IFT1063 Patrice MARCOTTE novembre 1998

CHAPITRE 1: LOGIQUE, ENSEMBLES, SUITES, FONCTIONS

1. Une **proposition** (notée p, q, ...) est un énoncé qui est soit **vrai** (**V** ou 1) soit **faux** (**F** ou 0). Les opérations usuelles sur les propositions sont les suivantes ("ssi" est utilisée comme abréviation de "si et seulement si"):

   négation (non): $\neg p = \mathbf{V}$ ssi $p = \mathbf{F}$
   disjonction (ou): $p \vee q = \mathbf{V}$ ssi p ou q (ou les deux) est **V**
   conjonction (et): $p \wedge q = \mathbf{V}$ ssi p et q sont **V**
   ou exclusif: $p \oplus q = \mathbf{V}$ ssi p ou q est **V**, mais *pas* les deux
   conditionnelle: $p \rightarrow q = \mathbf{F}$ ssi $p = \mathbf{V}$ et $q = \mathbf{F}$.
   On dit: "p implique q" ou: "si p alors q"
   p est l' **hypothèse** ou **condition suffisante** et q la **conclusion** ou **condition nécessaire**.
   biconditionnelle: $p \leftrightarrow q = \mathbf{V}$ ssi $p = q$
   On dit: "p si et seulement si q".

   Les opérateurs précédents peuvent se représenter à l'aide de **tables de vérité**:

p	$\neg p$
V	**F**
F	**V**

p	q	$p \wedge q$
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**F**

p	q	$p \vee q$
V	**V**	**V**
V	**F**	**V**
F	**V**	**V**
F	**F**	**F**

p	q	$p \oplus q$
V	**V**	**F**
V	**F**	**V**
F	**V**	**V**
F	**F**	**F**

p	q	$p \rightarrow q$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

p	q	$p \leftrightarrow q$
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**V**

   tautologie: proposition qui est toujours **V** quelle que soit la valeur des énoncés qui la composent; une **contradiction** est une proposition qui est toujours fausse. Deux propositions p et q sont **logiquement équivalentes** si $p \leftrightarrow q$ est une tautologie, c'est-à-dire que p et q ont les mêmes tables de vérité. On note $p \equiv q$ ou $p \iff q$. Si $p \rightarrow q$ est une tautologie, on note $p \Rightarrow q$.

   contraposée de $p \rightarrow q$: $(\neg q) \rightarrow (\neg p) \equiv p \rightarrow q$
   réciproque de $p \rightarrow q$: $q \rightarrow p$
   lois de de Morgan: $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$ $\quad \neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$
   commutativité: $p \vee q \equiv q \vee p$ $\quad p \wedge q \equiv q \wedge p$
   associativité: $p \vee (q \vee r) \equiv (p \vee q) \vee r$ $\quad p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
   distributivité: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $\quad p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

   On peut définir des opérations logiques sur des **bits** (0 ou 1) ou des chaînes de bits de même longueur.

2. Une proposition contenant une ou plusieurs **variables** est une **fonction propositionnelle**, notée $P(x)$, $Q(x,y)$, etc. Sa valeur de vérité dépend des valeurs assignées aux variables. Si $P(x) = \mathbf{V}$ pour toute valeur de la variable x appartenant à l'**univers** du **discours** D, la proposition $\forall x \in D \; P(x)$ est vraie, et fausse sinon. Si le contexte est clair on écrit simplement $\forall x \; P(x)$; $\forall$ est le **quantificateur universel**. S'il existe *au moins* une valeur de x pour laquelle $P(x) = \mathbf{V}$, alors la proposition $\exists x \; P(x)$ est vraie; $\exists$ est le **quantificateur existentiel**. Une variable affectée par un quantificateur ou ayant une valeur assignée est dite **liée**. Sinon elle est dite **libre**. Lorsqu'on assigne des valeurs aux variables libres d'une fonction propositionnelle, on obtient une proposition.

   lois de de Morgan: $\neg \exists x \; P(x) \equiv \forall x \; \neg P(x)$; $\quad \neg \forall x \; P(x) \equiv \exists x \; \neg P(x)$

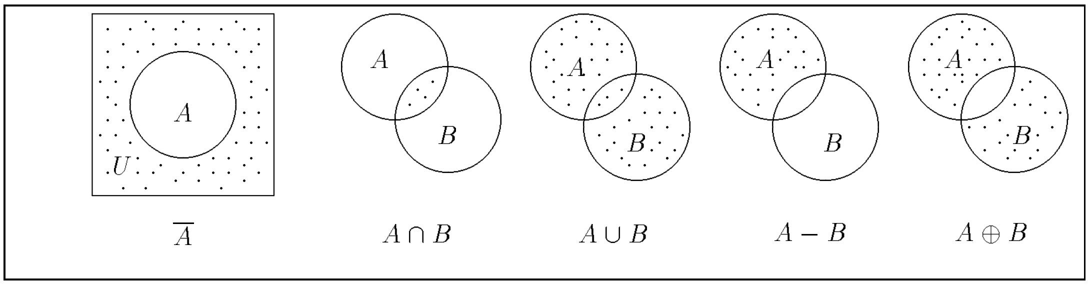
3. Un **ensemble** peut se décrire en donnant une liste de ses **éléments** ou en décrivant la propriété commune à tous ses éléments. On écrit: x (élément) $\in A$ (ensemble). L'**ensemble vide** $\emptyset$ ne contient aucun élément. Deux ensembles sont **égaux** ($A = B$) s'ils ont les mêmes éléments. A est un **sous-ensemble** de B ($A \subset B$) si tout élément de A est élément de B. Si $A \subset B$ et $A \neq B$, A est un sous-ensemble **propre** de B. La cardinalité d'un ensemble fini A, notée $|A|$, est son nombre d'éléments. L'ensemble de tous les sous-ensembles de A est appelé l'**ensemble des parties** de A, et est noté $\mathcal{P}(\mathcal{A})$ ou 2^A. Si A est un ensemble fini: $|\mathcal{P}(A)| = 2^{|A|}$.

   On nomme n-**uplet** l'ensemble ordonné $(a_1, a_2, \ldots, a_n)$ où $a_1 \in A_1, \ldots, a_n \in A_n$. Deux n-uplets sont égaux si leurs éléments correspondants sont égaux. Le **produit cartésien** des ensembles $A_1, A_2, \ldots, A_n$ est défini par: $A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) | \forall i \; a_i \in A_i\}$.

4. On note par U l'**univers** des éléments considérés. Tout ensemble est un sous-ensemble de U. On définit les opérations suivantes sur les ensembles:

union:	$A \cup B = \{x \mid x \in A \ \vee \ x \in B\}$
intersection:	$A \cap B = \{x \mid x \in A \ \wedge \ x \in B\}$
différence:	$A - B = \{x \mid x \in A \ \wedge \ x \notin B\}$
complément:	$\overline{A} = \{x \in U \ \wedge x \notin A\}$
différence symétrique:	$A \oplus B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$

Les opérations peuvent se représenter graphiquement à l'aide de **diagrammes de Venn**:



On a les propriétés importantes suivantes

lois de de Morgan:	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
commutativité:	$A \cup B = B \cup A$	$A \cap B = B \cap A$
associativité:	$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$
distributivité:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Ces identités peuvent se démontrer par raisonnement logique ou à l'aide de **tables d'appartenance** où toutes les combinaisons d'appartenance et non-appartenance à l'un ou l'autre des ensembles sont considérées. Noter la similitude avec les tables de vérité.

Notation: $\bigcup_{i=1}^{n} A_i = A_1 \cup \ldots \cup A_n \qquad \bigcap_{i=1}^{n} A_i = A_1 \cap \ldots \cap A_n$

Soit A un ensemble fini. On peut représenter un sous-ensemble B de A par une chaîne de bits $(b_1, \ldots, b_n)$ où $b_i = 1$ si le $i$ème élément de A fait partie de B, et $b_i = 0$ sinon. Les opérations sur les sous-ensembles peuvent être effectuées sur les chaînes de bits correspondantes.

5. Une **fonction** de X dans Y associe d'une façon *unique* un élément de Y (Y est le **codomaine de** f) à *tout* élément de X (X est le **domaine** de f). On écrit: $f(a) = b$ si $b \in Y$ est associé à $a \in X$. L'**image** de f est le sous-ensemble du codomaine de f défini par $\mathrm{Im}(f) = f(X) = \{b \in Y \mid \exists a \in X \mid f(a) = b\}$. Si $S \subset X$, alors on définit $f(S) = \{f(x) \mid x \in S\}$. Une fonction est **injective** si $x \neq y$ implique $f(x) \neq f(y)$. Une fonction est **surjective** si $f(X) = Y$. Une fonction **bijective** est à la fois injective et surjective. Si $f : X \to Y$ est bijective, sa fonction inverse f^{-1} est définie par: $f^{-1}(y) = x$, où x est l'**unique** élément de X tel que $f(x) = y$. Le **graphe** d'une fonction f de domaine A est l'ensemble des couples ordonnés $\{(a, f(a)), a \in A\}$. La fonction composée $f \circ g$ est définie par: $(f \circ g)(a) = f(g(a))$.

   Deux ensembles A et B ont la même **cardinalité** s'il existe une bijection entre A et B. La cardinalité d'un ensemble fini correspond au nombre de ses éléments. Tout ensemble infini ayant la même cardinalité que $\mathbb{N}$ est **dénombrable**. Un ensemble infini qui n'est pas dénombrable est **non dénombrable**. L'ensemble des nombres rationnels $\mathbb{Q}$ est dénombrable. L'ensemble des nombres réels $\mathbb{R}$ est non dénombrable.

   Notation: $\lfloor x \rfloor$: plus grand entier plus petit que x
   $\lceil x \rceil$: plus petit entier plus grand que x

   Une **suite** dans S est une fonction f de $\mathbb{N}$ dans S. On note: $f(n) = a_n$; a_n est un **terme** de la suite. En informatique, une **chaîne** $a_1, \ldots, a_n$ de longueur n correspond à la suite finie $a_1, \ldots, a_n$. On définit:

$$\sum_{j=m}^{n} a_j = a_m + \ldots + a_n.$$

Une **progression géométrique** est une suite de la forme: $a_n = ar^n$; r est la **raison** de la suite. La somme des termes d'une suite est une **série**. On a:

$$\sum_{j=0}^{n} ar^j = a\frac{r^{n+1}-1}{r-1}.$$

6. **Croissance des fonctions.**

Notation O: $f(x) \in O(g(x))$ s'il existe des constantes C et k telles que $|f(x)| \leq C|g(x)| \quad \forall x \geq k$.

Si $f(x) \in O(g(x))$ et $g(x) \in O(f(x))$, f et g sont du même **ordre** et on écrit: $f(x) \in \Theta(g(x))$. Ces notations sont surtout utilisées pour les fonctions positives et croissantes de $\mathbb{N}$ dans $\mathbb{N}$. Les résultats suivants sont immédiats:

$$\left.\begin{array}{l} f_1(x) \in O(g_1(x)) \\ f_2(x) \in O(g_2(x)) \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} (f_1+f_2)(x) \in O(\max(g_1(x), g_2(x))) \\ (f_1 f_2)(x) \in O(g_1(x)g_2(x)) \end{array}\right.$$

$$\sum_{i=0}^{n} a_i x^i \in O(x^n) \qquad \text{si} \quad a_n \neq 0.$$

Classement des fonctions usuelles à l'aide de la notation O:

$$O(1) \subset O(\lg n) \subset O(n) \subset O(n \lg n) \subset O(n^2) \subset O(2^n) \subset O(n!)\ .$$

CHAPITRE 2: ALGORITHMES ET MATRICES

1. Un **algorithme** est une procédure de résolution d'un problème en un nombre *fini* d'étapes bien définies. La **complexité** d'un algorithme peut s'exprimer en temps (complexité-temps, nombre d'opérations) ou en espace (complexité-espace) requis pour résoudre le problème. La complexité peut être établie en fonction du **pire cas** ou du **cas moyen**. Les complexités les plus fréquemment rencontrées sont les complexités **constante** ($O(1)$), **logarithmique** ($O(\log n)$), **linéaire** ($O(n)$), $n \log n$, **polynômiale** ($O(n^k)$), **exponentielle** ($O(k^n)$) et **factorielle** ($O(n!)$).

2. **Théorie des nombres.**

Notations:

$a \mid b$:	a divise b
$a \not\mid b$:	a ne divise pas b
PGCD(a,b):	Plus Grand Commun Diviseur de a et b
PPCM(a,b):	Plus Petit Commun Multiple de a et b
$a \bmod m$:	reste (positif ou nul) de la division de a par m
$a \equiv b \bmod m$	$\iff a \bmod m = b \bmod m$
	$\iff (a-b) \bmod m = 0$

Deux nombres a et b sont **premiers entre eux** si PGCD$(a,b) = 1$.

Tout entier positif peut s'exprimer *de façon unique* comme produit de puissances de nombres premiers. Les résultats suivants sont faciles (!) à démontrer:

$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
$(ab) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$
$\exists\, s,t \in \mathbb{Z}$ tels que $\mathrm{PGCD}(a,b) = sa + tb$
$\mathrm{PGCD}(a,b) \times \mathrm{PPCM}(a,b) = ab$
$(\mathrm{PGCD}(a,b) = 1) \quad \wedge \quad (a \mid bc) \quad \Rightarrow \quad (a \mid c)$
si $a = bq + r$, $\mathrm{PGCD}(a,b) = \mathrm{PGCD}(b,r)$
$\mathrm{PGCD}(a,b) = \mathrm{PGCD}(a, b \bmod a)$
$ab = \mathrm{PGCD}(a,b)\mathrm{PPCM}(a,b)$

Le dernier résultat constitue la base théorique d'une méthode efficace (algorithme d'Euclide) permettant de calculer PGCD(a,b):

procédure PGCD(a,b)
$x \leftarrow a \quad y \leftarrow b$
tant que $y \neq 0$ faire $\quad r \leftarrow x \bmod y$
$\qquad\qquad\qquad\qquad x \leftarrow y \quad y \leftarrow r$
PGCD$(a,b) = x$

Soit b un entier positif appelé **base**. Tout nombre entier n peut s'exprimer de façon unique comme:

$$n = a_k b^k + \ldots + a_1 b + a_0$$

où $0 \leq a_k < b$ pour tout k et $a_k \neq 0$. On écrit:

$$n = (a_k a_{k-1} \ldots a_0)_b.$$

Les algorithmes suivants permettent de passer d'une base à une autre, ainsi que d'additionner et de multiplier deux entiers en base 2:

procédure expression de n en base b; résultat dans la chaîne a
$q \leftarrow n \quad k \leftarrow 0$
tant que $q \neq 0$ faire $\quad a_k \leftarrow q \bmod b$
$\qquad\qquad\qquad\qquad q \leftarrow \lfloor q/b \rfloor$
$\qquad\qquad\qquad\qquad k \leftarrow k+1$

procédure additionner (a, b) en base 2; résultat dans la chaîne s
retenue $\leftarrow 0$
pour $j \leftarrow 0$ **à** $n-1$ faire $\quad d \leftarrow \lfloor (a_j + b_j + \text{retenue})/2 \rfloor$
$\quad s_j \leftarrow a_j + b_j + \text{retenue} - 2d$
$\quad \text{retenue} \leftarrow d$
$s_n \leftarrow$ retenue

procédure multiplier (a, b) en base 2; résultat dans la chaîne p
$p \leftarrow 0$
pour $j \leftarrow 0$ **à** $n-1$ faire **si** $b_j = 1$ **alors** $c_j \leftarrow a$ décalé à gauche de j positions
$\quad p \leftarrow p + c_j$

3. Dans le système du **complément à 1**, un entier m $(-(2^n-1) \leq m \leq 2^n - 1)$ sera noté $m = [b_n b_{n-1} \dots b_1 b_0]_1$ et défini de la façon suivante:

$$\begin{array}{lll} \text{si } m > 0: & b_n = 0 \quad \text{et} \quad m = (b_{n-1} \dots b_0)_2 \\ \text{si } m < 0: & b_n = 1 \quad \text{et} \quad |m| = (\neg(b_{n-1} \dots b_0)) \\ 0 = 0 \dots 0 & -0 = 1 \dots 1. \end{array}$$

L'addition de deux nombres s'effectue de façon normale, en base 2; s'il y a une retenue sur le bit de gauche, on rajoute 1 au nombre obtenu.

Dans le système du **complément à 2**, un entier m $(-2^n \leq m \leq 2^n - 1)$ sera noté $m = [b_n b_{n-1} \dots b_1 b_0]_2$ et défini de la façon suivante:

$$\begin{array}{lll} \text{si } m > 0: & b_n = 0 \quad \text{et} \quad m = (b_{n-1} \dots b_0)_2 \\ \text{si } m < 0: & \text{on ajoute 1 au complément à 1 de } m \\ 0 = 0 \dots 0 & -0 = 0 \dots 0. \end{array}$$

L'addition s'effectue normalement en base 2.

4. **Matrices.** Une matrice A est **booléenne** si ses éléments a_{ij} sont égaux à 0 ou à 1. Si A et B sont des matrices booléennes, on définit "élément à élément" $\neg A$, $A \vee B$, $A \wedge B$, etc.

Etant donnés deux opérateurs binaires $\circ$ et $\bullet$, le **produit généralisé** $C = A \circ \bullet B$ de deux matrices $A: m \times p$ et $B: p \times n$ est défini par

$$c_{ij} = (a_{i1} \bullet b_{1j}) \circ (a_{i2} \bullet b_{2j}) \circ \dots \circ (a_{ik} \bullet b_{kj}) \qquad i = 1, \dots, m \quad j = 1, \dots, n.$$

Si $\circ$ représente l'addition et $\bullet$ la multiplication ordinaires définis sur les réels, on retrouve la formule habituelle

$$c_{ij} = a_{i1} b_{1j} + \dots + a_{ik} b_{kj}.$$

Si A et B sont des matrices booléennes, $\circ = \vee$ et $\bullet = \wedge$, on obtient le **produit booléen** $C = A \odot B$:

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee \dots \vee (a_{ik} \wedge b_{kj}).$$

Si $\circ = \max$ et $\bullet = \min$ on obtient:

$$c_{ij} = \max\Big(\min(a_{i1}, b_{1j}), \dots, \min(a_{ik}, b_{kj})\Big).$$

CHAPITRE 3: RAISONNEMENT MATHÉMATIQUE

1. Un **théorème** est un énoncé vrai obtenu par raisonnement logique à partir d'**axiomes** (énoncés dont on accepte *sans discuter* la véracité) et de tautologies appelées **règles d'inférence**. Une **conjecture** est un énoncé dont on ne connaît pas la valeur de vérité. Les règles d'inférence les plus fréquemment utilisées sont les suivantes:

$$\begin{array}{lll} p \to (p \vee q) & (p \wedge q) \to p & [p \wedge (p \to q)] \to q \\ (\neg q \wedge (p \to q)) \to \neg p & [(p \to q) \wedge (q \to r)] \to (p \to r) & [(p \vee q) \wedge \neg p] \to q. \end{array}$$

2. On substitue parfois à la **preuve directe** $p \to q$ d'un théorème la preuve de sa contraposée: $\neg q \to \neg p$. Cette technique porte le nom de **preuve par contradiction**. La preuve par contradiction peut également être utilisée comme suit: pour montrer que $p = \mathbf{V}$ on montre que $\neg p = \mathbf{F}$.

3. Si p est l'énoncé composé $p_1 \vee p_2 \vee \ldots \vee p_n$ on procède parfois par décomposition (**preuve par cas**):

$$\begin{aligned} p \to q &\equiv (p_1 \vee p_2 \vee \ldots \vee p_n) \to q \\ &\equiv (p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q). \end{aligned}$$

4. Le théorème $p \leftrightarrow q$ se démontre à l'aide de l'équivalence $(p \leftrightarrow q) \equiv (p \to q) \wedge (q \to p)$. Plus généralement: $(p_1 \leftrightarrow \ldots \leftrightarrow p_n) \equiv (p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \ldots \wedge (p_n \to p_1)$.

5. Une **preuve d'existence** permet de démontrer un théorème de la forme $\exists x\ P(x)$. Une telle preuve est **constructive** si l'on peut exhiber un élément a tel que $P(a) = \mathbf{V}$. Il existe des preuves d'existence **non constructives**, obtenues habituellement en démontrant que l'énoncé $\neg(\exists x\ P(x))$ est faux.

6. Le principe d'**induction mathématique** est basé sur l'axiome baptisé **principe du bon ordre**: "Tout ensemble non vide d'entiers positifs ou nuls possède un plus petit élément".

   Pour démontrer que $\forall n \in \mathbb{N}\ P(n)$, on procède en deux étapes:

   1. Base de l'induction: $P(1) = \mathbf{V}$.
   2. Induction: $(P(n) \to P(n+1)) = \mathbf{V}$ pour tout $n \in \mathbb{N}$.

   Une forme équivalente du principe d'induction remplace l'étape d'induction par:

   2. Induction: $[P(1) \wedge \ldots \wedge P(n)) \to P(n+1)] = \mathbf{V}$ pour tout $n \in \mathbb{N}$.

   Les deux formes sont équivalentes.

7. On peut définir de façon **récursive** une fonction f définie sur $\mathbb{N}$ en spécifiant $f(0)$ ainsi qu'une règle permettant de déterminer $f(n+1)$ à partir de $f(n)$. On peut également définir récursivement un ensemble S en se donnant une règle créant un élément de S à partir d'éléments déjà connus de S.

CHAPITRE 4: COMBINATOIRE ET DÉNOMBREMENT

1. **Principe multiplicatif.** Si un travail se compose de k tâches $T_1, \ldots, T_k$ et qu'il y a n_i façons de remplir chaque tâche T_i, alors il y a $n_1 \times \ldots n_k$ façons d'effectuer le travail.

2. **Principe d'inclusion-exclusion:**

$$\begin{aligned} |A_1 \cup A_2| &= |A_1| + |A_2| - |A_1 \cap A_2| \\ |\cup_{i=1}^n A_i| &= \sum_{r=1}^{n} (-1)^{r+1} \sum_{1 \le i_1 < \ldots < i_r \le n} |\bigcap_{k=1}^{r} A_{i_k}|. \end{aligned}$$

3. On peut utiliser une **arborescence** pour dénombrer toutes les possibilités correspondant à la définition d'un événement.

4. **Principe du pigeonnier:** Si plus de k objets occupent k cases, alors il existe au moins une case contenant plus d'un objet. De façon plus générale, si N objets occupent k cases, alors il existe au moins une case contenant au moins $\lceil N/k \rceil$ objets.

5. Une **permutation** de n objets distincts correspond à une liste *ordonnée* de ces objets. Il existe $n!$ permutations possibles de n objets distincts.

6. Un **arrangement** de r objets choisis parmi un ensemble E de n objets distincts correspond à une liste ordonnée de r objets distincts de E. Il y a

$$A(n,r) \stackrel{\text{def}}{=} n(n-1)\ldots(n-r+1) = \frac{n!}{(n-r)!}$$

arrangements possibles. Si $r = n$, on obtient comme cas particulier le nombre de permutations de n objets.

7. Une **combinaison** de r objets distincts choisis parmi un ensemble E de n objets distincts correspond à une liste *non ordonnée* de r objets de E, c'est-à-dire un sous-ensemble de r éléments de E. Il existe

$$\binom{n}{r} = C(n,r) \stackrel{\text{def}}{=} \frac{n!}{r!(n-r)!}$$

combinaisons possibles. Puisque $|2^E| = 2^n$, on a: $\sum_{r=0}^{n} C(n,r) = 2^n$. Aussi: $C(n,r) = C(n, n-r)$ et (**théorème du binôme de Newton**):

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}.$$

Les coefficients $\binom{n}{r}$ de l'expression précédente sont appelés **coefficients binômiaux**.

Identité de Pascal: $C(n+1,k) = C(n,k-1) + C(n,k)$.

Identité de Vandermonde: $C(m+n,r) = \sum_{k=0}^{r} C(m, r-k)C(n,k)$.

8. Il y a $\overline{A}(n,r) \stackrel{\text{def}}{=} n^r$ **arrangements avec répétition** de r objets choisis parmi n objets distincts (on tient compte de l'ordre).

9. Si l'on ne tient *pas* compte de l'ordre, il existe $\overline{C}(n,r) \stackrel{\text{def}}{=} C(n+r-1,r)$ **combinaisons avec répétitions** de r objets choisis parmi n objets distincts.

10. Le nombre de permutations de n objets dont n_i sont du type i, $i = 1, \ldots, k$ est égal à $n!/(n_1! \ldots n_k!)$.

    On peut dresser le schéma récapitulatif suivant pour les dénombrements:

	avec répétition	sans répétition
ordonnés (arrangements)	$\overline{A}(n,r) = n^r$	$A(n,r) = \frac{n!}{(n-r)!}$
non ordonnés (combinaisons)	$\overline{C}(n,r) = \frac{(n+r-1)!}{r!(n-1)!}$	$C(n,r) = \frac{n!}{r!(n-r)!}$

11. Pour engendrer la permutation succédant à la permutation $P = (a_1, \ldots, a_n)$ en ordre lexicographique, on trouve le couple (a_j, a_{j+1}) de P le plus à droite tel que $a_j < a_{j+1}$, on remplace a_j par

$$a_{j^*} = \min\{k : \; a_k \in \{a_{j+1}, \ldots, a_n\} \text{ et } a_k > a_j\},$$

    puis on réordonne les éléments dans les positions $j+1, \ldots, n$.

12. On engendre tous les sous-ensembles en utilisant la correspondance entre sous-ensembles et chaînes de bits. Un sous-ensemble de r éléments pouvant être représenté à l'aide de r bits, il suffit d'engendrer les nombres de 0 à $2^r - 1$ en notation binaire.

13. Soit $(a_1, \ldots, a_r)$ $(a_1 < a_2 \ldots < a_r)$ une combinaison de r nombres choisis parmi les entiers de 1 à n. Pour trouver la prochaine combinaison en ordre lexicographique, on choisit l'élément a_i le plus à droite qui puisse être augmenté $(a_i < n - r + i)$, on l'augmente de 1, puis on suit l'ordre naturel pour les nombres se trouvant à droite de a_i.

CHAPITRE 5: RELATIONS

1. Une **relation** (ou **relation binaire**) R sur les **domaines** A et B est un sous-ensemble de $A \times B$. Si $a \in A$ est en relation avec $b \in B$ on écrit aRb ou $(a,b) \in R$. Une fonction est un cas particulier de relation où $aRb \cap aRc \rightarrow b = b'$. Une relation R sur A est

   réflexive si aRa pour tout $a \in A$

   symétrique si $aRb \iff bRa$ pour tout $a, b \in A$

   antisymétrique si $(aRb) \wedge (bRa) \Rightarrow (a = b)$

   transitive si $(aRb) \wedge (bRc) \Rightarrow (aRc)$.

2. Les relations étant des ensembles, on peut leur appliquer les opérations classiques sur les ensembles: union, intersection, etc. Si R est une relation sur $A \times B$ et S une relation sur $B \times C$, la **relation composée** $S \circ R$ est définie par:
$$S \circ R = \{(a,c) | a \in A, c \in C \ \wedge \ \exists b | (a,b) \in R \ \wedge \ (b,c) \in S\}.$$
   Si R est une relation sur A, on définit récursivement:
$$R^1 = R \qquad R^{n+1} = R^n \circ R.$$
   Si R est transitive, on a: $R^n \subset R$ pour tout entier positif n.

3. Une **relation n-aire** (ou **de degré** n) sur les ensembles $A_1, \ldots, A_n$ est un sous-ensemble de $A_1 \times \ldots \times A_n$.

4. On peut représenter une relation sur des ensembles finis $A = \{a_1, \ldots, a_m\}$ et $B = \{b_1, \ldots, a_n\}$ à l'aide d'une matrice binaire M , c'est-à-dire: $a_i R b_j \iff m_{ij} = 1$. On a:

   $M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2} \quad M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}$
   $M_{S \circ R} = M_R \odot M_S \qquad M_{R^n} = M_R^{[n]}$ (puissance booléenne)

   On peut aussi représenter une relation à l'aide d'un **graphe orienté**, c'est-à-dire un ensemble V de **sommets** et E d'**arcs** reliant des couples (pas forcément distincts) de sommets. Lorsqu'un graphe représente une relation sur E, les sommets correspondent aux éléments de E et l'on crée un arc entre deux sommets a et b si et seulement si aRb. La relation R est réflexive si, dans le graphe associé, il existe des arcs de a vers a (**boucles**) pour tout a dans A; R est symétrique si la présence de l'arc (a,b) implique celle de l'arc (b,a); R est antisymétrique si $(a,b) \in E \ \wedge \ (b,a) \in E \Rightarrow (a = b)$; R est transitive si $(a,b) \in E \ \wedge \ (b,c) \in E \Rightarrow (a,c) \in E$.

5. Soit R une relation sur un ensemble fini A et G sa représentation graphique. La **fermeture réflexive** de R est la relation R' définie par:
$$aR'b \iff (aRb) \ \vee \ (a = b).$$
   R' est la plus petite relation réflexive contenant R. Similairement on définit la **fermeture symétrique** $\overline{R}$ de R:
$$a\overline{R}b \iff (aRb) \ \vee \ (bRa).$$
   La **fermeture transitive** de R est la relation R^* définie par:
$$aR^*b \iff \exists\, a_1, a_2, \ldots, a_n | (aRa_1) \wedge (a_1 R a_2) \wedge \ldots \wedge (a_{n-1} R a_n),$$
   c'est-à-dire qu'il existe un **chemin** (suite ordonnée d'arcs contigus) du sommet représentant a dans G au sommet représentant b. Si G contient n sommets et s'il existe un chemin entre les sommets a et b, alors il existe au moins un chemin de longueur inférieure ou égale à n. On en déduit:
$$R^* = \cup_{k=1}^n R^k \qquad M_{R^*} = \vee_{k=1}^n M_R^{[k]}$$
   avec:
$$M_R^{[k]} = M_R \odot M_R \cdots \odot M_R \quad (k \text{ produits booléens}).$$

L'**algorithme de Warshall** calcule efficacement la fermeture transitive d'un graphe (ou d'une relation). A l'étape k, l'algorithme établit s'il existe, pour tout couple de sommets (i, j), un chemin de i à j n'utilisant *que* des sommets intermédiaires d'indice inférieur ou égal à $k-1$. Soit $W^{[0]} = R$. On définit par récurrence:

$$W_{ij}^{[k]} = W_{ij}^{[k-1]} \vee (W_{ik}^{[k-1]} \wedge W_{kj}^{[k-1]}).$$

Après n itérations on obtient $M_{R^*} = W^{[n]}$. Complexité: $O(n^3)$.

6. Une relation réflexive, symétrique et transitive sur un ensemble A est une **relation d'équivalence**. Si $a \in A$, l'ensemble de tous le éléments b de A tels que aRb est la **classe d'équivalence** de a, notée $[a]_R$ ou simplement $[a]$ s'il n'y a pas d'ambiguïté. Tout élément b de $[a]_R$ est un **représentant** de la classe d'équivalence et permet de reconstituer celle-ci sans ambiguïté. Les énoncés suivants sont équivalents:

$$aRb \qquad [a] = [b] \qquad [a] \cap [b] \neq \emptyset.$$

L'ensemble des classes d'équivalences de A définit une **partition** sur A. Réciproquement, étant donnée une partition sur A, il existe une relation d'équivalence dont les classes correspondent à cette partition.

7. Une relation réflexive, *antisymétrique* et transitive est une relation d'**ordre partiel**, notée $\preceq$. Un ensemble S muni d'un ordre partiel $\preceq$ est un **ensemble partiellement ordonné** ou **e.p.o.** $(S, \preceq)$. Si $a \preceq b$ et $a \neq b$ on écrit $a \prec b$. Deux éléments a et b sont **comparables** si soit $a \preceq b$ soit $b \preceq a$. Si tout couple d'éléments est comparable, l'ordre est **total**. Un ordre total R_1 est **compatible** avec un ordre partiel R_2 si $(aR_2b) \Rightarrow (aR_1b)$.

   Soit $(A_1, \preceq_1)$ et $(A_2, \preceq_2)$ deux e.p.o. . L'**ordre lexicographique** sur $A_1 \times A_2$ est défini de la façon suivante: $(a_1, a_2) \prec (b_1, b_2)$ si $a \prec_1 b_1$ ou $a_1 = b_1$ et $a_2 \prec_2 b_2$. Cette définition s'étend à n e.p.o. $(A_1, \preceq_1), \ldots, (A_n, \preceq_n)$.

8. On peut représenter un e.p.o. à l'aide d'un graphe G dont les arcs relient les éléments (sommets) comparables de S. Plusieurs de ces arcs peuvent être éliminés sans perte d'information, en utilisant la transitivité de la relation d'ordre partiel. Ainsi, si (a, b) et (b, c) font partie de G, on a automatiquement $a \preceq c$ et on peut sans danger éliminer l'arc (a, c) de G. Le graphe obtenu après élimination de tous les arc inutiles est appelé **graphe de Hasse**.

9. Un élément u est **maximal** s'il n'existe pas d'élément a tel que $u \preceq a$. Un élément v est **minimal** s'il n'existe pas d'élément b tel que $b \preceq v$. Tout e.p.o. fini non vide possède au moins un élément minimal.

   Un élément u est **maximum** si $a \preceq u$ pour tout a dans S. Un élément v est **minimum** si $v \preceq a$ pour tout a dans S.

   On peut obtenir un ordre total compatible avec un ordre partiel donné en effectuant un **tri topologique**:

procédure tri topologique(S)	
$k \leftarrow 1$	
tant que $S \neq \emptyset$ faire	1. $a_k \leftarrow$ un élément minimal de S
	2. $S \leftarrow S - \{a_k\}$
	3. $k \leftarrow k + 1$
$\{a_1, a_2, \ldots, a_n\}$ est l'ordre total cherché	

Définition: Un e.p.o. $(S, \preceq)$ est **bien ordonné** si tout sous-ensemble de S possède un élément minimum.

CHAPITRE 6: RÉCURRENCE

1. Une **relation de récurrence** est une suite de la forme $a_n = f(a_{n-1}, a_{n-2}, \ldots, a_1, a_0)$. La **suite de Fibonacci** est définie par la récurrence:
$$f_0 = 0 \qquad f_1 = 1 \qquad f_n = f_{n-1} + f_{n-2}.$$
   Une relation de récurrence **homogène de degré** k a la forme
$$a_n = \sum_{i=1}^{k} c_i a_{n-i} \qquad \text{où} \quad c_k \neq 0.$$
   Une telle suite est définie de façon unique par les **conditions initiales**: $a_0, a_1, \ldots, a_{k-1}$.

   Soit $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ une récurrence linéaire du second ordre et $p(r) = r^2 - c_1 r - c_2$ son **polynôme caractéristique**. La solution générique de cette équation de récurrence est donnée par
$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$
   si $p(r)$ possède deux racines distinctes (réelles **ou** complexes) r_1 et r_2, et par
$$a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$$
   si $p(r)$ possède une solution unique r_0. Les conditions initiales permettent de déterminer les coefficients α_1 et α_2.

2. **Diviser pour régner.** Il est parfois efficace de résoudre récursivement un problème en le divisant en n sous-problèmes. La recherche dichotomique (ou recherche binaire) constitue un exemple classique de cette stratégie.

   Soit $f(n)$ le nombre d'opérations requis pour résoudre un problème de taille n. Si l'on divise le problème en a sous-poblèmes de tailles égales à n/b (que l'on supposera entier), la complexité de l'algorithme s'exprime récursivement comme:
$$f(n) = af(n/b) + g(n)$$
   où $g(n)$ est le nombre d'opérations supplémentaires requises pour réduire un problème de taille n à a problèmes de tailles n/b. Le tableau ci-dessous donne la complexité d'algorithmes satisfaisant deux relations de récurrences courantes ($a > 1$, $b > 1$, $c > 0$ et $d > 0$):
$$f(n) = af(n/b) + c \qquad f(n) = \begin{cases} O(n^{\log_b a}) & \text{si } a > 1 \\ O(\log n) & \text{si } a = 1. \end{cases}$$
   Plus généralement:
$$f(n) = af(n/b) + cn^d \qquad f(n) = \begin{cases} O(n^d) & \text{if } a < b^d \\ O(n^d \log n) & \text{si } a = b^d \\ O(n^{\log_b a}) & \text{si } a > b^d\ . \end{cases}$$

CHAPITRE 7: GRAPHES

1. **graphe** $G = (V, E)$: ensemble de sommets $v \in V$ et d'arcs $e \in E$ reliant des couples de sommets de V. On note: $e = (v, w)$ si e relie les sommets v et w.

   graphe orienté: graphe où les arcs ont une direction, c-à-d: $(v, w) \neq (w, v)$.

   graphe non orienté: (v, w) et (w, v) désignent le même arc.

   multigraphe: il peut exister plusieurs copies distinctes d'un même arc (arcs parallèles).

   graphe simple: graphe sans **boucles** c-à-d arcs de la forme (v, v).

   degré d'un sommet: dans un graphe non orienté, le degré d'un sommet est égal au nombre d'arcs qui lui sont incidents. On a: $\sum_{v \in V} \deg(v) = 2|E|$. Dans un graphe orienté, on distingue le $\frac{1}{2}$**-degré intérieur** $\deg^-(v)$, c-à-d le nombre d'arcs ayant v comme **sommet terminal** et le $\frac{1}{2}$**-degré extérieur** $\deg^+(v)$, c-à-d le nombre d'arcs ayant v comme **sommet initial**. On a: $\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E|$.

   chemin: suite de sommets adjacents $v_1, v_2, v_3 \ldots v_{r-1}, v_r$. Un chemin est **simple** si aucun sommet n'est répété.

   cycle: chemin de la forme $v_1, v_2, v_3 \ldots v_{r-1}, v_1$. Un cycle est **simple** si aucun sommet n'est répété, à l'exception du sommet initial v_1.

   circuit: cycle dans un graphe orienté. Un circuit est **simple** si aucun sommet n'est répété, à l'exception du sommet initial v_1.

   graphe connexe: graphe non orienté G où tout couple de sommets est relié par un chemin. Si le graphe non orienté sous-tendant G est connexe, on dit que G est **faiblement connexe**, ou connexe tout simplement.

   graphe fortement connexe: graphe orienté où tout couple de sommets est relié par un chemin.

   graphe bipartite: graphe non orienté où $V = V_1 \cup V_2$, $V_1 \cap V_2 = \emptyset$, et tout arc de G joint un sommet de V_1 à un sommet de V_2.

   graphe complet: K_n: $\forall\ u, v, \in V \times V$, $\exists\ (u, v) \in E$.

   sous-graphe: $G_1 = (V_1, E_1)$ est un sous-graphe de $G = (V, E)$ si $V_1 \subset V$ et $E_1 \subset E$.

   union: l'union de deux graphes G_1 et G_2 est le graphe obtenu en faisant l'union des sommets et des arcs de G_1 et G_2.

   matrice d'adjacence: $a_{ij} = 1$ s'il existe un arc de i à j et $a_{ij} = 0$ sinon. Les éléments de A^r sont égaux au nombre de chemins distincts de longueur r entre les couples de sommets de G.

   matrice d'incidence: (sommets-arcs) d'un graphe sans boucle: matrice $|V| \times |E|$ où chaque colonne correspond à un arc $e = (v, w)$ et comporte deux éléments non nuls: $a_{ve} = -1$ et $a_{we} = +1$. Dans le cas d'un graphe non orienté: $a_{ve} = a_{we} = 1$. Dans le cas d'un multigraphe, toute colonne est multipliée par la multiplicité de l'arc correspondant.

2. Deux graphes $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$ sont **isomorphes** s'il existe une fonction bijective (**isomorphisme**) f de V_1 dans V_2 telle que $(v, w) \in E_1 \iff (f(v), f(w)) \in E_2$. Deux graphes isomorphes ont le même nombre de sommets et d'arcs. De plus, v et $f(v)$ doivent avoir des degrés identiques. S'il existe un chemin (cycle) de longueur k dans G_1, il doit exister un chemin (cycle) de longueur k dans G_2.

3. Un graphe non orienté est **eulérien** s'il possède un cycle simple passant par tous les arcs de G. Un graphe est eulérien si et seulement si tous ses sommets sont de degré pair.

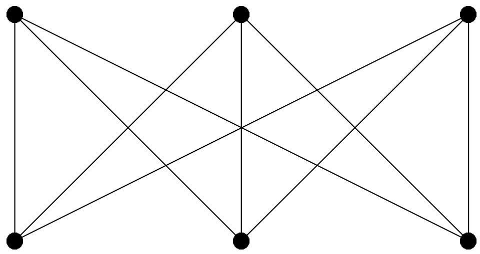
4. Un graphe non orienté $G = (V, E)$ est **hamiltonien** s'il existe un cycle simple passant par tous les sommets du graphe. Si G est connexe, $|V| \geq 3$ et $\deg(v) \geq |V|/2$ pour tout $v \in V$, alors G est hamiltonien.

5. Un graphe G est **planaire** si on peut le "dessiner" dans le plan sans sans qu'il y ait croisement d'arcs. Un graphe planaire divise le plan en régions.

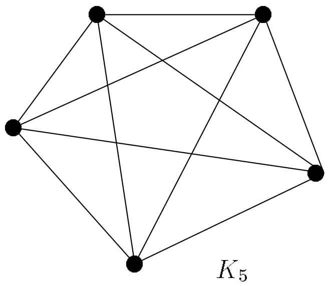
   formule d'Euler: Soit r le nombre (unique) de régions correspondant à une représentation planaire du graphe G. On a: $r = |E| - |V| + 2$.

   Si G est planaire et simple et $|V| \geq 3$, alors $|E| \leq 3|V| - 6$. Si de plus G n'a pas de cycle de longueur 3, alors: $|E| \leq 2|V| - 4$.

Deux graphes sont **homéomorphes** si l'un ne peut être obtenu de l'autre par une suite de **subdivisions élémentaires**, où deux arcs (u, w) et (w, v) sont substitués à l'arc (u, v). Un graphe n'est *pas* planaire si et seulement s'il contient un sous-graphe homéomorphe à $K_{3,3}$ ou K_5. (voir figure ci-dessous)



$K_{3,3}$



K_5

6. Un **coloriage** d'un graphe est obtenu en associant à chaque sommet une couleur de telle sorte que deux sommets adjacents n'aient pas la même couleur. Le **nombre chromatique** d'un graphe est le nombre minimum de couleurs requises pour colorier le graphe.

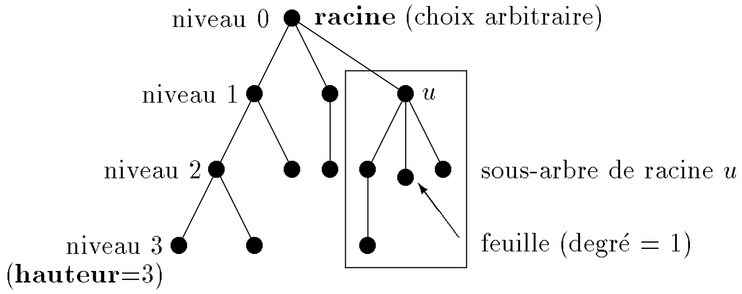
   théorème des quatre couleurs: le nombre chromatique d'un graphe planaire est inférieur ou égal à 4.

7. Dans un cycle, une **corde** est un arc reliant deux sommets non adjacents du cycle. Un graphe est **triangulé** si tout cycle de longueur supérieure ou égale à 4 possède une corde.

   Soit $\mathcal{F}$ une famille d'intervalles $\mathcal{F} = \{I_1, I_2, \ldots, I_r\}$. Un **graphe d'intervalles** est obtenu en associant un sommet v à chaque intervalle I_v et en créant un arc (u, v) si et seulement si les intervalles I_u et I_v ont une intersection non vide. On peut établir que tout graphe d'intervalles est triangulé. La réciproque n'est pas vraie cependant.

CHAPITRE 8: ARBRES

1. Définitions équivalentes:
   - $T = (V, E)$ est un arbre
   - T est connexe et acyclique
   - pour tout couple de sommets (u, v), il existe un et un seul chemin de u à v
   - T est connexe et $|E| = |V| - 1$
   - T est acyclique et $|E| = |V| - 1$



   Si $(v_0, v_1, \ldots, v_n)$ est un chemin dans T, on définit:
   - v_{n-1}: **père** de v_n
   - v_n **enfant** de v_{n-1}
   - $v_0, v_1, \ldots, v_{n-1}$: **ancêtres** de v_n
   - v est un **descendant** de u si u est un ancêtre de v
   - u et v sont **frères** s'ils ont le même père

2. Dans un **arbre binaire**, un sommet possède au plus deux enfants. Tout enfant est soit un **enfant de gauche** soit un **enfant de droite**. Dans un arbre binaire **complet**, tout sommet possède 2 enfants (**sommet interne**) ou aucun enfant (feuille). Si i représente le nombre de sommets internes, alors l'arbre binaire complet possède $i + 1$ feuilles. Si h désigne sa hauteur et t le nombre total de feuilles, alors $t \leq 2^h$.

3. Dans un **arbre de recherche binaire**, les données associées au sous-arbre de gauche sont toutes inférieures aux données du sous-arbre de droite.

4. On peut parcourir un arbre binaire, c'est-à-dire visiter ses sommets, de plusieurs façons différentes. Chaque technique conduit à une représentation de l'arbre comme une suite ordonnée de ses sommets qui se suffit par elle-même; on n'a plus besoin de spécifier les arcs de l'arbre! Les trois techniques principales sont représentées par les algorithmes récursifs suivants:

procédure préordre (T)		
tant que $T \neq \emptyset$ faire	1. visiter la racine	RACINE-GAUCHE-DROITE
	2. préordre (sous-arbre de gauche)	
	2. préordre (sous-arbre de droite)	

procédure ordre (T)		
tant que $T \neq \emptyset$ faire	1. enordre (sous-arbre de gauche)	GAUCHE-RACINE-DROITE
	2. visiter la racine	
	2. ordre (sous-arbre de droite)	

procédure postordre (T)		
tant que $T \neq \emptyset$ faire	1. postordre (sous-arbre de gauche)	GAUCHE-DROITE-RACINE
	2. postordre (sous-arbre de droite)	
	2. visiter la racine	

5. Un **arbre sous-tendant** d'un graphe connexe G est un sous-graphe de G qui est un arbre et possède le même nombre de sommets que G. On peut déterminer un arbre sous-tendant de G en généralisant le parcours en préordre d'un arbre à un graphe connexe quelconque, et en ne conservant que les arcs qui ne forment pas de cycle avec les arcs précédemment insérés dans l'arbre. La technique qui en découle est appelée **recherche en profondeur** d'un graphe.

   On peut également utiliser la **recherche en largeur** où l'arbre sous-tendant est construit par niveaux successifs. Dans l'algorithme qui suit, on suppose que S est une liste ordonnée, c'est-à-dire que ses éléments sont retirés dans l'ordre où ils ont été insérés.

   procédure RechercheEnLargeur $(G = (V, E))$, résultat dans $T = (V_T, E_T)$
   $V_T \leftarrow \{v\} \quad E_T \leftarrow \emptyset \quad S \leftarrow \{v\}$
   tant que $|V_T| < |V|$ faire 1. choisir le premier élément u de S
   2. $S \leftarrow S - \{u\}$
   3. **pour tout** $(u, u') \in E$ faire **si** $u' \notin V_T$ faire
   3.1 $V_T \leftarrow V_T \cup \{u'\}$
   3.2 $S \leftarrow S \cup \{u'\}$
   3.3 $E_T \leftarrow E_T \cup \{(u, u')\}$

CHAPITRE 1: EXEMPLES

1. • p_1: l'équation $x^3 - 7 = 0$ possède une solution unique;

   p_2: il existe une infinité de nombres premiers;

   p_3: $2 + 2 = 2$;

   On a:

   $p_1 = \mathbf{F}$ $\quad p_2 = \mathbf{V}$ $\quad p_3 = \mathbf{F}$

   $\neg p_1 = \mathbf{V}$ $\quad p_1 \vee p_2 = \mathbf{V}$ $\quad p_1 \wedge p_2 = \mathbf{F}$ $\quad p_1 \oplus p_2 = \mathbf{V}$

   $\neg p_1 \vee (p_2 \oplus r) = \mathbf{V}$ $\quad p_2 \rightarrow p_1 = \mathbf{F}$ $\quad p_1 \leftrightarrow \neg p_2 = \mathbf{V}$

   $p \vee \neg p$ est une tautologie; $\neg p \vee q \equiv p \rightarrow q$ (voir table ci-dessous)

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$	$\neg p \vee q \leftrightarrow p \rightarrow q$
V	**V**	**F**	**V**	**V**	**V**
V	**F**	**F**	**F**	**F**	**V**
F	**V**	**V**	**V**	**V**	**V**
F	**F**	**V**	**V**	**V**	**V**

   • Preuve que $(p \wedge q) \rightarrow (p \vee q)$ est une tautologie:

$$\begin{aligned}(p \wedge q) \rightarrow (p \vee q) &\equiv (\neg(p \wedge q)) \vee (p \vee q) \\ &\equiv (\neg p \vee \neg q) \vee (p \vee q) \\ &\equiv (\neg p \vee p) \vee (\neg q \vee q) \equiv \mathbf{V} \vee \mathbf{V} \equiv \mathbf{V}.\end{aligned}$$

   • $0001 \oplus 1101 = 1100$.

2. • Définition de la limite $\lim_{x \to a} f(x) = L$:

$$\forall \epsilon > 0 \quad \exists \delta > 0 \quad \forall x \quad (0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon).$$

   Les variables ϵ, δ et x sont liées. Les variables f, a et L sont libres.

   • $\neg \, \exists x \; \forall y \; P(x, y) \; \equiv \; \forall x \; \neg \, (\forall y \; P(x, y)) \; \equiv \; \forall x \; \exists y \; \neg P(x, y)$.

3. • L'ensemble $\{2, 4, 6, 8\}$ peut aussi s'écrire $\{x \in \mathbb{N} | x \text{ est pair et } x \leq 9\}$.

   • Si $S = \{a, b, c\}$, $2^S = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ et $|2^S| = 2^{|S|} = 2^3 = 8$. Le sous-ensemble $T = \{a, c\}$ de S peut être représenté par la chaîne de bits 101.

4. • Preuve que $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

$$\begin{aligned}\overline{A \cap B} &= \{x | x \notin A \cap B\} = \{x | \neg(x \in A \cap B)\} \\ &= \{x | \neg((x \in A) \wedge (x \in B))\} = \{x | (x \notin A) \vee (x \notin B)\} \\ &= \{x | (x \in \overline{A}) \vee (x \in \overline{B})\} = \{x | x \in (\overline{A} \cup \overline{B})\}.\end{aligned}$$

   Preuve par table d'appartenance:

A	B	$\overline{A \cup B}$	$\overline{A} \cap \overline{B}$
0	0	1	1
0	1	0	0
1	0	0	0
1	1	0	0

   • Si $S = \{a, b, c, d\}$ on peut écrire $\{a, c\} \cap \{a\} = \{a\}$ ou $1010 \wedge 1000 = 1000$.

5. • $f_1(x) = x^3$ est bijective sur $\mathbb{R}$ et $f_1^{-1}(x) = x^{1/3}$.

   $f_2(x) = x^3 - 1$ est surjective sur $\mathbb{R}$.

   $f_3(x) = 1/(1 + x^2)$ est injective sur $\mathbb{R}$; f_3 est bijective comme fonction de $\mathbb{R}^+$ dans $[0, 1)$; son inverse est alors $f_3^{-1}(y) = (-1 + \sqrt{1 + 4y})/(2y)$.

   • Soit la suite $a_n = \lceil n/2 \rceil$. On a: $a_0 = 0$, $a_1 = 0$, $a_2 = 1$, $a_3 = 1$, $a_4 = 2$, etc.

   • $\sum_{j=2}^{5} 3^j = \sum_{j=0}^{3} 3^{j+2} = 9 \sum_{j=0}^{3} 3^j = 9(3^{3+1} - 1)/(3 - 1) = 360$.

6. $\log n! \leq \log n^n = n \log n \quad \Rightarrow \quad \log n! \in O(n \log n)$.

CHAPITRE 2: EXEMPLES

1. L'algorithme suivant (**recherche binaire** ou **recherche dichotomique** détermine la position d'un entier x dans une liste de n entiers ordonnés par ordre croissant $a_1 < a_2 \ldots < a_n$. Si x ne se trouve pas dans la liste, l'algorithme retourne la valeur de position 0.

```
procédure recherche binaire; résultat dans la variable "position"
initialisation: i ← 1   j ← n
tant que i < j faire   m ← ⌊(i + j)/2⌋
                       si x > a_m   alors i ← m + 1
                                    sinon j ← m
si x = a_i alors position← i sinon position← 0
```

Si $n = 2^k$, au plus k évaluations sont requises pour déterminer la position de x. La complexité de l'algorithme de recherche binaire est donc $O(\log n)$.

2. • $17 = 22 \mod 5$ puisque $(17 - 22) \mod 5 = -5 \mod 5 = 0$.
   • $\mathrm{PGCD}(18, 25) = 1 \Rightarrow 18$ et 25 sont premiers entre eux.
   • $(6 \times 7) \mod 4 = ((6 \mod 4) \times (7 \mod 4)) \mod 4 = (2 \times 3) \mod 4 = 2$.
   • $\mathrm{PGCD}(3, 7) = 1$ et $3|7c \Rightarrow 3|c$.
   •

$$\begin{aligned}\mathrm{PGCD}(15,25) &= \mathrm{PGCD}(15, 25 \mod 15) &&= \mathrm{PGCD}(15,10)\\ &= \mathrm{PGCD}(10, 15 \mod 10) &&= \mathrm{PGCD}(10,5)\\ &= \mathrm{PGCD}(5, 10 \mod 5) &&= \mathrm{PGCD}(5,0) = 5\end{aligned}$$

   • $\mathrm{PGCD}(18, 25) = 1$. Cherchons s et t tels que $18s + 25t = 1$. Par l'algorithme d'Euclide on obtient:

$$25 = 1 \times 18 + 7 \quad 18 = 2 \times 7 + 4 \quad 7 = 1 \times 4 + 3 \quad 4 = 1 \times 3 + 1$$

et, en rebroussant chemin:

$$\begin{aligned}1 &= 4 - (7 - 4) = 2 \times 4 - 7\\ &= 2 \times (18 - 2 \times 7) - 7 = 2 \times 18 - 5 \times 7\\ &= 2 \times 18 - 5 \times (25 - 18)\\ &= 7 \times 18 - 5 \times 25.\end{aligned}$$

   • Expression de $(127)_{10}$ en base 4:

$$\begin{aligned}(127/4) &= 31 \quad \text{reste } 3 \Rightarrow a_0 = 3\\ (31/4) &= 7 \quad \text{reste } 3 \Rightarrow a_1 = 3\\ (7/4) &= 1 \quad \text{reste } 3 \Rightarrow a_2 = 3 \quad .\end{aligned}$$

Par conséquent: $(127)_{10} = (1333)_4 = 1 \times 4^3 + 3 \times 4^2 + 3 \times 4^1 + 3 \times 4^0$.

3. • $(10111)_2 + (101011)_2 = (1000010)_2 \qquad (101)_2^2 = (11001)_2$.
   • $31 = [011111]_1 \qquad -25 = [100110]_1$
   • $31+(-25)$: on additionne $(011111)_2$ et $(100110)_2$ pour obtenir $(1000101)_2$ *plus* une retenue sur le bit de gauche. Le résultat est donc: $(1000101)_2 + 1 = (000110)_2$ qui est la représentation de 6 dans le système du complément à 1.
   • $31 = [011111]_2 \qquad -25 = [100111]_2$
   $31 + (-25) = (011111)_2 + (100111)_2 = (000110)_2$, qui est la représentation de 6 dans le système du complément à 2.

4. • Soit $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$. On a: $C = A \odot B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

En particulier: $c_{11} = (1 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 0) = 1$.

Si $\circ = \min$ et $\bullet = \max$ on obtient: $D = A \circ \bullet B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

En particulier: $d_{12} = \min(\max(1,0), \max(0,0), \max(1,1)) = \min(1,0,1) = 0$.

• Si $A:\ 5 \times 2$, $B:\ 2 \times 7$ et $C:\ 7 \times 1$, le calcul du produit ABC par l'algorithme "classique" exige $(2 \times 7 \times 1) + (5 \times 2 \times 1) = 24$ multiplications si l'on choisit l'ordre $A(BC)$ et $(5 \times 2 \times 7) + (5 \times 7 \times 1) = 105$ multiplications si l'on choisit l'odre $(AB)C$.

CHAPITRE 3: EXEMPLES

1. **Théorème 1** *Si $n > 2$ alors $n^2 - 1$ n'est pas un nombre premier.*

   Preuve On a: $n^2 - 1 = (n+1)(n-1)$. Puisque $n > 2$, les deux termes du produits sont distincts et différents de 1. On en conclut que $n^2 - 1$ n'est pas premier (nombre **composé**).

   • L'équivalence $\neg(\forall x \ P(x)) \ \equiv \ \exists x \ \neg P(x)$ permet de démontrer la fausseté de l'assertion $\forall x \ P(x)$ en exhibant un contre-exemple. Ainsi l'assertion

   $$\forall n \in \mathbb{N} \quad 2^n + 1 \quad \text{est premier}$$

   est fausse puisque $2^3 + 1 = 9$ n'est pas un nombre premier.

2. **Théorème 2** *Si $3n + 2$ est impair alors n est impair.*

   Preuve (par contradiction): si n est pair, alors il existe un entier k tel que $n = 2k$ et: $3n + 2 = 6k + 2$ est pair, ce qui contredit l'hypothèse.

   Théorème 3 *$\log_2 3$ est irrationnel.*

   Preuve (par contradiction): supposons que $\log_2 3 = p/q$ où p et q sont entiers. On a alors:

   $$3 = 2^{p/q} \Rightarrow 3^q = 2^p,$$

   ce qui est clairement impossible.

3. **Théorème 4** *Si $1 \leq n \leq 5$ alors $2^n - 1$ est premier ou $2^n + 1$ est premier (ou les deux).*

   Preuve (par cas):
   $n = 1$: $2^1 + 1 = 3$ est premier
   $n = 2$: $2^2 + 1 = 5$ est premier
   $n = 3$: $2^3 - 1 = 7$ est premier
   $n = 4$: $2^4 + 1 = 17$ est premier
   $n = 5$: $2^5 - 1 = 31$ est premier.

4. Démontrons que les trois énoncés suivants sont équivalents:

   $$p_1: \quad n \bmod 3 \neq 0 \qquad p_2: \quad n \not| \ 3 \qquad p_3: \quad n^2 \equiv 1 \bmod 3.$$

   $p_1 \Rightarrow p_2$: $n = 3k + r$ avec $r \neq 0$; par conséquent, n ne peut être divisible par 3
   $p_2 \Rightarrow p_3$: preuve par cas:
   1er cas: $n = 3k + 1 \Rightarrow n^2 = 9k + 6k + 1 \Rightarrow n^2 \equiv 1 \bmod 3$
   2e cas: $n = 3k + 2 \Rightarrow n^2 = 9k + 6k + 3 + 1 \Rightarrow n^2 \equiv 1 \bmod 3$
   $p_3 \Rightarrow p1$: preuve par contradiction: $\neg p_1 \rightarrow \neg p_3$
   $n \bmod 3 = 0 \ \Rightarrow \ n = 3k \ \Rightarrow \ n^2 = 9k \equiv 0 \bmod 3 \neq 1 \bmod 3.$

5. **Théorème 5** *Pour tout entier $n > 1$ il existe une suite de n nombres entiers consécutifs composés.*

   Preuve (constructive): considérons la suite $(n+1)! + 2, \ldots, (n+1)! + (n+1)$. Il est clair que $(n+1)! + i$ est divisible par i, $i = 2, \ldots, n+1$.

   Théorème 6 *Pour tout entier n il existe un nombre premier plus grand que n.*

   Preuve (par contradiction): le nombre $n! + 1$ n'est pas divisible par $2, \ldots, n$. Il doit donc comporter un facteur plus grand que n (il se peut que $n! + 1$ lui-même soit premier, mais pas forcément; par exemple: $4! + 1 = 25$ est divisible par 5 qui est plus grand que 4).

6. Démontrons par induction la proposition $P(n)$: $S_n = \sum_{k=0}^{n} r^k = (1 - r^{n+1})/(1-r)$ si $r \neq 1$.

   Base de l'induction: $P(0)$: $\sum_{k=0}^{0} r^k = r^0 = 1 = (1 - r^{0+1})/(1-r) = 1$

   Induction: $P(n) \Rightarrow P(n+1)$

   $$\begin{aligned} S_{n+1} &= \sum_{k=0}^{n+1} r^k = S_n + r^{n+1} \\ &= \frac{1 - r^{n+1}}{1 - r} + r^{n+1} \qquad \text{puisque } P(n) = \mathbf{V} \\ &= \frac{1 - r^{n+1} + r^{n+1} - r^{n+2}}{1 - r} = \frac{1 - r^{n+2}}{1 - r} \quad \Rightarrow \quad P(n+1) = \mathbf{V}. \end{aligned}$$

7. Définition récursive des nombres de Fibonacci:

$$f_0 = 0 \quad f_1 = 1 \qquad f_n = f_{n-2} + f_{n-1} \qquad \text{si } n \geq 2.$$

On a: $f_2 = f_0 + f_1 = 0 + 1 = 1$, $f_3 = f_1 + f_2 = 1 + 2 = 3$, $f_4 = 3$, $f_5 = 5$, $f_6 = 8$, etc.

CHAPITRE 4: EXEMPLES

1. Une plaque minéralogique est formée de 7 symboles donts les 3 premiers sont des lettres et les quatre suivants des chiffres dont le premier est non nul. Il y a au total: $26 \times 26 \times 26 \times 9 \times 10 \times 10$ combinaisons possibles de plaques distinctes.

2. • Soit

   A_1: nombre de chaînes de 8 bits commençant par 1
   A_2: nombre de chaînes de 8 bits se terminant par 00
   A_3: nombre de chaînes de 8 bits où $b_2 = b_3 = b_5 = b_7 = 0$

   On a:

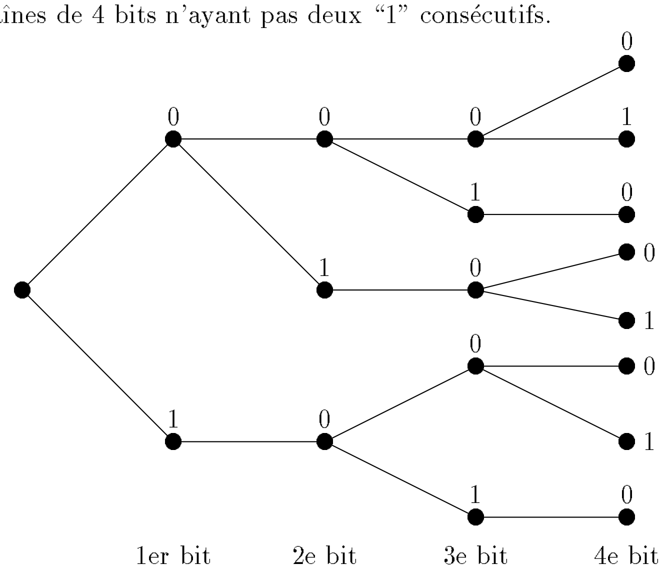
$$\begin{aligned} |A_1 \cup A_2| &= |A_1| + |A_2| - |A_1 \cap A_2| = 2^7 + 2^6 - 2^5 = 160 \\ |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_3 \cap A_1| + |A_1 \cap A_2 \cap A_3| \\ &= (2^7 + 2^6 + 2^4) - (2^5 + 2^3 + 2^3) + (2^2) = 164. \end{aligned}$$

   • Cet exemple repose sur les notions vues aux paragraphes 5 et 7. Un **dérangement** est une permutation laissant aucun élément dans sa position originelle. Soit D_n le nombre de dérangements de n éléments, et dénotons par E_k l'ensemble des permutations laissant en place l'élément k. On a:

$$\begin{aligned} D_n &= n! - |E_1 \cup \ldots \cup E_n| = n! - \Big(\sum_{i=1^n} |E_i| - \sum_{i=1}^{n} \sum_{1 \le j \le n, j>i} |E_i \cap E_j| + \ldots\Big) \\ &= n! - n(n-1)! + \binom{n}{2}(n-2)! - \ldots = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \end{aligned}$$

   La probabilité p_n d'un dérangement est $p_n = D_n/n!$ et l'on a: $\lim_{n\to\infty} p_n = 1/e$.

3. Il y a 8 chaînes de 4 bits n'ayant pas deux "1" consécutifs.



4. Vingt processeurs numérotés de 1 à 20 sont interconnectés (ou non). Soit a_i le nombre de processeurs auxquels le processeur i est connecté. La proposition

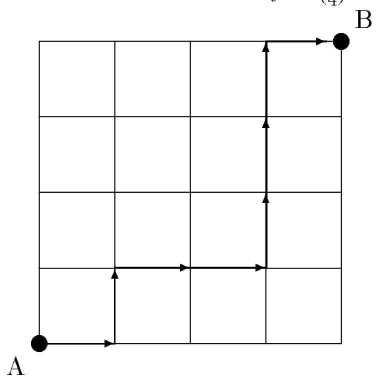
$$\exists i\ \exists j\ a_i = 0\ \wedge\ a_j = 19$$

   est clairement fausse. Par conséquent, la fonction a_i ne peut prendre plus de 19 valeurs distinctes. On en déduit, en appliquant le principe du pigeonnier, qu'il existe deux processeurs i et j ayant le même nombre de connexions, c'est-à-dire tels que $a_i = a_j$.

5. Il y a 10!=3 628 800 façons de disposer 10 personnes autour d'une table.

6. Il y a $10 \times 9 \times 8$ façons de choisir une présidente, une vice-présidente et un secrétaire parmi 10 candidats.

7. Un robot se déplace du point A au point B suivant un plus court chemin (voir figure). Un tel chemin peut s'exprimer sous forme d'une suite de 8 symboles prenant soit la valeur D (Droite) ou H (Haut) et comportant exactement 4 D et 4 H. Il y a $\binom{8}{4} = 70$ parcours distincts possibles.



8. • $2^n = (1+1)^n = \sum_{r=0}^{n} \binom{n}{r} 1^r 1^{n-r} = \sum_{r=0}^{n} \binom{n}{r}$.
   • Le triangle de Pascal d'ordre 4 et les polynômes correspondants sont:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array} \qquad \begin{array}{rc} (1+x)^0 = & 1 \\ (1+x)^1 = & 1+x \\ (1+x)^2 = & 1+2x+x^2 \\ (1+x)^3 = & 1+3x+3x^2+x^3 \\ (1+x)^4 = & 1+4x+6x^2+4x^3+x^4 \end{array}$$

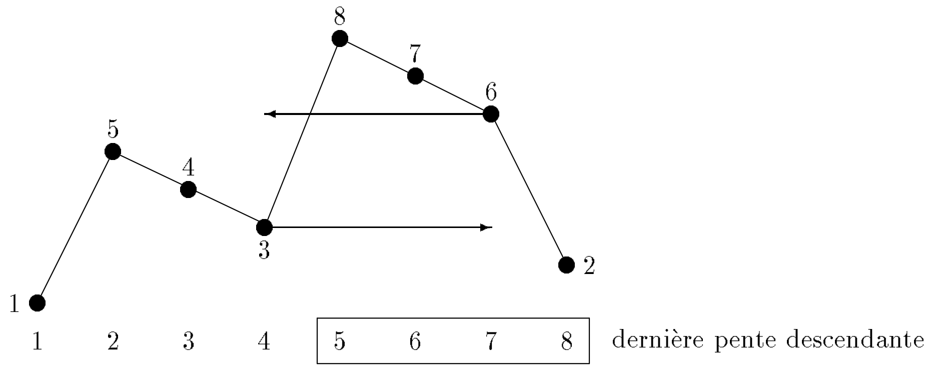
   • On peut former 26^8 mots de huit lettres distincts.

9. • Si l'on ne tient pas compte de l'ordre (comme dans un dictionnaire de Scrabble), il y a $C(26+8-1, 8) = C(33, 8)$ mots de huit lettres possibles.

   • Pour obtenir une solution entière non négative de l'équation $x_1 + x_2 + \ldots + x_n = r$, il suffit de choisir r objets de type $x_1, x_2, \ldots, x_n$ avec répétition. Le nombre de tels choix est $\overline{C}(n, r) = C(n + r - 1, r)$.

10. • Le nombre de permutations distinctes de 9 lettres contenant trois A, deux B et quatre C est égal à $9!/(3!2!4!) = 35 \times 36$.

11. • Examinons le schéma suivant. La permutation 15438762 ne peut être augmentée en conservant l'ordre lexicographique sans toucher à un élément à gauche de la "pente" 8762 (sinon on obtient une permutation plus petite). On échange alors les élément 3 (élément "pivot") et 6 pour obtenir une permutation "un peu plus grande'. On obtient ainsi la permutation 15462378.



- Génération en ordre lexicographique des 6 premières permutations d'ordre 4. L'indice j correspondant au pivot et l'exposant $*$ l'élément qui prend sa place.

$$
\begin{array}{ccccc}
123_j4^* & \to & 124_j3^* & \to & 1243 \\
12_j43^* & \to & 13_j24^* & \to & 1324 \\
132_j4^* & \to & 134_j2^* & \to & 1342 \\
13_j4^*2 & \to & 14_j3^*2 & \to & 1423 \\
142_j3^* & \to & 143_j2^* & \to & 1432
\end{array}
$$

12. Génération de tous les sous-ensembles de A, B, C:

$$
\begin{array}{lcl}
000 & \to & \emptyset \\
001 & \to & \{C\} \\
010 & \to & \{B\} \\
011 & \to & \{B, C\} \\
100 & \to & \{A\} \\
101 & \to & \{A, C\} \\
110 & \to & \{A, B\} \\
111 & \to & \{A, B, C\}.
\end{array}
$$

13. Génération des 10 combinaisons de 3 parmi 5 nombres (les cinq premiers) en ordre lexicographique:

$$
\begin{array}{ccccc}
123 & 124 & 125 & 134 & 135 \\
145 & 234 & 235 & 245 & 345.
\end{array}
$$

CHAPITRE 5: EXEMPLES

1. Soit la relation: aRb si a divise b.
   . R est réflexive si on admet que 0 divise 0
   . R n'est pas symétrique car $2|4$ mai $4 \not| 2$
   . R est antisymétrique: $(a|b) \ \wedge \ (b|a) \ \Rightarrow \ a = b$
   . R est transitive: $(a|b) \ \wedge \ (b|c) \ \Rightarrow \ a|c$.
2. Soit $R = \{(1,2),(2,3),(3,1),(4,4),(3,5)\}$. On a:
   $R^2 = \{(1,3),(2,1),(2,5),(3,2),(4,4)\}$ $\quad R^3 = \{(1,1),(1,5),(2,2),(3,3),(4,4)\}$ $\quad R^4 = \{(1,2),(2,3),(3,1),(3,5),(4,4)\}$.
3. La relation $R = \{(1,0,0),(0,0,1),(1,0,1),(1,1,0)\}$ est une relation ternaire sur $\{0,1\}^3$.

4.5. Soient les relations

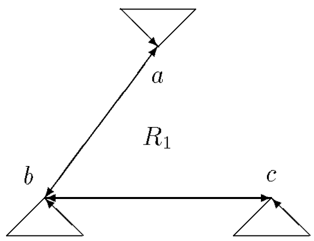
$$\begin{aligned} R_1 &= \{(a,a),(a,b),(b,a),(b,b),(b,c),(c,b),(c,c)\} \\ R_2 &= \{(a,a),(a,c),(b,a),(c,b)\}. \end{aligned}$$

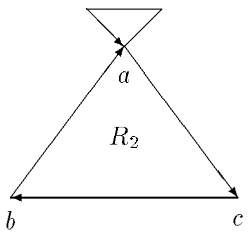
On a:

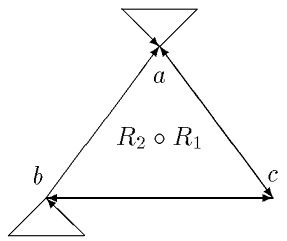
$$M_{R_1} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad M_{R_2} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

La relation R_1 est réflexive (tous les éléments diagonaux de sa représentation matricielle sont égaux à 1), symétrique (M_{R_1} est symétrique), mais ni antisymétrique (il y a des éléments égaux à 1 et symétriques par rapport à la diagonale) ni transitive (aRb et bRc mais $\neg(aRc)$). On a aussi:

$$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, M_{R_1 - R_2} = M_{R_1} - M_{R_2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, M_{R_2 \circ R_1} = M_{R_1} \odot M_{R_2} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$







Soient R', $\overline{R}$ et R^* les fermetures réflexive, symétrique et transitive de R_2, respectivement. On a:

$$M_{R'} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad M_{\overline{R}} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad M_{R^*} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

La fermeture transitive R^* s'obtient en appliquant l'algorithme de Warshall. Posons: $W^{[0]} = R_2$. A l'itération k, la ligne k et la colonne k ne sont pas modifiées. On a ainsi:

$$\begin{aligned} W_{22}^{[1]} &= W_{22}^{[0]} \vee (W_{21}^{[0]} \wedge W_{12}^{[0]}) = 0 \vee (1 \wedge 0)) = 0 \\ W_{23}^{[1]} &= W_{23}^{[0]} \vee (W_{21}^{[0]} \wedge W_{13}^{[0]}) = 0 \vee (1 \wedge 1)) = 1 \\ W_{32}^{[1]} &= 1 \\ W_{33}^{[1]} &= 0. \end{aligned}$$

En continuant de la sorte on obtient les matrices successives:

$$W^{[1]} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad W^{[2]} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad W^{[3]} = W_{R^*} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

6. Représentation matricielle d'une relation d'équivalence R sur l'ensemble $A = \{1, 2, 3, 4, 5\}$:

$$M_R = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

On peut écrire $A = [1]_R \cup [3]_R$ où $[1]_R$ et $[3]_R$ sont les deux classes d'équivalences de la relation R.

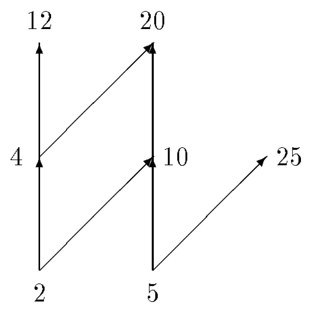
7. • Soit l'ensemble $E = \{1, 2, 3, 4\}$ muni de la relation d'ordre partiel

$$\preceq = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (3,3), (4,4)\}.$$

Le couple $\{E, \preceq\}$ est un e.p.o. . On peut écrire: $2 \preceq 3$. Par contre les éléments 1 et 3 ne sont pas comparables. L'ordre total (1,2,3,4) est compatible avec $\preceq$.

• Soit $E = \{a, b, c, \ldots, y, z\}$ muni de l'ordre alphabétique. Soit $A = E^5$ l'ensemble des mots de 5 lettres. On a: $abac \leq abbd$ selon l'ordre lexicographique.

8.9. Soit $E = \{2, 4, 5, 10, 12, 20, 25\}$ un ensemble muni de l'ordre partiel: $a \preceq b$ si $a|b$. Le diagramme de Hasse de la relation est illustré ci-dessous.



Les éléments 2 et 5 sont minimaux. Les éléments 12, 20 et 25 sont maximaux. Il n'y a ni élément minimum ni élément maximum.

Appliquons la procédure de tri topologique pour obtenir un ordre total compatible avec l'ordre partiel $\preceq$.

$$\begin{array}{ll} S \leftarrow \{2, 4, 5, 10, 12, 20, 25\} & a_1 = 5 \\ S \leftarrow \{2, 4, 10, 12, 20, 25\} & a_2 = 2 \\ S \leftarrow \{4, 10, 12, 20, 25\} & a_3 = 4. \end{array}$$

On peut continuer et obtenir: $a_4 = 10$, $a_5 = 25$, $a_6 = 12$ et $a_7 = 20$. Un ordre total compatible (il n'est pas unique!) est donc $T = (5, 2, 4, 10, 25, 12, 20)$. L'élément minimum de T est 5 et l'élément maximum 20.

CHAPITRE 6: EXEMPLES

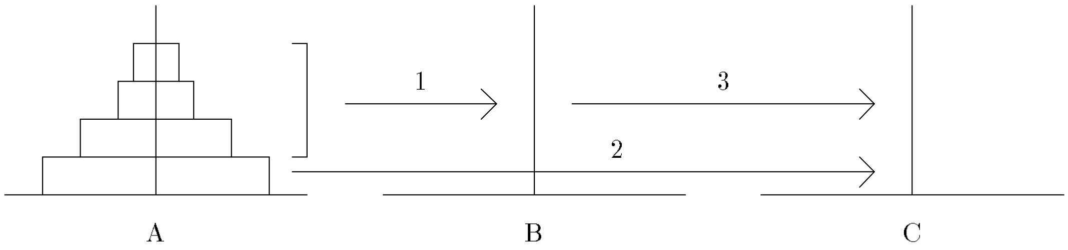
1. • **Intérêt composé**: Soit X_0 un montant d'argent placé à la banque à 5% d'intérêt. On a la relation de récurrence:

$$X_n = X_{n-1} + .05X_{n-1} = 1.05X_{n-1}.$$

C'est une relation de récurrence homogène (il n'y a pas de terme constant) d'ordre 1.

• **la tour de Hanoï**: Ce problème d'origine ancienne consiste à déplacer les n disques de la tour de gauche (A) à l'une des deux tours de droite (B ou C). La stratégie consiste à déplacer les $n-1$ disques supérieurs vers la tour B, à déplace le disque restant en A vers la tour C, puis à déplacer les disques de la tour B à la tour C. Si a_n représente le nombre de déplacements requis, on a la relation de récurrence du premier ordre: $a_n = 2a_{n-1} + 1$, avec la condition initiale $a_1 = 1$. Ceci constitue un cas particulier d'une relation de récurrence du deuxième ordre. On peut cependant retrouver rapidement:

$$\begin{aligned} a_n &= 2a_{n-1} + 1 = 2(2a_{n-2} + 1) + 1 = 4a_{n-2} + 2 + 1 \\ &= 2^{n-k}a_{n-k} + 2^{k-1} - \cdots + 1 \\ &= 2^{n-1}a_1 + 2^{n-2} + \cdots + 2 + 1 \\ &= 2^{n-1} + \cdots + 1 = 2^n - 1. \end{aligned}$$



• Le polynôme caractéristique associé à la suite de Fibonacci est: $p(r) = r^2 - r - 1$, dont les racines sont $(1 \pm \sqrt{5})/2$. On a donc:

$$f_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Puisque $f_0 = 0$ et $f_1 = 1$ on obtient:

$$\alpha_1 + \alpha_2 = 0 \qquad (1+\sqrt{5})\alpha_1 + (1-\sqrt{5})\alpha_2 = 1.$$

La solution de ce système linéaire est $\alpha_1 = 1/2\sqrt{5}$, $\alpha_2 = -1/2\sqrt{5}$. Finalement:

$$f_n = \frac{1}{2\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{2\sqrt{5}} \left(\frac{-1+\sqrt{5}}{2}\right)^n.$$

• Soit la relation de récurrence $a_n = 2a_{n-1} - 2a_{n-2}$ avec les conditions initiales $a_0 = 0$ et $a_1 = 1$. Les racines du polynôme caractéristique $p(r) = r^2 - 2r + 2$ sont $r = 1 \pm i$. On a donc:

$$a_n = \alpha_1(1+i)^n + \alpha_2(1-i)^n.$$

Les conditions initiales permettent d'écrire:

$$\alpha_1 + \alpha_2 = 0 \qquad \alpha_1(1+i) + \alpha_2(1-i) = 1.$$

La solution du système linéaire est: $\alpha_1 = 1/(2i)$, $\alpha + 2 = -1/(2i)$. Ainsi:

$$a_n = \frac{(1+i)^n - (1-i)^n}{2i}.$$

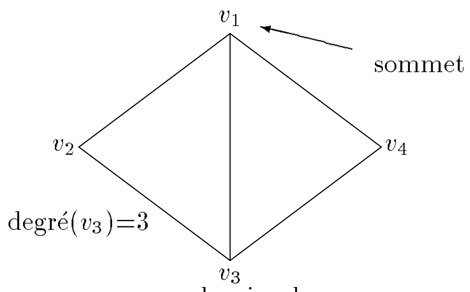
On vérifie aisément que le membre de droite de cette égalité donne toujours un nombre entier.

- Soit la relation de récurrence $a_n = 2a_{n-1} - a_{n-2}$ avec les conditions initiales $a_0 = 1$ et $a_1 = 3$. Le polynôme caractéristique $p(r) = r^2 - 2r + 1 = (r-1)^2$ a une racine double $r = 1$. L'équation de récurrence prend donc la forme: $a_n = \alpha_1 + \alpha_2 n$. Les conditions initiales permettent de déterminer que $\alpha_1 = 1$ et $\alpha_2 = 2$. Ainsi: $a_n = 1 + 2n$.

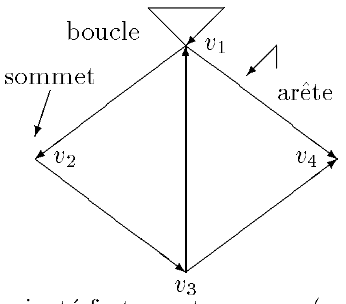
2. Si $f(n) = 2f(n/3) + 3$ alors $f(n) = O(n^{\log_3 2})$.
   Si $f(n) = f(n/2) + 1$ alors $f(n) = O(\log n)$.
   Si $f(n) = 3f(n/2) + n^2$ alors $f(n) = O(n^2)$.
   Si $f(n) = 4f(n/2) + 2n^2$ alors $f(n) = O(n^2 \log n)$.

CHAPITRE 7: EXEMPLES

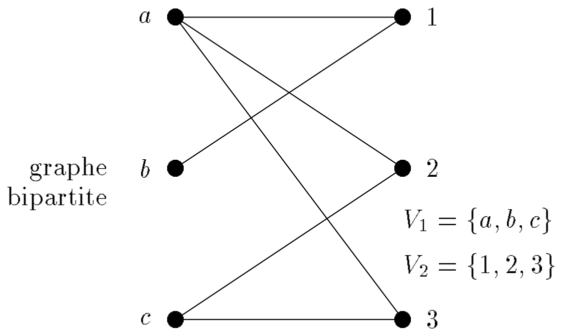
1. •

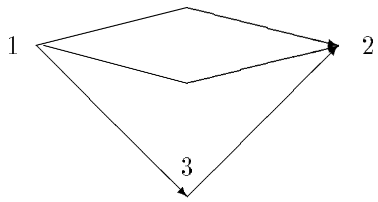


graphe simple
(v_1, v_2, v_3, v_1): cycle



graphe orienté fortement connexe (non simple)
(v_1, v_2, v_3, v_1): circuit
(v_1, v_2, v_3, v_4): chemin simple





multigraphe

- Matrices d'adjacence des deux graphes du haut de cette page:

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \end{array} \qquad \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

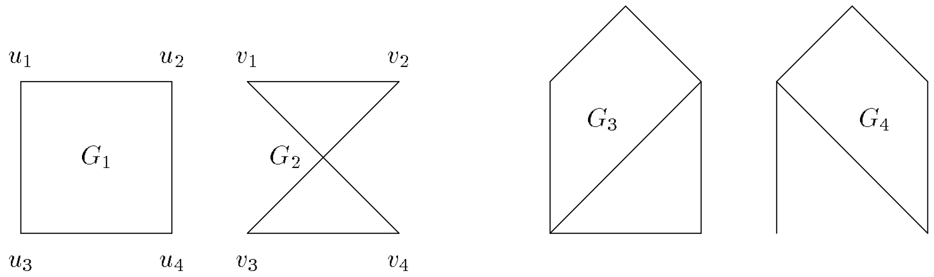
La matrice d'incidence du multigraphe ci-dessus est

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} (1,2) & (1,3) & (3,2) \end{array} \\ \begin{pmatrix} -2 & -1 & 0 \\ +2 & 0 & +1 \\ 0 & +1 & -1 \end{pmatrix} \end{array}$$

2. Dans la figure ci-dessous, G_1 et G_2 sont isomorphes. Un isomorphisme possible (ce n'est pas le seul) est:

$$f(u_1) = v_1 \quad f(u_2) = v_2 \quad f(u_3) = v_4 \quad f(u_4) = v_3.$$

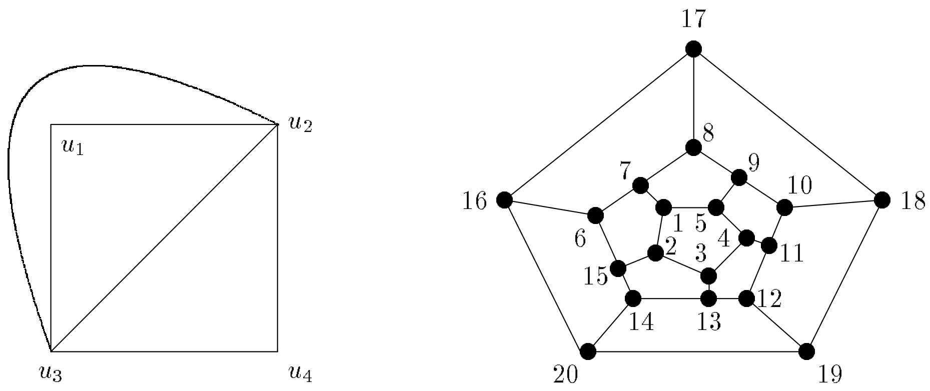
Par contre les graphes G_3 et G_4 ne sont pas isomorphes car il y a un sommet de degré 4 dans G_4 alors qu'il n'y en a pas dans G_3. On observe également qu'il y a un cycle de longueur 4 dans G_3, alors qu'il n'y en a pas dans G_4.



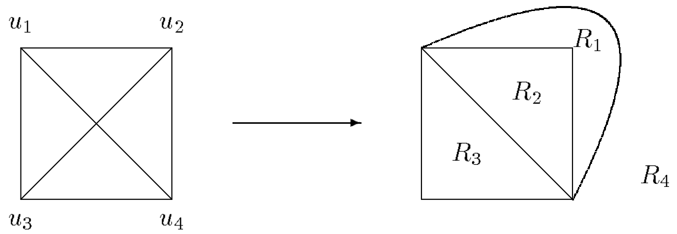
3. Le graphe de gauche ci-dessous est eulérien; $(u_3, u_1, u_2, u_3, u_4, u_2, u_3)$ constitute un cycle d'Euler.

Le graphe de droite est hamiltonien. Un cycle hamiltonien est donné par

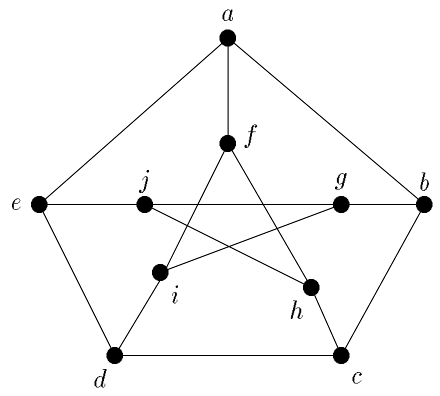
$$(1, 5, 4, 3, 13, 14, 20, 16, 17, 18, 19, 12, 11, 10, 9, 8, 7, 6, 15, 2, 1).$$

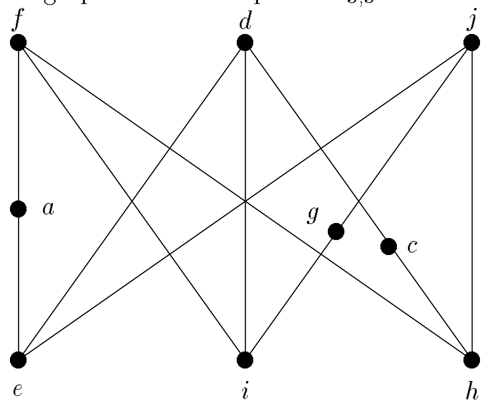


4. Le graphe ci-dessous est planaire. Pour le constater, il suffit de déplacer l'arête (u_1, u_4). On vérifie la formule d'Euler: $4 = |E| - |V| + 2 = 6 - 4 + 2$.

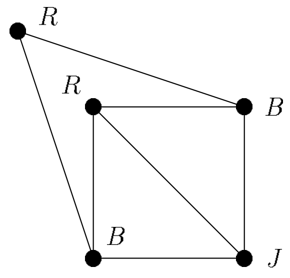


5. Le graphe ci-dessous (gauche) est appelé **graphe de Petersen**. Il est joli, et de plus on peut montrer qu'il n'est pas planaire en montrant qu'il possède un sous-graphe homéomorphe à $K_{3,3}$.





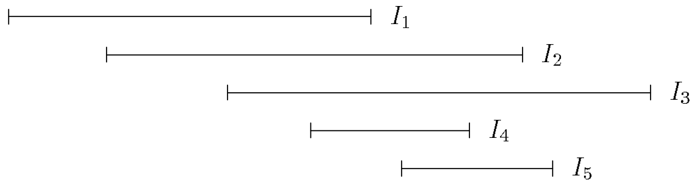
6. Graphe ayant un nombre chromatique égal à 3:

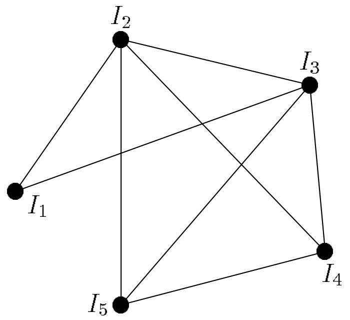


nombre chromatique=3

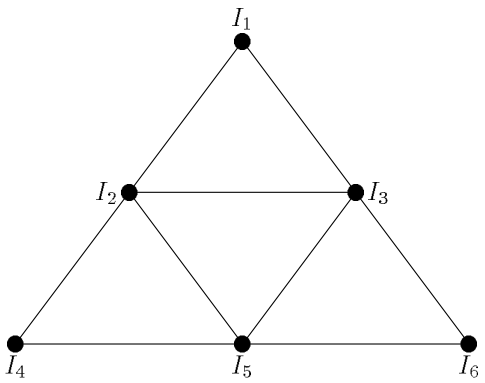
R = Rouge J = Jaune B = Bleu

7. • Une famille d'intervalles et son graphe associé:

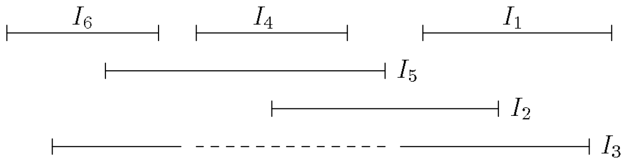




- Il se peut qu'un graphe triangulé ne soit *pas* un graphe d'intervalles:



Essayons en effet de disposer les intervalles I_1 à I_6. I_1 ne peut être situé entre I_4 et I_6 car alors on ne saurait placer I_5. On doit donc place les intervalles disjoints I_4 et I_6 à gauche ou à droite de I_1. Sans perte de généralité, plaçons-les à gauche de I_1. I_4 ne peut se trouver à gauche de I_6 car alors on ne saurait placer I_2. On dispose maintenant les intervalles I_5 et I_2, pour s'apercevoir que I_3 ne peut croiser les intervalles I_1, I_2, I_5 et I_6 sans croiser également I_4.

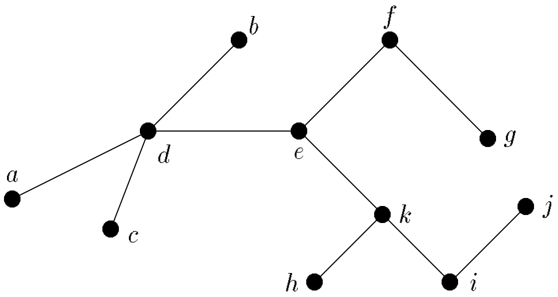


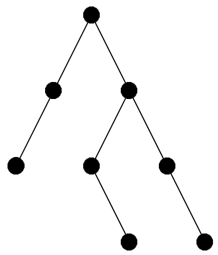
CHAPITRE 8: EXEMPLES

1. Un arbre peut servir à représenter un arbre généalogique, l'organigramme hiérarchique d'une compagnie, etc.

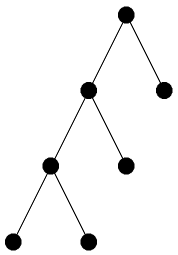
   L'arbre ci-dessous possède une hauteur de 5 si le sommet a est choisi comme racine (le niveau du sommet j est 5) et une hauteur de 3 si le sommet e est choisi comme racine.

   Soit a la racine. Les sommets e et f sont des descendants de d; a et e sont des ancêtres de g; f et k sont frères (ou sœurs).



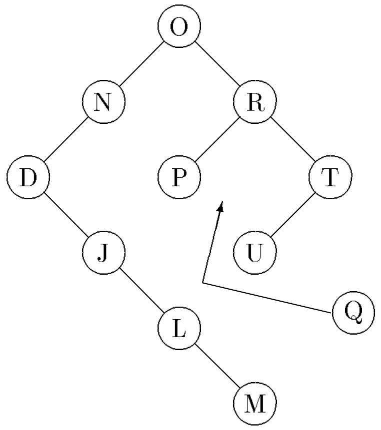


arbre binaire



arbre binaire complet

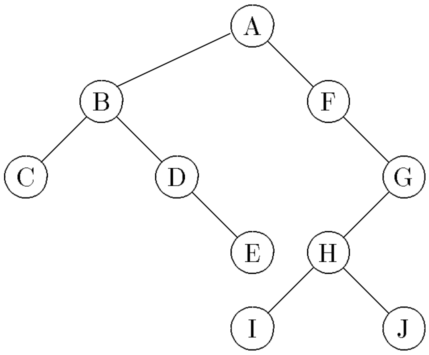
2.



3.

Recherche de la clé J			Insertion de la clé Q		
J<O	→	gauche	Q>O	→	droite
J<N	→	gauche	Q<R	→	gauche
J>D	→	droite	Q>P	→	droite
J=J	→	trouvé!	feuille	→	insérer Q comme fils droit de P

4. •

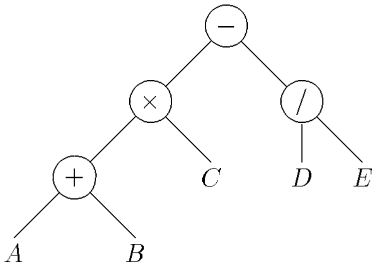


préordre: ABCDEFGHIJ

en ordre: CBDEAFIHJG

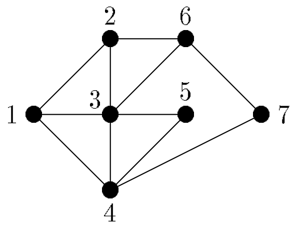
postordre: CEDBIJHGFA

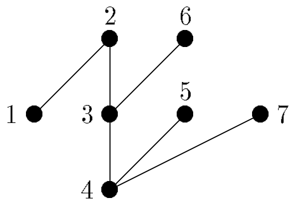
- Soit l'expression complètement parenthésée $(((A + B) \times C) - (D/E))$ et sa représentation à l'aide d'un arbre:

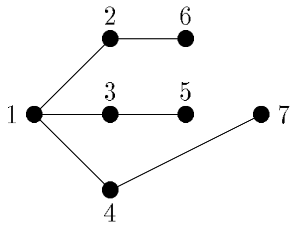


La notation polonaise correspond au préordre $- \times +ABC/DE$ et la notation polonaise inverse au postordre $AB + C \times DE/-$.

5. Les figures ci-dessous représentent un graphe ainsi que deux arbres sous-tendants de ce graphe obtenus par les recherches en profondeur et en largeur, respectivement. (on utilise le sommet 1 comme racine.)







profondeur: 1-2-3-4-5-7-6 largeur: 1-2-3-4-6-5-7