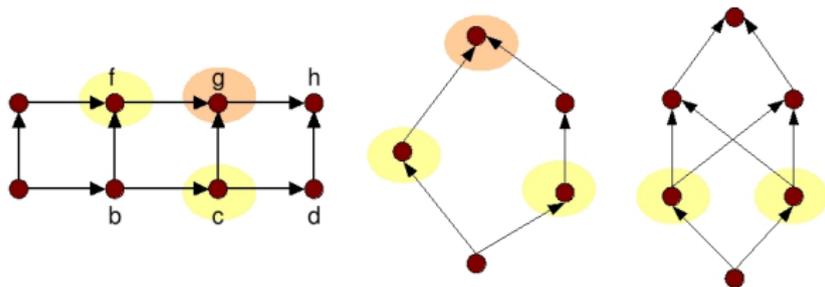
Soit  $A$  un ensemble ordonné, et  $x, y$  des éléments qcq de  $A$ .

## Borne supérieure de $x$ et de $y$

Quand l'ensemble des majorants communs à  $x$  et  $y$  possède un plus petit élément : on le note  $\sup(x, y)$  ou encore  $x \vee y$ .

## Borne inférieure de $x$ et de $y$

Quand l'ensemble des minorants communs à  $x$  et  $y$  possède un plus grand élément : on le note  $\inf(x, y)$  ou encore  $x \wedge y$ .

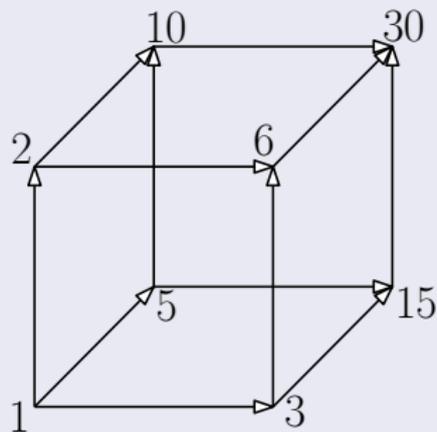


# Qu'est-ce qu'un treillis

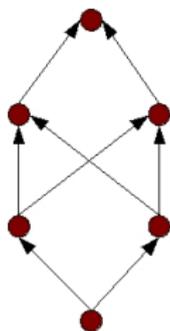
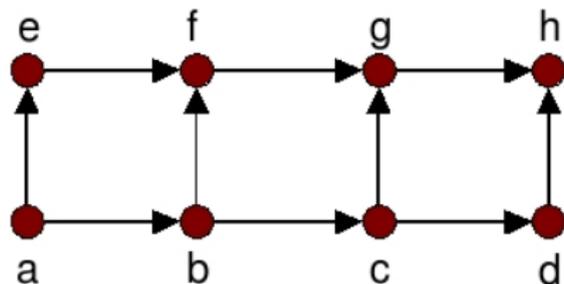
## Définition

On dit qu'un ensemble ordonné  $A$  est un **treillis** si, pour tous  $x$  et  $y$  dans  $A$ , les bornes  $x \vee y$  et  $x \wedge y$  existent.

## Diviseurs entiers positifs de 30



# Exemples de treillis (ou non)



# Quelques résultats

## Théorèmes

- Les ensembles totalement ordonnés sont des treillis
- Dans un treillis, quels que soient  $x$ ,  $y$  et  $z$  :  
 $x \vee y = y \vee x$  et  $x \wedge y = y \wedge x$   
 $x \vee (y \wedge z) = (x \vee y) \wedge z$  et  $x \wedge (y \vee z) = (x \wedge y) \vee z$
- Tout treillis **fini** possède un plus grand et un plus petit éléments.  
 $\sup(A) = x_1 \vee x_2 \vee \cdots \vee x_n$   
 $\inf(A) = x_1 \wedge x_2 \wedge \cdots \wedge x_n$   
Attention : faux dans le cas où  $A$  est infini, par exemple  $\mathbb{Z}$ .

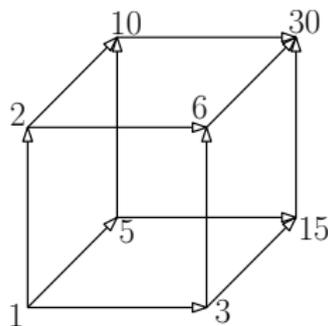
# Treillis distributif

## Définition

On dit qu'un treillis est distributif si l'on a, pour tous  $x, y$  et  $z$  :

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$



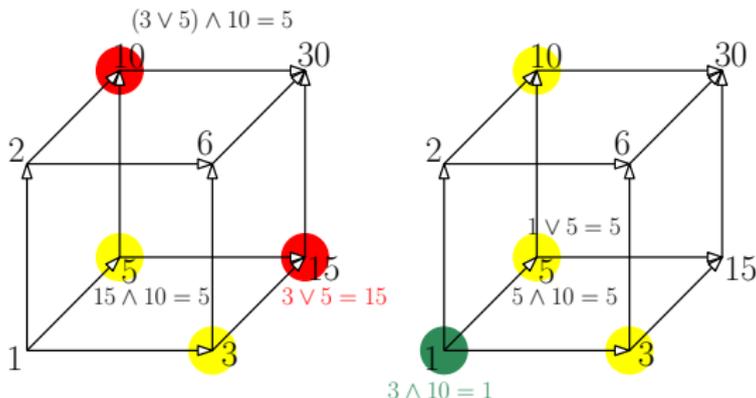
# Treillis distributif

## Définition

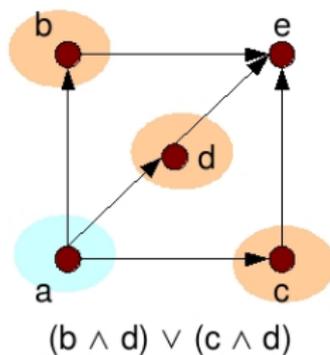
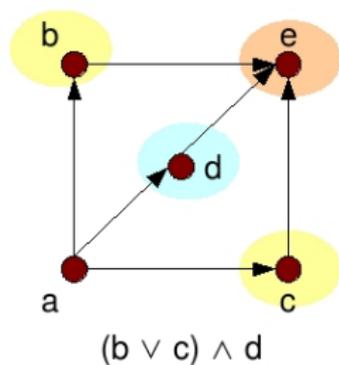
On dit qu'un treillis est distributif si l'on a, pour tous  $x, y$  et  $z$  :

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$



# Treillis non distributif

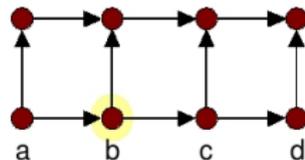
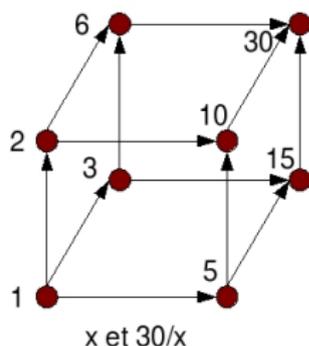
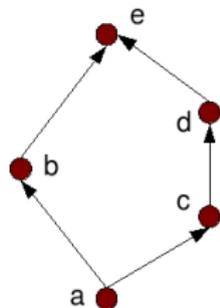




# Treillis complémenté

## Définition

Un treillis est complémenté si chacun de ses éléments possède au moins un complément.



# Définition algébrique d'un treillis

## Nouvelle définition de treillis

Un treillis est un ensemble  $E$  muni de deux lois internes habituellement notées  $\vee$  et  $\wedge$  vérifiant :

- Les deux lois sont commutatives et associatives
- $\forall a \in E, a \vee a = a$  et  $a \wedge a = a$  (idempotence)
- $\forall a, b \in E, a \wedge (a \vee b) = a$  et  $a \vee (a \wedge b) = a$  (absorption)

## Lien avec les relations d'ordre $(E, \preceq)$

Définir sur  $E$  une relation d'ordre  $\preceq$  :

$$a \preceq b \iff a \vee b = b$$

# Preuve que $\preceq$ est une relation d'ordre

$$E : a \preceq b \iff a \vee b = b$$

## Antisymétrie

$$a \preceq b \text{ et } b \preceq a$$

$$\Rightarrow a \vee b = b \text{ et } b \vee a = a$$

$$\Rightarrow b = a \text{ par commutativité}$$

## réflexivité

$$a \vee a = a \text{ par idempotence}$$

$$\Rightarrow a \preceq a$$

# Preuve que $\preceq$ est une relation d'ordre

$$E : a \preceq b \iff a \vee b = b$$

## Transitivité

$$a \preceq b \text{ et } b \preceq c$$

$$\Rightarrow a \vee b = b \text{ et } b \vee c = c$$

$$\Rightarrow a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c \text{ par associativité}$$

$$\Rightarrow a \preceq c$$

## Une définition

Un treillis à la fois distributif et complété est une algèbre de Boole

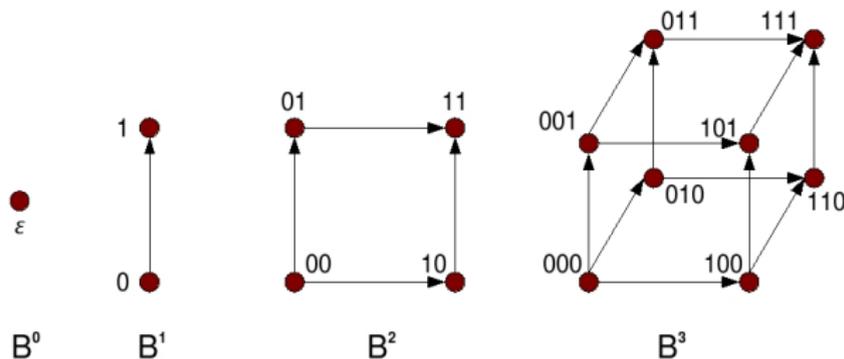
Exemple : les parties d'un ensemble non-vide  $E$

$\mathcal{P}(E)$  ordonné par la relation d'inclusion large  $\subseteq$ , est une algèbre de Boole.

# Exemple d'algèbre de Boole : $\mathbb{B}^n$

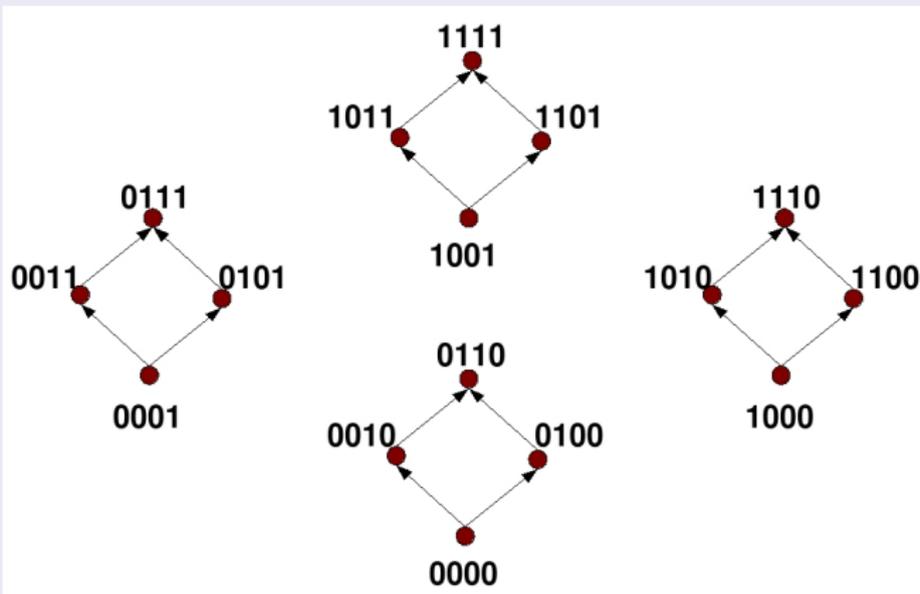
- 1  $\mathbb{B}^0$  : un seul élément (cas dégénéré)
- 2  $\mathbb{B}^1$  :  $0 \preceq 1, 0 \preceq 0, 1 \preceq 1$
- 3  $\mathbb{B}^n$  ordonné par  $\preceq$  :

$$a_1 a_2 \cdots a_n \preceq b_1 b_2 \cdots b_n \text{ si } a_p \preceq b_p \forall 1 \leq p \leq n$$



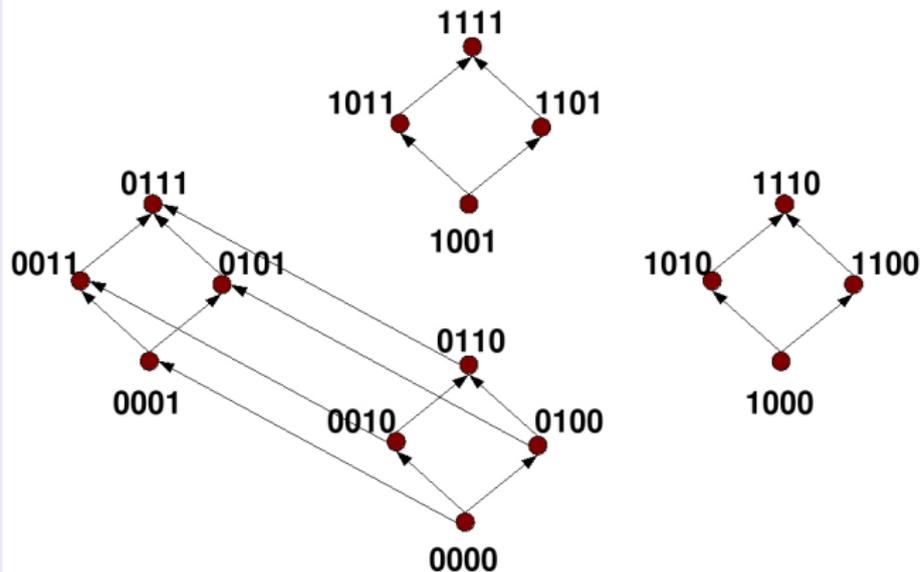
# Exemple d'algèbre de Boole : $\mathbb{B}^n$ (cont'd)

## Dessignons $\mathbb{B}^4$



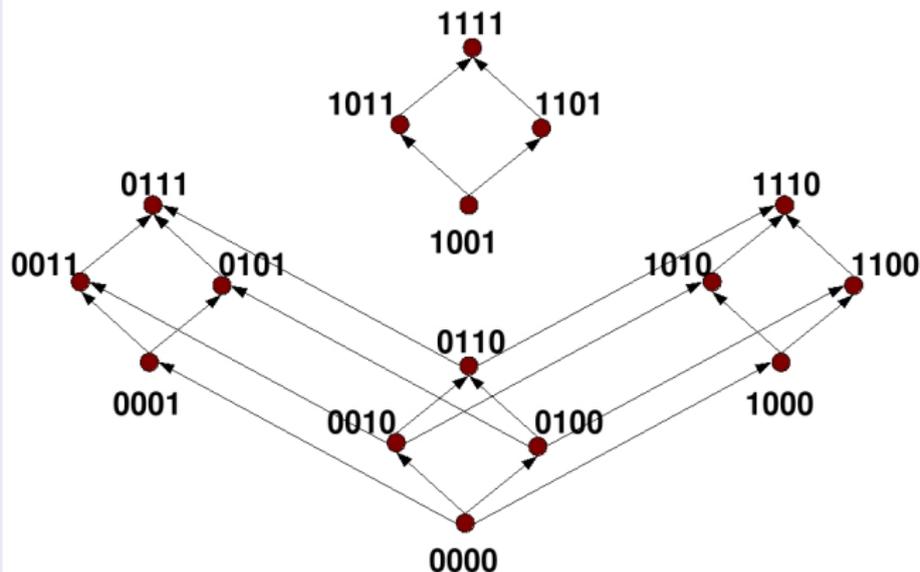
# Exemple d'algèbre de Boole : $\mathbb{B}^n$ (cont'd)

## Dessignons $\mathbb{B}^4$



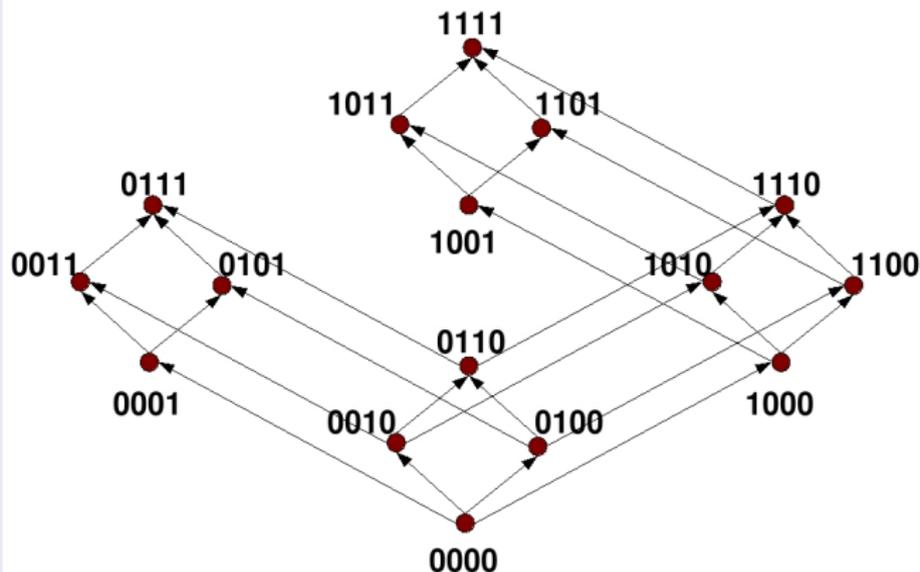
# Exemple d'algèbre de Boole : $\mathbb{B}^n$ (cont'd)

## Dessinons $\mathbb{B}^4$



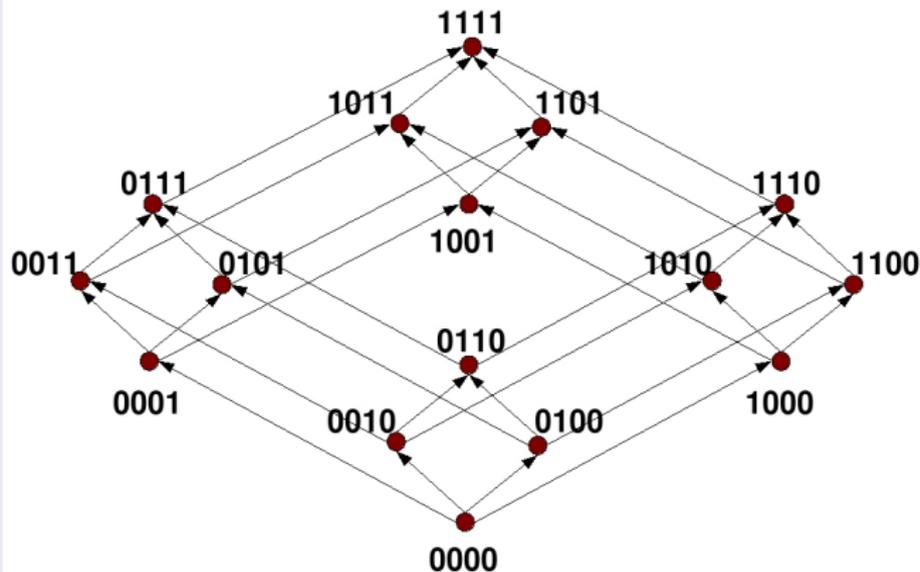
# Exemple d'algèbre de Boole : $\mathbb{B}^n$ (cont'd)

## Dessignons $\mathbb{B}^4$



# Exemple d'algèbre de Boole : $\mathbb{B}^n$ (cont'd)

Dessignons  $\mathbb{B}^4$



# Exemple d'algèbre de Boole : $\mathbb{B}^n$ (cont'd)

Soit  $a, b \in \mathbb{B}^n$  :  $a = a_1 \cdots a_n$  et  $b = b_1 \cdots b_n$

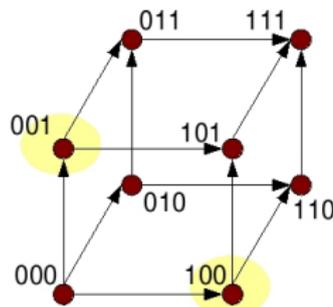
- 1 PpM :  $a \vee b = (a_1 \vee b_1)(a_2 \vee b_2) \cdots (a_n \vee b_n)$
- 2 PGm :  $a \wedge b = (a_1 \wedge b_1)(a_2 \wedge b_2) \cdots (a_n \wedge b_n)$
- 3 Complément :  $\bar{a} = \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n$

Exemple dans  $\mathbb{B}^3$

$$001 \vee 100 = 101$$

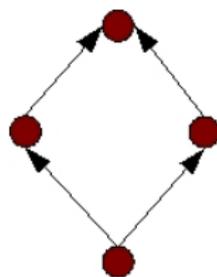
$$001 \wedge 100 = 000$$

$$\overline{001} = 110$$



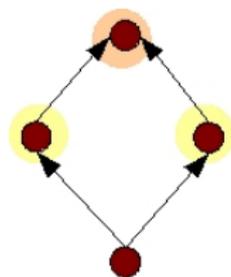
# Notations générales

- Algèbre de Boole :  $\mathcal{B}$ , de relation d'ordre  $\preceq$
- Plus petit majorant (PpM) de  $a$  et  $b$  :  $a \vee b$
- Plus Grand minorant (PGm) de  $a$  et  $b$  :  $a \wedge b$
- Complément de  $a$  :  $\bar{a}$  **unique** (à montrer)
- Plus grand élément de  $\mathcal{B}$  :  $\top$
- Plus petit élément de  $\mathcal{B}$  :  $\perp$



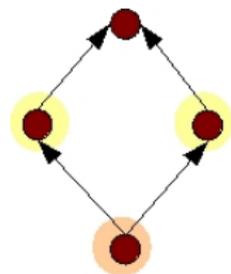
# Notations générales

- Algèbre de Boole :  $\mathcal{B}$ , de relation d'ordre  $\preceq$
- Plus petit majorant (PpM) de  $a$  et  $b$  :  $a \vee b$
- Plus Grand minorant (PGm) de  $a$  et  $b$  :  $a \wedge b$
- Complément de  $a$  :  $\bar{a}$  **unique** (à montrer)
- Plus grand élément de  $\mathcal{B}$  :  $\top$
- Plus petit élément de  $\mathcal{B}$  :  $\perp$



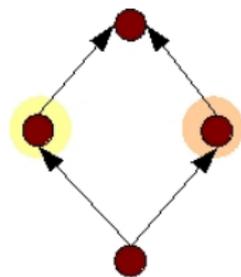
# Notations générales

- Algèbre de Boole :  $\mathcal{B}$ , de relation d'ordre  $\preceq$
- Plus petit majorant (PpM) de  $a$  et  $b$  :  $a \vee b$
- Plus Grand minorant (PGm) de  $a$  et  $b$  :  $a \wedge b$
- Complément de  $a$  :  $\bar{a}$  **unique** (à montrer)
- Plus grand élément de  $\mathcal{B}$  :  $\top$
- Plus petit élément de  $\mathcal{B}$  :  $\perp$



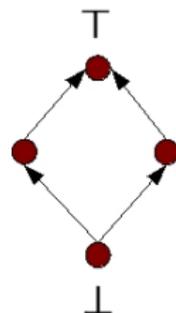
# Notations générales

- Algèbre de Boole :  $\mathcal{B}$ , de relation d'ordre  $\preceq$
- Plus petit majorant (PpM) de  $a$  et  $b$  :  $a \vee b$
- Plus Grand minorant (PGm) de  $a$  et  $b$  :  $a \wedge b$
- Complément de  $a$  :  $\bar{a}$  **unique** (à montrer)
- Plus grand élément de  $\mathcal{B}$  :  $\top$
- Plus petit élément de  $\mathcal{B}$  :  $\perp$



# Notations générales

- Algèbre de Boole :  $\mathcal{B}$ , de relation d'ordre  $\preceq$
- Plus petit majorant (PpM) de  $a$  et  $b$  :  $a \vee b$
- Plus Grand minorant (PGm) de  $a$  et  $b$  :  $a \wedge b$
- Complément de  $a$  :  $\bar{a}$  **unique** (à montrer)
- Plus grand élément de  $\mathcal{B}$  :  $\top$
- Plus petit élément de  $\mathcal{B}$  :  $\perp$



# Propriétés des opérations d'une algèbre de Boole

## Propriétés de $\vee$

$$x \vee y = y \vee x \quad (1)$$

$$x \vee (y \vee z) = (x \vee y) \vee z \quad (2)$$

$$x \vee \top = \top \quad (3)$$

$$x \vee \perp = x \quad (4)$$

$$x \vee x = x \quad (5)$$

# Propriétés des opérations d'une algèbre de Boole (cont'd)

## Propriétés de $\wedge$

$$x \wedge y = y \wedge x \quad (6)$$

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \quad (7)$$

$$x \wedge \top = x \quad (8)$$

$$x \wedge \perp = \perp \quad (9)$$

$$x \wedge x = x \quad (10)$$

# Propriétés des opérations d'une algèbre de Boole (cont'd)

## Distributivités

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad (11)$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad (12)$$

## Lois d'absorption

$$x \wedge (x \vee y) = x \quad (13)$$

$$x \vee (x \wedge y) = x \quad (14)$$

# Propriétés des opérations d'une algèbre de Boole (cont'd)

## Propriétés de la complémentation

$$x \vee \bar{x} = \top \quad (15)$$

$$x \wedge \bar{x} = \perp \quad (16)$$

$$\overline{\bar{x}} = x \quad (17)$$

$$\overline{\top} = \perp \quad (18)$$

$$\overline{\perp} = \top \quad (19)$$

# Propriétés des opérations d'une algèbre de Boole (cont'd)

## Lois de De Morgan

$$\overline{x \wedge y} = \bar{x} \vee \bar{y} \quad (20)$$

$$\overline{x \vee y} = \bar{x} \wedge \bar{y} \quad (21)$$

## Liens entre $\vee$ , $\wedge$ et $\preceq$

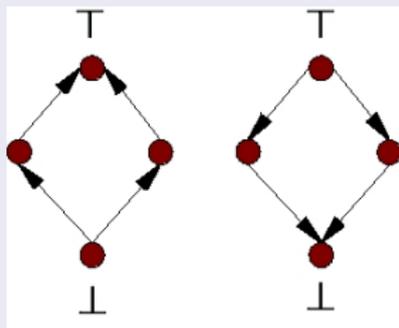
$$x \wedge y = x \text{ équivaut à } x \preceq y \quad (22)$$

$$x \vee y = y \text{ équivaut à } x \preceq y \quad (23)$$

# Principe de dualité

## Constatation

- En renversant la relation d'ordre de  $\mathcal{B}$ ,  $\vee$  et  $\wedge$  s'échangent.
- Plus précisément : si  $x \preceq y$  alors  $\bar{y} \preceq \bar{x}$  (DeMorgan et complémentation)



# Principe de dualité (cont'd)

## Théorème

Si  $x$  est le résultat d'un calcul fait à partir uniquement de  $\vee$  et  $\wedge$  et des éléments  $y, z, \text{ etc.}$ , et de leurs compléments alors  $\bar{x}$  s'obtient, en remplaçant dans le même calcul,  $y$  par  $\bar{y}$ ,  $z$  par  $\bar{z}$ , etc.,  $\vee$  par  $\wedge$  et  $\wedge$  par  $\vee$ .

## Éléments de preuve

Complémentation et lois de De Morgan.

## Exemple

$$x = (y \vee z) \wedge (\bar{a} \vee b)$$

$$\bar{x} = (\bar{y} \wedge \bar{z}) \vee (a \wedge \bar{b})$$

# Théorème

Soit un ensemble  $E$  muni des opérations  $\nabla$ ,  $\Delta$  et  $\sim$ , et de deux éléments  $\alpha$  et  $\Omega$  vérifiant :

$$a \nabla b = b \nabla a \quad (24)$$

$$a \Delta b = b \Delta a \quad (29)$$

$$a \nabla (b \nabla c) = (a \nabla b) \nabla c \quad (25)$$

$$a \Delta (b \Delta c) = (a \Delta b) \Delta c \quad (30)$$

$$a \nabla \alpha = a \quad (26)$$

$$a \Delta \Omega = a \quad (31)$$

$$a \nabla \tilde{a} = \Omega \quad (27)$$

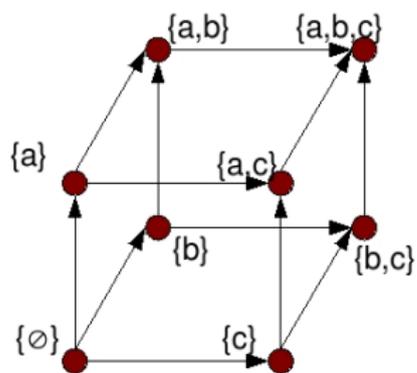
$$a \Delta \tilde{a} = \alpha \quad (32)$$

$$a \Delta (b \nabla c) = (a \Delta b) \nabla (a \Delta c) \quad (28)$$

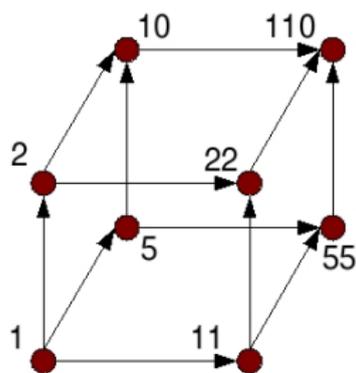
$$a \nabla (b \Delta c) = (a \nabla b) \Delta (a \nabla c) \quad (33)$$

Alors il existe une relation d'ordre sur  $E$  qui en fait une algèbre de Boole pour laquelle  $\sim$ ,  $\Delta$ ,  $\nabla$ ,  $\alpha$  et  $\Omega$  sont respectivement  $\bar{\phantom{x}}$ ,  $\wedge$ ,  $\vee$ ,  $\perp$  et  $\top$ .

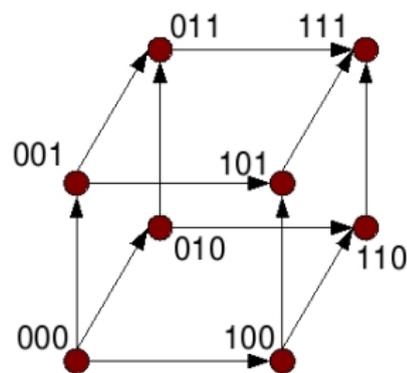
# Ressemblances des algèbres de Boole



$P(\{a,b,c\})$



Diviseurs de (110)



$B^3$

Pour aller plus loin : diagramme de Hasse d'une algèbre de Boole de  $2^n$  éléments = diagramme de Hasse de  $B^n$

# Définitions supplémentaires

## Atome d'une algèbre de Boole

- Un élément  $a$  est un atome de l'algèbre de Boole  $\mathcal{B}$  si c'est un successeur immédiat de  $\perp$
- Exemple : les atomes de  $\mathcal{P}(\{a, b, c\})$  sont les trois singletons ; dans  $\mathbb{B}^3$  ce sont les mots 001, 010 et 100.

## Isomorphisme d'algèbre de Boole (du grec *même forme*)

- Similarité de diagrammes (sommets et flèches identiques)
- Il existe une bijection  $\phi$  entre deux algèbres de Boole isomorphes qui respecte leur relation d'ordre

$$\phi(x) \preceq \phi(y) \Leftrightarrow x \preceq y$$

# Théorème de Stone

- 1 Le nombre d'éléments d'une algèbre de Boole finie est toujours une puissance de 2
- 2  $\forall n > 0$ , il existe des algèbres de Boole à  $2^n$  éléments (et toutes sont isomorphes entre elles)
- 3 Une algèbre de Boole qui possède  $2^n$  éléments possède  $n$  atomes : elle est isomorphe à  $\mathbb{B}^n$  et son diagramme de Hasse est un  $n$ -cube.

Une algèbre de Boole finie est entièrement connue dès lors que l'on connaît son nombre d'éléments

# Lemme pour prouver le théorème de Stone

## Lemme

Soit  $a \neq \perp$  un élément d'une algèbre de boole  $\mathcal{B}$ .

L'élément  $a$  peut s'exprimer de manière unique comme plus petit majorant d'un ensemble d'atomes

$\{b_1, b_2, \dots, b_k\}$ .

On a donc  $a = b_1 \vee b_2 \vee \dots \vee b_k$