MATHÉMATIQUES DISCRÈTES

Raphaël Alexandre

2 avril 2015

Sommaire

Chapitre 1

Dénombrement

Notation. Soit $n \in \mathbf{N} \setminus \{0\}$. On note

$$[n] = \{1, \dots, n\}.$$

1 Fonctions et sous-ensembles

Rappel. Soient X, Y des ensembles. Une application (ou fonction) de X dans Y est un ensemble de couples $(x, y) \in X \times Y$ tel que tel que pour tout $x \in X$, il existe exactement un couple ayant pour première coordonnée x.

Proposition 1.1
Le nombre d'applications d'un ensemble N à n éléments dans un ensemble M à m éléments est m^n.

Démonstration
Par récurrence sur n. Si $n = 0$ alors $N = \emptyset$. Il existe une seule application et la formule est vérifiée.
On suppose avoir montré la formule pour $|N| = n$. On suppose $|N| = n + 1$.
Soit $a \in N$. Une application f de N dans M est donnée par :
- la valeur de $f(a)$;
- une application de $N \setminus \{a\} \to M$.

Il y a m choix pour la valeur de $f(a)$ et par récurrence, m^n pour l'application de $N \setminus \{a\} \to M$.
En tout, il y a m^{n+1} applications.

Exercice. Combien de mots de longueur 5 sur l'alphabet $\{a, b \dots, z\}$. Réponse : 26^5, c'est le nombre d'applications de $[5]$ dans $\{a, \dots, z\}$.

Proposition 1.2
Soit X à n éléments. Le nombre de sous-ensembles de X est 2^n.

Démonstration
Considérons l'application :

$$\Theta\colon \begin{cases} \mathcal{P}(x) \to \{X \to \{0,1\}\} \\ A \mapsto f_A : x \mapsto \begin{cases} 1 \text{ si } x \in A \\ 0 \text{ sinon} \end{cases} \end{cases}.$$

f_A est appelée fonction caractéristique de l'ensemble A (parfois notée χ_A ou $\mathbf{1}_A$).
Montrons que Θ est une bijection.
- Θ est injective : si $A \neq A'$ il existe $x \in A \Delta A' = (A \setminus A') \cup (A' \setminus A)$ et alors $f_A(x) \neq f_{A'}(x)$.

— Θ est surjective : soit g une application de X dans $\{0,1\}$. Soit

$$A = \{x \in X \mid g(x) = 1\} \subset X.$$

On a bien $g = f_A = \Theta(A)$. Donc g est bien dans l'image de Θ.

Θ est donc bien bijective. On en déduit que

$$|\mathcal{P}(x)| = \left|\{0,1\}^X\right|.$$

Par la proposition précédente,

$$|\mathcal{P}(x)| = |\{0,1\}|^{|X|} = 2^{|X|}.$$

Proposition 1.3

Soit X un ensemble fini non vide. Le nombre de sous-ensembles de X de cardinal pair ou impair est $2^{|X|-1}$.

Démonstration

Soit X tel que $|X| > 0$. Soit $a \in X$. On va définir une bijection entre $\mathcal{P}(X \setminus \{a\})$ et les parties de cardinal pair de X. On pose

$$\Theta \colon \begin{cases} \mathcal{P}(X \setminus \{a\}) \to \{Y \subset X \mid |Y| = 0 \mod 2\} \\ \qquad A \mapsto \begin{cases} A \text{ si } |A| = 1 \mod 2 \\ A \cup \{a\} \text{ si } |A| = 0 \mod 2 \end{cases} \end{cases}.$$

— Θ est injective : si $\Theta(A) = \Theta(A') = B$. B est pair par construction. Si $a \in B$ alors nécessairement $A = A' = B \setminus \{a\}$. Si $a \notin B$ alors $A = A' = B$.

— Θ est surjective. Soit $Y \subset X$. $|Y|$ est pair et alors si $a \in Y$ (resp. n'appartient pas), $Y \setminus \{a\}$ (resp. Y) convient.

Θ est bijective et donc

$$|\mathcal{P}(X \setminus \{a\}| = |\{Y \subset X \mid |Y| = 0 \mod 2\}|.$$

Or

$$|\mathcal{P}(X \setminus \{a\})| = 2^{|X|-1}.$$

De plus

$$|\{Y \subset X \mid |Y| = 1 \mod 2\}| = |\mathcal{P}(x) \setminus \{Y \subset X \mid |Y| = 0 \mod 2\}|$$

et donc il y a

$$2^{|X|} - 2^{|X|-1} = 2^{|X|-1}$$

parties de X de cardinal impair.

Proposition 1.4

Le nombre d'applications injectives de N à $n \geq 0$ éléments dans M à $m \geq 0$ éléments est

$$m(m-1)\dots(m-n+1) = \prod_{i=0}^{n-1}(m-i).$$

Démonstration

Par récurrence sur n.

Si $n = 0$ alors l'application vide est injective et la formule est bien vérifiée.

Supposons que la formule est vraie pour $n \in N$. Supposons que $|N| = n+1$. Soit $a \in \mathbf{N}$. Une application f injective de N dans M est donnée par :

— la valeur de $f(a) \in M$;

— sa restriction $g : N \setminus \{a\} \to M \setminus \{f(a)\}$ injective.

Or il y a m choix de $f(a)$ et par hypothèse de récurrence pour g il y en a

$$\prod_{i=0}^{i=n-1} (m-1-i).$$

Finalement, il y a

$$\prod_{i=-1}^{n-1} (m-1-i) = \prod_{i=0}^{n} (m-i)$$

et donc la formule est vérifiée.

Remarque. Si $n > m$ alors l'un des facteurs est nul (principe des tiroirs).

Définition 1.5
Une permutation de X est une bijection de X sur X.

Exemple. Avec $X = \{a, b, c, d\}$ une permutation est par exemple $p(a) = b, p(b) = c, p(c) = a, p(d) = d$.

Notation. On note une permutation (telle que l'exemple ci-dessus) :

$$p = \begin{pmatrix} a & b & c & d \\ b & c & a & d \end{pmatrix}.$$

Lorsque $X = [n]$, on note aussi

$$p = [a_1, \ldots, a_n]$$

où $p(i) = a_i$ pour tout i.

Exemple.

$$p = [4, 8, 3, 5, 2, 9, 6, 1, 7]$$

signifie

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 3 & 5 & 2 & 9 & 6 & 1 & 7 \end{pmatrix}.$$

Dont les orbites sont

$$\begin{tikzcd} 1 \arrow[r] & 4 \arrow[r] & 5 \arrow[d] \\ & 8 \arrow[ul] & 2 \arrow[l] \end{tikzcd}$$

$$\begin{tikzcd} 3 \arrow[loop right] \end{tikzcd}$$

$$\begin{tikzcd} 6 \arrow[rr] & & 9 \arrow[dl] \\ & 7 \arrow[ul] & \end{tikzcd}$$

Proposition 1.6
Soit X un ensemble fini et $f \in X^X$. f est injective si, et seulement si, f est surjective si, et seulement si, f est bijective.

Le nombre de permutations de X est donc le nombre d'applications injectives de X dans X et donc par la proposition précédente avec $|X| = n$, il y a $n!$ permutations.

2 Coefficients binomiaux

Soient $n \geq k \geq 0$.

Définition 2.1
On définit le coefficient binomial

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Proposition 2.2
$\binom{n}{k}$ est le nombre de sous-ensembles à k éléments d'un ensemble à n éléments.

Démonstration
Soit

$$U = \{(a_1, \ldots, a_k) \mid \forall i \neq j,_i \in X \text{ et } a_j \neq a_i\}.$$

$|U|$ est le nombre d'applications injectives de $[k]$ dans X c'est-à-dire $n(n-1)\ldots(n-k+1)$.
D'après la proposition précédente, pour $\{a_1, \ldots, a_k\}$ fixé avec les a_i distincts il y a $k!$ façons de permuter l'ordre des a_i et donc il y a $k!$ uples dans U.
Finalement, le nombre parties à k éléments est

$$\frac{|U|}{k!} = \binom{n}{k}.$$

Soit X un ensemble, on note

$$\binom{X}{k} := \{Y \subset X \mid |Y| = k\}.$$

On vient de voir

$$\left|\binom{X}{k}\right| = \binom{|X|}{k}.$$

Application. Soient $n, p \geq 0$. Combien y a-t-il de solutions à l'équation

$$x_1 + x_2 + \ldots + x_p = n$$

avec $x_i \in \mathbf{N}$?

Il existe une bijection entre les solutions et les mots de longueur $n+(p-1)$ sur l'alphabet $\{|, \circ\}$ avec n « $\circ$ » et $p-1$ « $|$ ». Or il y a exactement

$$\binom{n+p-1}{n}$$

mots de telle sorte.

Proposition 2.3

$$\binom{n}{k} = \binom{n}{n-k}.$$

Proposition 2.4 (Triangle de Pascal)

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Démonstration

$$\begin{aligned}&\frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!}\\ &= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left[\frac{1}{n-k} + \frac{1}{k}\right] = \frac{n!}{k!(n-k)!}.\end{aligned}$$

Démonstration
Soit X de cardinal $n \geq 1$. Soit $a \in X$.
Les parties à k éléments de X on en a $\binom{n}{k}$.
Or, les parties à k éléments de X contenant a il y en a $\binom{n-1}{k-1}$ et des parties à k éléments de X ne contenant pas a il y en a $\binom{n-1}{k}$.

Théorème 2.5 (Formule du binôme de Newton)

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

Démonstration
On regarde le produit

$$(a+b)(a+b)\dots(a+b).$$

Il y a 2^n termes si l'on développe. Il y a $\binom{n}{k}$ manières d'avoir $a^k b^{n-k}$ puisque cela revient à sélectionner a dans k facteurs parmi les n.

Démonstration
Par récurrence.
Pour $n = 1$ on a bien

$$(a+b)^1 = \sum_{k=0}^{1} \binom{n}{k} a^k b^{n-k} = a + b.$$

Si c'est vérifié pour $n \in \mathbf{N}$ alors pour $n+1$:

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n(a+b)\\
(a+b)^{n+1} &= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right)(a+b)\\
(a+b)^{n+1} &= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}\\
(a+b)^{n+1} &= \binom{n}{0} a^0 b^{n+1} + \binom{n}{n} a^{n+1} b^0 + \sum_{k=1}^{n} a^k b^{n+1-k} \left(\binom{n}{k} + \binom{n}{k-1}\right)\\
(a+b)^{n+1} &= \binom{n}{0} a^0 b^{n+1} + \binom{n}{n} a^{n+1} b^0 + \sum_{k=1}^{n} a^k b^{n+1-k} \binom{n+1}{k}\\
(a+b)^{n+1} &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.
\end{aligned}$$

3 Estimations

Le but du chapitre est d'avoir un ordre de grandeur de $n!$, des coefficients binomiaux : savoir les comparer à des fonctions simples.

3.1 La fonction factorielle

On a un premier encadrement naïf :

$$2^{n-1} \leq n! \leq n^n.$$

Pour rendre cette estimation meilleure on peut partager en deux parties le produit :

$$n! = 1 \cdot 2 \cdots \frac{n}{2}\left(\frac{n}{2}+1\right) \cdots n \leq \left(\frac{n}{2}\right)^{n/2} n^{n/2} = \frac{n^n}{2^{n/2}} = \left(\frac{n}{\sqrt{2}}\right)^n$$

et

$$n! \geq \left(\frac{n}{2}\right)^{n/2} = \frac{n^{n/2}}{2^{n/2}} = \left(\sqrt{\frac{n}{2}}\right)^n.$$

Théorème 3.1
Pour tout $n \geq 1$:

$$e\left(\frac{n}{2}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n.$$

Démonstration
Par récurrence sur n :

— Pour la majoration.

1. Pour $n = 1$ c'est vérifié.
2. Au rang $n+1$:

$$\begin{aligned}(n+1)! = (n+1)n! &\leq (n+1)en\left(\frac{n}{e}\right)^n \\ &\leq e(n+1)\left(\frac{n+1}{e}\right)^{n+1}\left(\frac{e}{n+1}\right)^{n+1} n\left(\frac{n}{e}\right)^n\end{aligned}$$

Il s'agit de montrer que

$$\alpha = \left(\frac{e}{n+1}\right)^{n+1} n\left(\frac{n}{e}\right)^n$$

est plus petit que 1.

$$\alpha = \left(\frac{e}{n+1}\right)^{n+1} n\left(\frac{n}{e}\right)^n$$
$$\alpha = e\left(\frac{n}{n+1}\right)^{n+1}$$
$$\alpha = e\left(\frac{n+1-1}{n+1}\right)^{n+1}$$
$$\alpha = e\left(1-\frac{1}{n+1}\right)^{n+1},$$

$$\begin{aligned}\alpha \leq 1 &\iff e\left(1-\frac{1}{n+1}\right)^{n+1} \leq 1 \\ &\iff \left(1-\frac{1}{n+1}\right)^{n+1} \leq 1/e \\ &\iff 1-\frac{1}{n+1} \leq e^{\frac{-1}{n+1}}.\end{aligned}$$

Mais comme $x \mapsto \exp x$ est convexe, elle est au-dessus de sa tangente en tout point. En particulier au point $-1/(n+1)$ on a l'inégalité voulue.

— Pour la minoration :

1. C'est encore vrai pour $n = 1$.
2. Au rang $n+1$:

$$\begin{aligned}(n+1)! = (n+1)n! \geq (n+1)e\left(\frac{n}{e}\right)^n \\ &\geq e\left(\frac{n+1}{e}\right)^{n+1}(n+1)\left(\frac{n}{e}\right)^n\left(\frac{e}{n+1}\right)^{n+1} \\ &\geq e\left(\frac{n+1}{e}\right)^{n+1} e\left(\frac{n}{n+1}\right)^n.\end{aligned}$$

On cherche donc à montrer que

$$\beta = e\left(\frac{n}{n+1}\right)^n \geq 1.$$

$$\begin{aligned}\beta \geq 1 &\iff e \geq \left(\frac{n+1}{n}\right)^n \\ &\iff e \geq \left(1+\frac{1}{n}\right)^n \\ &\iff e^{1/n} \geq 1 + \frac{1}{n}\end{aligned}$$

Ce qui est à nouveau toujours vrai car c'est l'inégalité de convexité au point $x = 1/n$.

Démonstration

On peut montrer cette fois par comparaison entre séries et intégrales.

$$\ln(n!) = \sum_{i=1}^{n} \ln(i) \leq \int_1^{n+1} \ln t \,\mathrm{d}t = (n+1)\ln(n+1) - (n+1) + 1$$

Ainsi,

$$\begin{aligned}n! &\leq e^{(n+1)\ln(n+1)-n} \\ n! &\leq \frac{(n+1)^{n+1}}{e^n} \\ n! = n(n-1)! &\leq n\frac{n^n}{e^{n-1}} = en\left(\frac{n}{e}\right)^n.\end{aligned}$$

Pour l'autre inégalité, on commence par remarquer que :

$$\ln(n!) \geq \int_1^n \ln t \,\mathrm{d}t = n\ln n - n + 1.$$

Et alors on a bien

$$n! \geq e^{n\ln n - n + 1} = \frac{n^n}{e^{n-1}} = e\left(\frac{n}{e}\right)^n.$$

3.2 Les coefficients binomiaux

On a en première estimation :

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq n^k.$$

Théorème 3.2
Pour $n \geq 1$ et $1 \leq k \leq n$. On a :

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

Démonstration
On a :

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i.$$

Pour $x > 0$ et en tronquant à l'ordre k :

$$\sum_{i=0}^{k} \binom{n}{i} x^i \leq (1+x)^n$$
$$\sum_{i=0}^{k} \binom{n}{i} \frac{x^i}{x^k} \leq \frac{(1+x)^n}{x^k}.$$

Mais pour $x \in]0,1[$ on a

$$\sum_{i=0}^{k} \binom{n}{i} \leq \sum_{i=0}^{k} \binom{n}{i} \left(\frac{1}{x}\right)^{k-i} \leq \frac{(1+x)^n}{x^k}.$$

Si on regarde

$$f(x) = \frac{(1+x)^n}{x^k}$$

cette fonction est dérivable sur $]0,1[$ et

$$f'(x) = \frac{n(1+x)^{n-1}x^k - (1+x)^n k x^{k-1}}{x^{2k}}.$$

f' s'annule en x_0 tel que

$$nx_0 - k(1+x_0) = 0$$
$$x_0[n-k] = k$$
$$x_0 = \frac{k}{n-k} = \frac{k}{n(1-k/n)}.$$

f atteint sont minimum local en x_0.

$$\binom{n}{k} \leq \left(1+\frac{k}{n}\right)^n \left(\frac{n}{k}\right)^k.$$

On veut donc montrer que

$$\left(1+\frac{k}{n}\right)^n \leq e^k.$$

Or c'est équivalent à :

$$\left(1+\frac{k}{n}\right)^{n/k} \leq e \iff 1+\frac{k}{n} \leq e^{k/n}$$

et c'est la même inégalité de convexité que précédemment.

Remarque. On a :

$$\binom{n}{k+1} = \binom{n}{k}\frac{n-k}{k+1}$$

et donc pour $k < n/2$ on a $k \leq n/2 - 1/2$ et donc $n - k \geq 2k + 1 - k \geq k + 1$ et donc

$$\binom{n}{k+1} \geq \binom{n}{k}.$$

Si $k \geq n/2$ on a $(n-k)/(k+1) \geq 1$ et donc

$$\binom{n}{k+1} \leq \binom{n}{k}.$$

On s'intéresse dans la suite au terme $\binom{n}{\lfloor n/2 \rfloor}$ qui est le plus grand coefficient. On a comme premier encadrement :

$$\frac{1}{n+1}2^n \leq \binom{n}{\lfloor n/2 \rfloor} \leq 2^n.$$

Proposition 3.3
On a :

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}.$$

Démonstration
On pose

$$\alpha = \frac{1}{2^{2m}}\binom{2m}{m}$$

et on veut montrer que

$$\frac{1}{2\sqrt{m}} \leq \alpha \leq \frac{1}{\sqrt{2m}}.$$

$$\begin{aligned}
\alpha &= \frac{1}{2^{2m}}\frac{(2m)!}{m!m!} \\
\alpha &= \frac{(2m)(2m-1)\cdots 1}{(2m)(2m-2)\cdots 2(2m)(2m-2)\cdots 2} \\
\alpha &= \frac{(2m-1)(2m-3)(2m-5)\cdots 1}{2m(2m-2)(2m-4)\cdots 2}.
\end{aligned}$$

— Pour la majoration on remarque :

$$\begin{aligned}
A &= \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{4^2}\right)\cdots\left(1 - \frac{1}{(2m)^2}\right) \\
A &= \left(1 - \frac{1}{2}\right)\left(1 + \frac{1}{2}\right)\left(1 - \frac{1}{4}\right)\left(1 + \frac{1}{4}\right)\cdots\left(1 - \frac{1}{2m}\right)\left(1 + \frac{1}{2m}\right) \\
A &= \frac{1\cdot 3}{2\cdot 2}\cdot\frac{3\cdot 5}{4\cdot 4}\cdots\frac{(2m-1)(2m+1)}{2m\cdot 2m} \\
A &= \alpha^2(2m+1).
\end{aligned}$$

Or $A \leq 1$ donc $\alpha^2 \leq 1/(2m+1)$ et donc

$$\alpha \leq \frac{1}{2m+1} \leq \frac{1}{2m}.$$

— Pour la minoration on remarque :

$$B = \left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\cdots\left(1 - \frac{1}{(2m-1)^2}\right)$$
$$B = \frac{2\cdot 4}{3\cdot 3}\frac{4\cdot 6}{5\cdot 5}\cdots\frac{(2m-2)(2m)}{(2m-1)(2m-1)}$$
$$B = \frac{1}{\alpha^2}\frac{1}{2(2m)}.$$

Mais $B \leq 1$ et donc

$$\alpha \geq \frac{1}{2\sqrt{m}}.$$

4 Le principe d'inclusion-exclusion

On a

$$A \cup B = (A \setminus B) \sqcup (A \cap B) \sqcup (B \setminus A)$$

et donc

$$|A \cup B| = |A \setminus A| + |A \cap B| + |B \setminus A| = |A| + |B| - |A \cap B|.$$

On a de même :

$$|A \cup B \cup C| = |A| + |B| + \mathrm{C} - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Théorème 4.1
Soient $A_1, \ldots, A_n$ des ensembles finis,

$$\left|\bigcup_{i=1}^n A_i\right| = \sum_{k=1}^n (-1)^{k+1} \sum_{\substack{I\subset[n]\\|I|=k}} \left|\bigcap_{i\in I} A_i\right|$$
$$\left|\bigcup_{i=1}^n A_i\right| = \sum_{\substack{I\subset[n]\\I\neq\emptyset}} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right|.$$

Démonstration (Par récurrence)
Par récurrence sur n. Pour $n = 1, 2$ c'est vérifié.

Pour $n \geq 2$:

$$\begin{aligned}
\left|\bigcup_{i=1}^{n+1} A_i\right| &= \left|\left(\bigcup_{i=1}^{n} A_i\right) \cup A_{n+1}\right| \\
&= \left|\bigcup_{i=1}^{n} A_i\right| + |A_{n+1}| - \left|\left(\bigcup_{i=1}^{n} A_n\right) \cap A_{n+1}\right| \\
&= \sum_{\substack{I\subset[n] \\ I\neq\emptyset}} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right| + |A_{n+1}| - \left|\bigcup_{i=1}^{n} (A_i \cap A_{n+1})\right| \\
&= \sum_{\substack{I\subset[n+1] \\ n+1\notin I}} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right| + |A_{n+1}| - \sum_{\substack{I\subset[n] \\ I\neq\emptyset}} (-1)^{|I|+1} \left|\bigcap_{i\in I} (A_i \cap A_{n+1})\right| \\
&= \sum_{\substack{I\subset[n+1] \\ n+1\notin I}} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right| + |A_{n+1}| + \sum_{\substack{I\subset[n] \\ I\neq\emptyset}} (-1)^{|I|+2} \left|\bigcap_{i\in I\cup\{n+1\}} A_i\right| \\
&= \sum_{\substack{I\subset[n+1] \\ n+1\notin I}} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right| + |A_{n+1}| + \sum_{\substack{I'\subset[n+1] \\ \{n+1\}\subsetneq I'}} (-1)^{|I'|+1} \left|\bigcap_{i\in I'} A_i\right| \\
&= \sum_{\substack{I\subset[n+1] \\ n+1\notin I}} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right| + \sum_{\substack{I'\subset[n+1] \\ (n+1)\in I'}} (-1)^{|I'|+1} \left|\bigcap_{i\in I'} A_i\right| \\
&= \sum_{\substack{I\subset[n+1] \\ I\neq\emptyset}} (-1)^{|I|+1} \left|\bigcap_{i\in I} A_i\right|.
\end{aligned}$$

Démonstration (Avec les fonctions caractéristiques)
On pose

$$A = \bigcup_{i=1}^{n} A_i$$

et on définit

$$\chi_{A_i} : \begin{cases} A \to \{0,1\} \\ x \mapsto \begin{cases} 1 \text{ si } x \in A_i \\ 0 \text{ sinon} \end{cases} \end{cases}$$

Soit $a \in A$,

$$\prod_{i=1}^{n} (1 - \chi_{A_i}(a)) = 0.$$

On a :

$$\begin{aligned}
\prod_{i=1}^{n} (1 - X_i) &= \sum_{I\subset[n]} (-1)^{|I|} \prod_{i\in I} X_i \\
&= 1 + \sum_{\substack{I\subset[n] \\ I\neq\emptyset}} (-1)^{|I|} \prod_{i\in I} X_i.
\end{aligned}$$

Ainsi, pour $a \in A$,

$$0 = \prod_{i=1}^{n} (1 - \chi_{A_i}(a)) = 1 + \sum_{\substack{I\subset[n] \\ I\neq\emptyset}} (-1)^{|I|} \prod_{i\in I} \chi_{A_i}(a).$$

On somme cette expression sur les $a \in A$:

$$\begin{aligned} 0 &= |A| + \sum_{a \in A} \sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|} \prod_{i \in I} \chi_{A_i}(a) \\ &= |A| + \sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|} \sum_{a \in A} \prod_{i \in I} \chi_{A_i}(a). \end{aligned}$$

Or

$$\prod_{i \in I} \chi_{A_i} = \chi_{\bigcap_{i \in I} A_i}$$

et donc :

$$\sum_{a \in A} \prod_{i \in I} \chi_{A_i}(a) = \left| \bigcap_{i \in I} A_i \right|.$$

Donc :

$$0 = |A| + \sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|$$

$$|A| = \sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|.$$

Application 1. Nombre, $N_{n,p}$, de surjections de $[n]$ sur $[p]$.

1. Si $p > n$ alors $N_{n,p} = 0$.
2. Supposons $p \leq n$. On pose pour $i \in [p]$ l'ensemble A_i des applications qui n'atteignent pas i. L'union
$$\bigcup_{i \in [p]} A_i$$
est l'ensemble des applications non injectives. En particulier,
$$N_{n,p} = p^n - \left| \bigcup_{i \in [p]} A_i \right|.$$
$$\left| \bigcup_{i=1}^{p} A_i \right| = \sum_{\substack{I \subset [p] \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|.$$
De plus $\bigcap_{i \in I} A_i$ est l'ensemble des applications de $[n]$ dans $[p] \setminus I$. Mais
$$\left| \bigcap_{i \in I} A_i \right| = (p - |I|)^n.$$

Ainsi,

$$\begin{aligned}
N_{n,p} &= p^n - \left(\sum_{\substack{I \subset [p] \\ I \neq \emptyset}} (-1)^{|I|+1} (p - |I|)^n \right) \\
N_{n,p} &= p^n - \sum_{k=1}^{p} (-1)^{k+1} \sum_{I \in \binom{[p]}{k}} (p-k)^n. \\
N_{n,p} &= p^n + \sum_{k=1}^{p} (-1)^k \binom{p}{k} (p-k)^n \\
N_{n,p} &= \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^n \\
N_{n,p} &= \sum_{k=1}^{p} (-1)^{p-k} \binom{p}{k} k^n.
\end{aligned}$$

Application 2. Le nombre de permutations sans point fixe $[n]$. On pose A_i l'ensemble des permutations qui laissent fixe i. On cherche

$$N_n = n! - \left| \bigcup_{i=1}^{n} A_i \right|.$$

On a

$$\left| \bigcup_{i \in [n]} A_i \right| = \sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|.$$

De plus, $\bigcap A_i$ est l'ensemble des permutations qui fixent chaque $i \in I$. Or

$$\left| \bigcap_{i \in I} A_i \right| = (n - |I|)!.$$

Ainsi,

$$\begin{aligned}
N_n &= n! - \sum_{\substack{I \subset [n] \\ I \neq \emptyset}} (-1)^{|I|+1} (n - |I|)! \\
N_n &= n! - \sum_{k=1}^{n} (-1)^{k+1} \sum_{I \in \binom{[n]}{k}} (n-k)! \\
N_n &= n! - \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)! \\
N_n &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \\
N_n &= \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k!.
\end{aligned}$$

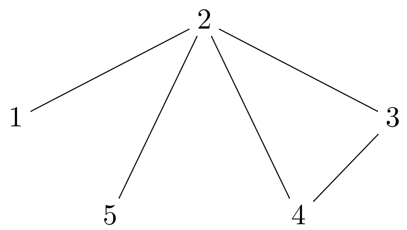
Chapitre 2

Graphes

1 Graphes non orientés

> Définition 1.1
> Un *graphe* est un couple (V, E) avec E un ensemble de pairs de V. V est *l'ensemble des sommets* et si $\{x, y\} \in E$ alors c'est une *arête reliant x à y* (distincts).
> Si $e = \{u, v\}$ on dit que u et e sont *adjacents* et que u est *voisin* de v.

Représentation d'un graphe.



Avec

$$V = \{1, 2, \ldots, 5\}, \ E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{2, 4\}, \{2, 5\}\}.$$

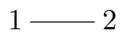
Graphes usuels.

— Pour $n \geq 1$, le *graphe complet* à n sommets, K_n. On a alors $V = [n]$ et $E = \{\{i, j\} \mid 1 \leq i < j \leq n\}$.

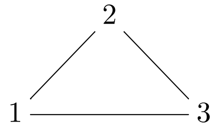
1. K_1 :

   1

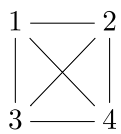
2. K_2 :



3. K_3 :

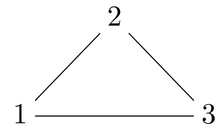


4. K_4 :

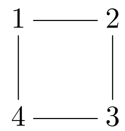


Pour $n \geq 3$, les *cycles* à n sommets, C_n.

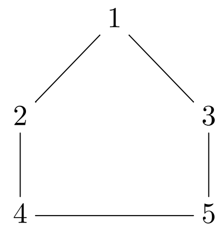
1. C_3 :



2. C_4 :



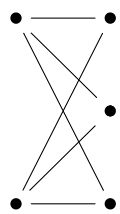
3. C_5 :



— Pour $n \geq 0$, le chemin de longueur n, P_n.
— Pour $n, p \geq 1$, le *graphe biparti complet* $K_{n,p}$. Avec $K_{n,p} = (V, E)$ on a

$$V = \{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_p\}\ ,\ E = \{\{a_i, b_j\} \,|\, i \in [n],\ j \in [p]\}\ .$$

$K_{2,3}$:



DÉFINITION 1.2
$G = (V, E)$ est *biparti* s'il existe une partition de V, $V_1 \cup V_2$ telle que

$$E \subset \{\{u_1, u_2\} \,|\, u_1 \in V_1,\ u_2 \in V_2\}\ .$$

DÉFINITION 1.3
$G(V, E)$ et $G' = (V', E')$ sont égaux si $V = V'$ et $E = E'$.

DÉFINITION 1.4
$G = (V, E)$ et $G' = (V', E')$ sont *isomorphes* s'il existe $f : V \to V'$ bijective telle que

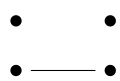
$$\forall u, v \in V,\ \{u, v\} \in E \iff \{f(u), f(v)\} \in E'$$

On note $G \cong G'$.

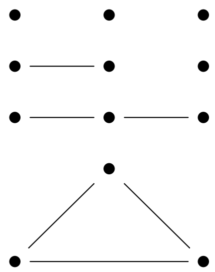
Combien existe-t-il de graphes non isomorphes à n sommets ?

1. Pour $n = 1$ il n'y en a qu'un :

2. Pour $n = 2$:



3. Pour $n = 3$:



Combien de graphes non isomorphes sur $V = [n]$?
Il y a $\binom{n}{2}$ pairs de sommets. Il y a donc

$$2^{\binom{n}{2}}$$

graphes. On a un encadrement du nombre de graphes non isomorphes, N_n :

$$n \leq N_n \leq 2^{\binom{n}{2}}.$$

Si G est un graphe sur $[n]$ alors il y a au plus $n!$ graphes isomorphes à G. Et donc :

$$\frac{2^{\binom{n}{2}}}{n!} \leq N_n \leq 2^{\binom{n}{2}}$$

Définition 1.5
Soit $G = (V, E)$ un graphe. Le *degré* d'un sommet $v \in V$ est :

$$\mathrm{d}_G(v) = |\{u \in V \mid \{u, v\} \in E\}|.$$

1.1 Sous-graphes

Définition 1.6
Soit $G = (V, E)$ un graphe.

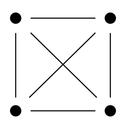
— Soit $V' \subset V$ et soit $E' := E \cap \binom{V'}{2}$, c'est-à-dire :

$$E' = \big\{\{u, v\} \in E \,\big|\, u, v \in V'\big\}.$$

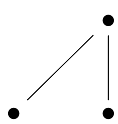
Le graphe $G' = (V', E')$ est appelé un *sous-graphe induit* de G.

— Soit $V' \subset V$ et $E' \subset \binom{V'}{2}$. Le couple $G' = (V', E')$ est appelé un *sous-graphe partiel* de G.

Exemple. K_4 :



A un sous-graphe partiel de K_4, $K_{1,2}$:



Mais $K_{1,2}$ n'est pas un sous graphe induit de K_4.

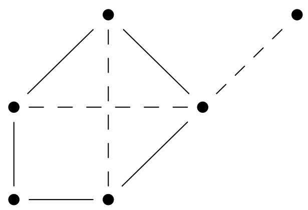
Définition 1.7
Soit $G = (V, E)$ un graphe.
Une *chaine élémentaire* est une suite $(v_0, v_1, \ldots, v_t)$ avec :

1. les v_i tous distincts ;
2. $\{v_i, v_{i+1}\} \in E$ pour tout $i \leq t$.

Un *cycle élémentaire* est une suite $(v_0, v_1, \ldots, v_t)$ avec :

1. $v_0, v_1, \ldots, v_{t-1}$ tous distincts ;
2. $v_0 = v_t$;
3. $\{v_i, v_{i+1}\} \in E$ pour tout i.

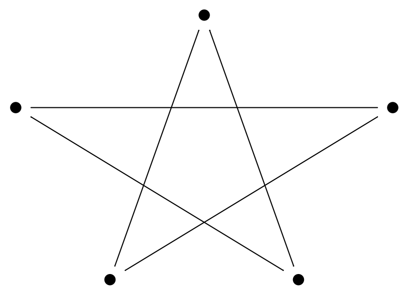
Exemple. Cycle élémentaire :



1.2 Connexité

Définition 1.8
Soit $G = (V, E)$ est connexe si pour tout $x, y \in V$ il existe une chaine élémentaire de x à y.

Remarque. (x) est une chaine élémentaire de x à x. Le graphe :



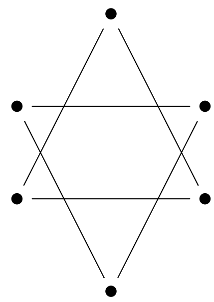
est connexe.

Définition 1.9
On pose $x \sim y$ s'il existe une promenade de x à y.
Une promenade de v_0 à v_t est une suite $(v_0, \ldots, v_1, v_t)$ avec $\{v_i, v_{i+1}\} \in E$.

Proposition 1.10
$\sim$ est une relation d'équivalence.

Définition 1.11
Comme (x) est une promenade, c'est une relation réflexive.
Si $x \sim y$ avec la promenade $(x, v_1, \ldots, v_{t-1}, y)$ alors la promenade $(y, v_{t-1}, \ldots, v_1, x)$ montre que $y \sim x$.
Si $x \sim y$ via $(x, v_1, \ldots, v_{t-1}, y)$ et $y \sim z$ via $(y, w_1, \ldots, w_{q-1}, z)$ alors la promenade $(x, v_1, \ldots, v_{t-1}, y, w_1, \ldots, w_{q-1}, z)$ montre que $x \sim z$.

Remarque. G est connexe si $V/\sim$ a une seul classe. Les classes d'équivalences sont appelées composantes connexes de G. Le graphe :



a deux composantes connexes.

1.3 Distance

Définition 1.12
Soit $G = (V, E)$ un graphe connexe et soient $v, v' \in V$. On note $\mathrm{d}_G(v, v')$ la longueur de la chaine élémentaire la plus courte de v à v' (appelée distance de v à v').

Proposition 1.13
d_G est une distance.

Démonstration
On a bien :

1. pour tous x, y, $\mathrm{d}_G(x, y) \geq 0$;
2. pour tous x, x' on a $\mathrm{d}_G(x, x') = 0$ si, et seulement si, $x = x'$;
3. pour tous x, y, $\mathrm{d}_G(x, y) = \mathrm{d}_G(y, x)$;
4. pour tous x, y, z on a l'inégalité triangulaire : $\mathrm{d}_G(x, z) \leq \mathrm{d}_G(x, y) + \mathrm{d}_G(y, z)$.

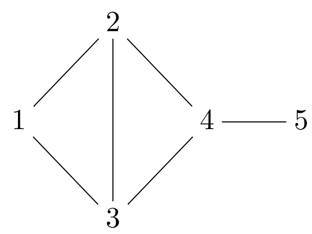
1.4 Matrice d'adjacence d'un graphe

Soit $G = (V, E)$ un graphe avec $V = \{v_1, \ldots, v_n\}$.

Définition 1.14
La matrice d'adjacence de G est la matrice A_G de taille $n \times n$ définie par :

$$a_{i,j} = \begin{cases} 1 \text{ si } \{v_i, v_j\} \in E \\ 0 \text{ sinon.} \end{cases}$$

Exemple. Avec :



on a :

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

Remarque. A_G est symétrique et avec des 0 sur la diagonale.

Proposition 1.15
Le nombre

$$\left(A_G^k\right)_{i,j}$$

est le nombre de promenades de v_i à v_j de longueur k.

Démonstration
Pour $k = 0$ on a bien $A_G^0 = I_d$.
Pour $k+1$, une promenade v_i à v_j de longueur $k+1$ se décompose en une promenade de longueur k de v_l à v_j et une promenade de longueur 1 de v_i à v_l.

$$v_i \longrightarrow v_l \overset{k}{\leadsto} v_j$$

Ainsi, le nombre de promenades de longueur $k+1$ de v_i à v_j est

$$\begin{aligned} &\sum_{v_l \mid \{v_i, v_l\} \in E} (A_G^k)_{l,j} \\ &= \sum_{l \in [n]} (A_G)_{i,l} (A_G^k)_{l,j} \\ &= (A_G A_G^k)_{i,j} = (A_G^{k+1})_{i,j}. \end{aligned}$$

Corollaire 1.16

$$\mathrm{d}_G(v_i, v_j) = \min_k \left\{ (A_G^k)_{i,j} \neq 0 \right\}.$$

1.5 Sur les degrés

Soit $G = (V, E)$ un graphe.

Proposition 1.17

$$\sum_{v \in V} \deg(v) = 2\,|E|$$

Proposition 1.18
Tout graphe a un nombre pair de sommets de degré impair.

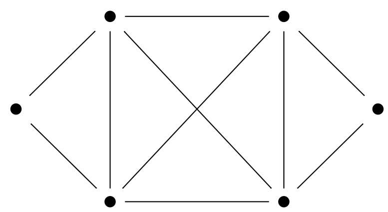
Démonstration
En effet,

$$\begin{aligned}\sum_{v\in V} \deg(v) &\equiv 2\,|E| = 0 \mod 2 \\ &\equiv \sum_{\substack{v\in V\\ \deg(v)\text{ pair}}} \deg(v) + \sum_{\substack{v\in V\\ \deg(v)\text{ impair}}} \deg(v) \equiv |\{v \in V \mid \deg V = 1 \mod 2\}|\,.\end{aligned}$$

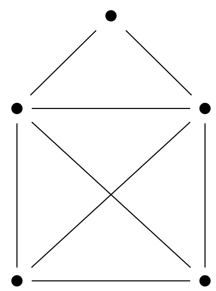
1.6 Graphe eulérien

Définition 1.19
Un graphe est eulérien si on peut le dessiner sans lever le stylo, en revenant au point de départ, sans repasser sur une arête.

Exemple.



est eulérien.



n'est pas eulérien.

Proposition 1.20
$G = (V, E)$ est un graphe eulérien si, et seulement si, tous les sommets sont de degrés pairs et si G est connexe.

Démonstration
Une promenade simple est une suite $(v_0, \ldots, v_t)$ avec $\{v_i, v_{i+1}\} \in E$ pour tout i et pour tous $i \neq j$ on a

$$\{v_i, v_{i+1}\} \neq \{v_j, v_{j+1}\}\,.$$

Une promenade simple est fermée si $v_0 = v_t$.
G est eulérien si, et seulement si, il existe une promenade simple fermée qui passe par toutes les arrêtes.
Si G est eulérien alors on a $(v_0, \ldots, v_0)$ qui est une promenade simple. De plus, pour chaque sommet, on entre et on sort le même nombre de fois. Comme on voit chaque arrête exactement une fois, le degré de chaque sommet est pair.
Réciproquement, si $G = (V, E)$ est tel que $\deg(v)$ est pair pour tout sommet v alors on considère $(v_0, v_1, \ldots, v_m)$ une promenade simple de longueur maximale. On va montrer que cette promenade est un cycle eulérien.

— Si $v_0 \neq v_m$ alors on est entré dans v_m une fois de plus qu'on en est sorti et comme $\deg v_m$ est pair, la promenade n'est pas maximal.

— Supposons qu'il existe $w \in V$ qui ne soit pas dans la promenade. On considère $(w, w_1, \ldots, w_l, v_p)$ une chaine de longueur minimale de w à $\{v_0, \ldots, v_n\}$ (qui existe car G connexe). Mais alors $(v_p, \ldots, v_0, \ldots, v_p, w_l, w_{l-1}, \ldots, w)$ est une promenade simple plus longue.

— Supposons qu'il existe une arrête $\{v_i, v_j\}$ pas dans la promenade. Alors la promenade simple $(v_i, \ldots, v_0, \ldots, v_i, v_j)$ est plus longue.

Donc la promenade est bien un cycle eulérien.

2 Graphe orienté

Définition 2.1
Soit $G = (V, E)$ un graphe avec $E \subset V \times V$. Les éléments de E sont appelés *arcs*. Un arc de type (v, v) est appelé bouclette. [§1]

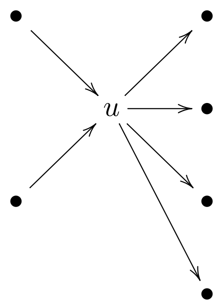
Définition 2.2
Soit $G = (V, E)$ un graphe orienté. Le graphe non orienté sous-jacent est $\tilde{G} = (V, \tilde{E})$ avec
$$\tilde{E} = \{\{u, v\} \mid (u, v) \in E\}\,.$$

Définition 2.3
Soit $G = (V, E)$ un graphe orienté.

— Le degré sortant de $u \in V$ est :
$$\mathrm{d}^+(u) = |\{v \in V \mid (u, v) \in E\}|\,.$$

— Le degré entrant de $u \in V$ est :
$$\mathrm{d}^-(u) = |\{v \in V \mid (v, u) \in E\}|\,.$$

Exemple.

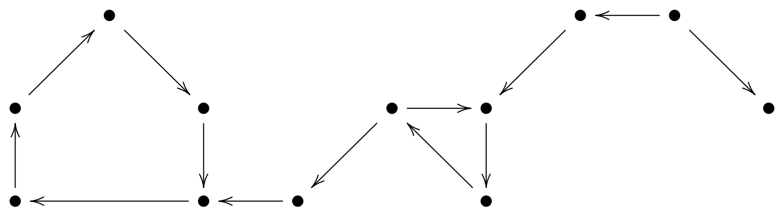


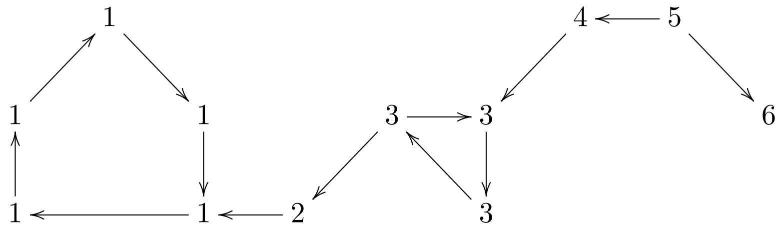
on a
$$\mathrm{d}^+(u) = 4,\ \mathrm{d}^-(u) = 2.$$

Définition 2.4
Soit $G = (V, E)$ orienté. On définit $x \sim y$ s'il existe un chemin de x à y et un chemin de y à x.

§1. Sauf mention du contraire, on considère des graphes simples (sans bouclette).

> Proposition 2.5
> $\sim$ est une relation d'équivalence.





> Définition 2.6
> Les classes d'équivalences sont les composantes fortement connexes de G.

> Définition 2.7
> $G = (V, E)$ est eulérien s'il existe un cycle passant exactement une fois par chaque arête.

> Proposition 2.8
> $G = (V, E)$ orienté est eulérien si, et seulement si, le graphe sous-jacent de G est connexe et si pour tout $v \in V$, $\mathrm{d}^+(v) = \mathrm{d}^-(v)$.

Application. Digicode et code de longueur 5. Quelle est la longueur minimum d'un mot qui ouvre toutes les portes. On a

$$12^5 + 4 \leq l \leq 12^5 \cdot 5.$$

On considère le graphe $G = (V, E)$ avec $V = \{0, 1, \ldots, 9, A, B\}^4 = \Sigma^4$ les mots de longueur 4. On pose

$$E = \{(a_1a_2a_3a_4, a_2a_3a_4a_5)e \,|\, a_i \in \Sigma\}.$$

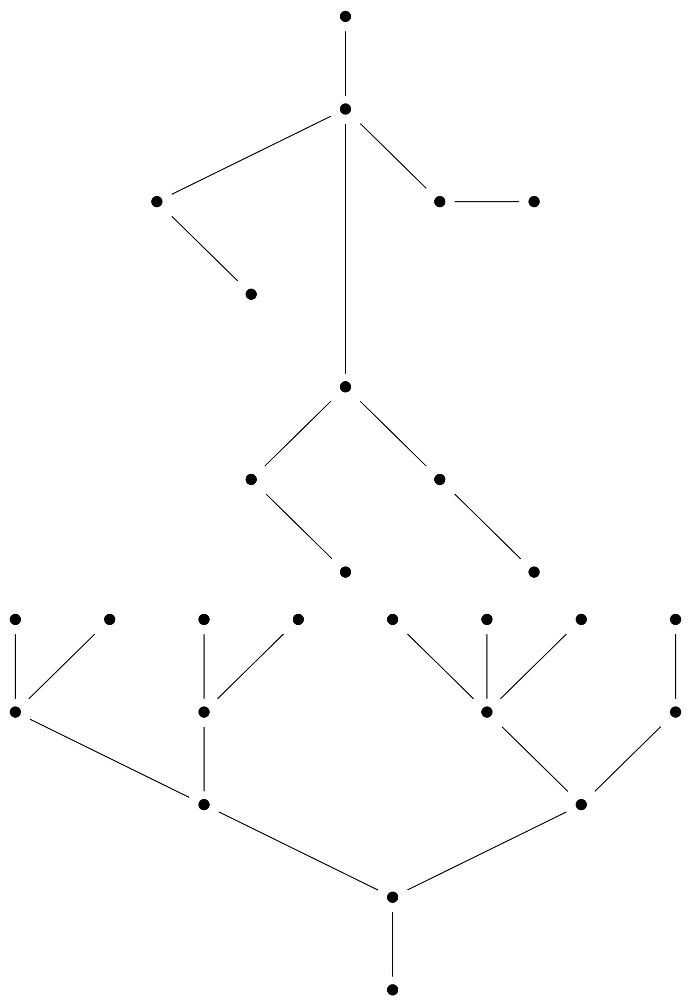
$$1A27 \xrightarrow{5} A275$$

Ce graphe est eulérien. En effet, le graphe sous-jacent est connexe et pour tout $v \in V$, $d^+(v) = 12 = d^-(v)$. Il existe donc un cycle eulérien et donc un mot de longueur $12^5 + 4$ qui ouvre toutes les portes.

3 Arbres

> Définition 3.1
> Un arbre est un graphe connexe sans cycle.

Exemples.



Théorème 3.2 (Caractérisation des arbres)
Pour un graphe $G = (V, E)$ les conditions suivantes sont équivalentes :

1. G est un arbre ;
2. pour tous $x, y \in V$ il existe un unique chemin élémentaire de x à y ;
3. G est connexe minimal ;
4. G est sans cycle maximal ;
5. G est connexe et $|V| = |E| + 1$.

Définition 3.3
Un sommet de degré 1 d'un graphe est appelé *feuille* (ou *sommet pendant*).

Lemme 3.4 (De la feuille)
Tout arbre à au moins deux sommets possède au moins deux feuilles.

Démonstration
Soit $v_0, v_1, \ldots, v_t$ un chemin élémentaire de longueur maximale. On a $t \geq 1$ car notre graphe a au moins deux sommets et est connexe.
Supposons que $\deg(v_0) > 1$. Soit $v' \in \Gamma(v_0) \setminus \{v_1\}$.

— Soit $v' \in \{v_2, \ldots, v_t\}$ est alors on a un cycle : $(v_0, \ldots, v_1, v_0)$.
— Soit $v' \notin \{v_2, \ldots, v_t\}$ ce qui est absurde car $v', v_0, \ldots, v_t$ serait une chaine élémentaire plus longue.

Donc $\deg(v_0) = 1$ donc v_0 est une feuille et on applique le même raisonnement à v_t.

REMARQUE.
- P_n pour $n \geq 1$ n'a que deux feuilles.
- Un graphe sans cycle connexe infini n'a pas nécessairement de feuille.

LEMME 3.5 (De l'arbre qui croît)
Soient $G = (V, E)$ un graphe, $v \in V$ une feuille de G. G est un arbre si, et seulement si, $G \setminus \{v\}$ est un arbre.

DÉMONSTRATION
Si G est sans cycle alors $G \setminus \{v\}$ également. G est encore connexe parce qu'un chemin passant par v doit s'y arrêter puisque $\deg v = 1$. Donc G est connexe.
Si $G \setminus \{v\}$ est un arbre alors il est connexe. On considère v' l'unique voisin de v dans G. Pour $x, y \in V \setminus \{v\}$ il existe un chemin de x à y dans $G \setminus \{v\}$ donc dans G. Pour $x \in V \setminus \{v\}$ il existe un chemin de x à v' dans $G \setminus \{v\}$ donc un chemin de x à v dans G. De plus, G n'a pas de cycle passant par v car $\deg v = 1$.

DÉMONSTRATION (Théorème 3.2 de caractérisation des arbres)
On va montrer l'équivalence de la propriété 1. avec les autres par récurrence sur le nombre de sommets. Pour $n = 1$ toutes les propriétés sont vérifiées.
Supposons $n \geq 2$. Soit $G = (V, E)$ un arbre à n sommets. Comme $n \geq 2$, G possède une feuille, v, et $G \setminus \{v\}$ est un arbre à $n - 1$ sommets. Mais par hypothèse de récurrence, $G \setminus \{v\}$ vérifie les quatre autres propriétés. Il reste à montrer qu'en rajoutant v les propriétés sont encore vraies.

2. Pour tous x, y, il y a un unique chemin de x à y dans $G \setminus \{v\}$, de même dans G. Si v' est l'unique voisin de v dans G alors il y a un unique chemin de x à v' et donc de x à v dans G.
3. v est de degré 1 donc G est encore connexe minimal.
4. G est sans cycle maximal puisque v ne peut pas créer de cycle.
5. En posant $G \setminus \{v\} = (V', E')$ on a $|V'| = |E'| + 1$ mais donc dans G, $|V| = |V'| + 1 = |E'| + 2 = |E| + 1$.

Réciproquement,

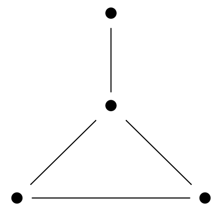
2. G est connexe puisqu'il existe un chemin entre tous points. Si G possède un cycle alors il est décomposable en deux chemins distincts, ce qui est impossible.
3. G est connexe par hypothèse. Supposons que G possède un cycle C. Soit e une arrête du cycle, $G \setminus \{e\}$ est encore connexe, impossible par hypothèse. Donc G est sans cycle, c'est un arbre.
4. G est sans cycle par hypothèse. Si G est non connexe, on rajoute une arrête $\{u, v\}$ où u et v sont dans deux composantes connexes disjointes et alors G est encore sans cycle. Donc G est connexe, c'est un arbre.
5. G est connexe on a alors $\deg(v) \geq 1$ pour tout sommet v. Comme
$$\sum_{v \in V} \deg(v) = 2|E| = 2|V| - 2$$
on a
$$\overline{\deg} = \frac{\sum \deg(v)}{|V|} < 2$$
donc il existe une feuille v_0 de degré 1.
Si v est une feuille de G et $(V', E') = G \setminus \{v\}$ alors $|V'| = |E'| + 1$ et $G \setminus \{v\}$ connexe donc par hypothèse de récurrence $G \setminus \{v\}$ est arbre mais donc G aussi.

4 Graphes planaires

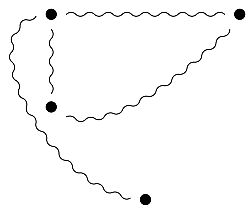
Il s'agit des graphes que l'on peut dessiner dans le plan sans que les arrêtes ne se croisent.

Un sommet v est représenté par $\alpha(v) \in \mathbf{R}^2$ et une arrête $\{u, v\}$ est représentée par un arc, une fonction continue $\theta : [0,1] \to \mathbf{R}^2$ avec $\theta(0) = \alpha(u)$, $\theta(1) = \alpha(v)$ et θ injective.

Exemple. Avec le graphe



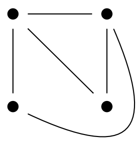
on a aussi dans le plan



donc ce graphe est planaire.

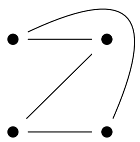
Exercice. Les graphes suivants sont-ils planaires :

— K_4, oui :

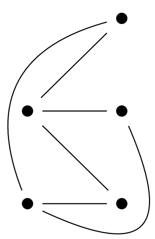


— K_5 ?

— $K_{2,2}$, oui :



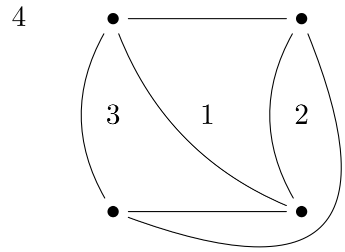
— $K_{2,3}$, oui :



— $K_{3,3}$?

> Théorème 4.1 (Jordan)
> Une courbe fermée dans le plan délimite deux régions : l'une bornée et l'autre non bornée.

Le dessin d'un graphe planaire dans le plan définit des régions. Par exemple avec K_4 :



Proposition 4.2 (Formule d'Euler)
Soit $G = (V, E)$ un graphe planaire connexe non vide. On considère un dessin de G dans le plan délimitant F régions. On a :

$$|V| - |E| + F = 2$$

et en particulier F ne dépend pas du dessin.

Démonstration
On procède par récurrence sur $|E|$.

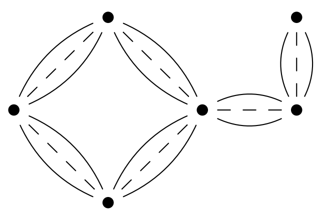
— Si $|E| = 0$ alors $|V| - |E| + F = 1 - 0 + 1 = 2$.

— Supposons $|E| > 0$.

1. Si $G = (V, E)$ est sans cycle alors G est un arbre et $F = 1$. Mais on a aussi $|V| = |E|+1$ donc $|V| - |E| + F = 2$.
2. Supposons que $G = (V, E)$ possède un cycle C. Soit e une arrête de ce cycle. Le graphe $G' = (V', E') = G \setminus \{e\}$ délimite F' régions et vérifie $|V'| - |E'| + F' = 2$ par hypothèse de récurrence. Or $|E'| = |E| - 1$ et $F' = F - 1$. Donc $|V| - |E| + F = 2$.

Proposition 4.3
K_5 et $K_{3,3}$ ne sont pas planaires.

Remarque. Si (V, E) est connexe à au moins 3 sommets. Alors en découpant chaque arrête en deux sur la longueur, chaque région est en contact avec au moins 3 demi-arrêtes. Il y a $2|E|$ arrêtes et ce nombre est au moins égal à $3F$. Donc $2|E| \geq 3F$.



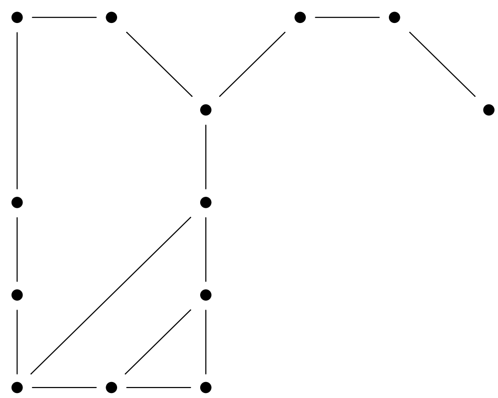
Démonstration
Dans l'ordre :

— Pour K_5, on a $|V| = 5$ et $|E| = \binom{5}{2} = 10$. Si on pouvait dessiner K_5 dans le plan, le nombre de région serait égal à $2 - 5 + 10 = 7$. Mais d'après la remarque précédente, on aurait $20 \geq 21$, absurde. Donc K_5 n'est pas planaire.

— Pour $K_{3,3}$, on a $|V| = 6$ et $|E| = 9$ donc $F = 2 - |V| + |E| = 5$.
Mais $K_{3,3}$ est un graphe biparti donc tout cycle est de longueur paire. Il y a au moins 4 demi-arêtes autour de chaque région. Donc $2|E| \geq 4F$ mais ici on a $2|E| = 18 < 4F = 20$.

DÉFINITION 4.4
Un *mineur* d'un graphe est obtenu par une suite d'opérations :
— supprimer un sommet ;
— supprimer une arête ;
— contracter une arête (fusionner x, y pour $\{x, y\} \in E$).

EXEMPLE.



C_8 est mineur de ce graphe.

PROPOSITION 4.5
Un mineur d'un graphe planaire est planaire

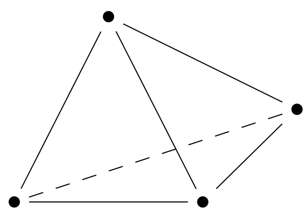
THÉORÈME 4.6 (KURATOWSKI 1930)
G est planaire si, et seulement si, $K_{3,3}$ et K_5 ne sont pas mineurs de G.

5 Solides platoniciens

Un polytope de $\mathbf{R}^3$ (ou polyèdre) est une intersection de demi-espaces.

Un polyèdre est régulier si chaque face est le même polygone régulier (à rotation/-translation près).

Liste des polyèdres réguliers :
— le tétraèdre ;



— le cube ;
— l'icosaèdre (20 face triangulaires).

Le graphe donné par les faces est :
— planaire ;
— régulier.

On définit n le nombre de sommets, m celui des arêtes et le solide a f faces. Chaque sommet a un degré égal à d. Il y a k arrêtes autour d'une face.

On a
$$\sum_{v \in V} \deg(v) = dn = 2\,|E| = 2m.$$

Donc $2m = dn$. De plus, la formule d'Euler dit

$$n - m + f = 2.$$

Le nombre de couples arête/face incidentes est égal à $2m = kf$. On a alors

$$\frac{2m}{d} - m + \frac{2m}{k} = 2 \iff m\left(\frac{2}{d} + \frac{2}{k} - 1\right) = 2.$$

Finalement

$$\frac{1}{d} + \frac{1}{k} = \frac{1}{m} + \frac{1}{2}.$$

Cherchons tous les couples (d, k) possibles avec $d, k \geq 3$. Donc $\min(k, d) = 3$.

Pour $d = 3$ on a $k \in \{3, 4, 5\}$ et pour $k = 3$ on a $d \in \{3, 4, 5\}$.

Finalement on a :

- $k = 3$, $d = 3$ c'est le tétraèdre ;
- $k = 3$, $d = 4$ donc $f = 8$, c'est un octaèdre ;
- $k = 3$, $d = 5$ donc $f = 20$ et c'est un dé à 20 faces ;
- $k = 4$, $d = 3$ donc $f = 6$ et c'est un cube ;
- $k = 5$, $d = 3$ donc $f = 12$ et c'est un dé à 12 faces.

6 Coloration des graphes planaires

Définition 6.1
Une coloration de $G = (V, E)$ avec les couleurs C est une application $\alpha : V \to C$.
Une coloration est propre pour toute arête $\{x, y\} \in E$, $\alpha(x) \neq \alpha(y)$.

Définition 6.2
On définit $\chi(G)$ ne nombre chromatique de G, c'est le plus petit nombre de couleurs nécessaires tel que G possède une coloration propre.

Exemple. $\chi(K_n) = n$, $\chi(C_8) = 2$, $\chi(C_{17}) = 3$, $\chi(K_{3,2}) = 2$.

Définition 6.3
Soit $\Delta(G)$ le degré maximum de $G = (V, E)$.

Proposition 6.4
Soit $G = (V, E)$,

$$\chi(G) \leq \Delta(G) + 1.$$

Démonstration
Par récurrence sur le nombre de sommets.
Si $n = 1$, $\Delta(G) = 0$ et on a bien $\chi(G) = 1 \leq 0 + 1$.
Pour $G = (V, E)$ à $n + 1$ sommets. Soit $v \in V$, on définit $G' = G \setminus \{v\}$. On a $\Delta(G') \leq \Delta(G)$.
Par hypothèse de récurrence, on colorie G' avec D couleurs. Comme $\deg_G(v) \leq D$ et comme on a $D + 1$ couleurs, on peut colorier v.

Proposition 6.5
Soit G planaire, $\chi(G) \leq 6$.

Lemme 6.6
Tout graphe planaire possède un sommet de degré au plus 5.

Démonstration (Lemme)
On peut supposer G connexe.
Si G a une seule arrête c'est vérifié.
Sinon, on a montré que $2e - 3f \geq 0$ où e est le nombre d'arêtes et f le nombre de faces. La formule d'Euler dit que $n - e + f = 2$ avec n le nombre de sommets.
Supposons par l'absurde que chaque sommet a un degré supérieur ou égal à 6. Alors

$$2e = \sum_{v \in V} \deg(v) \geq 6n.$$

On a alors aussi

$$2(2e - 3f) + (2e - 6n) \geq 0$$

et alors

$$-6(n - e + f) \geq 0$$

ce qui est impossible. Donc il existe un sommet de degré au plus 5.

Démonstration (Proposition)
Par récurrence sur le nombre de sommets avec $G = (V, E)$ planaire.
Soit $v \in V$ un sommet de degré au plus 5. Par hypothèse de récurrence on colorie $G \setminus \{v\}$ avec 6 couleurs. On peut colorier v en plus avec l'une des 6 couleurs car $\deg(v) \leq 5$.

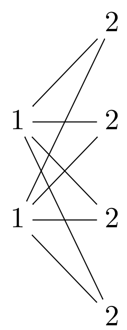
Définition 6.7
$G = (V, E)$ est k-liste coloriable si pour toute application C qui à chaque sommet associe un ensemble de k couleurs, il existe

$$\alpha : V \to \bigcup_{v \in V} C(v)$$

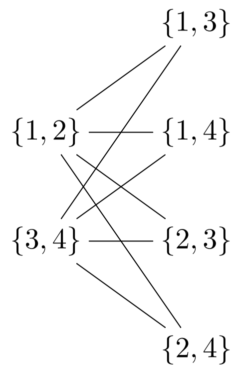
une coloration propre telle que pour tout v, $\alpha(v) \in C(v)$.

Proposition 6.8
Si G est k-liste coloriable alors $\chi(G) \leq k$.

La réciproque est fausse. $\chi(K_{2,4}) = 2$:

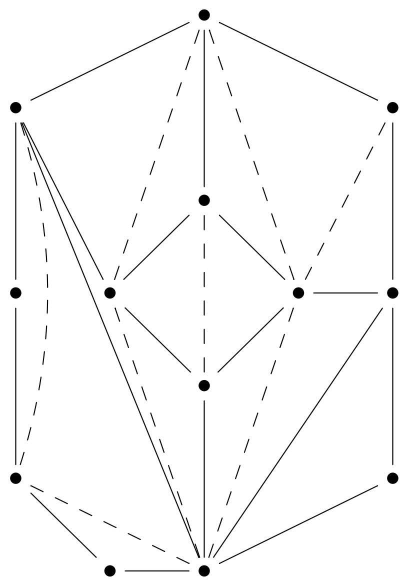


mais $K_{2,4}$ n'est pas 2-liste coloriable :



Théorème 6.9
Tout graphe planaire est 5-liste coloriable et est donc 5-coloriable.

Remarque. Si H est obtenu en ajoutant des arêtes à G et si H est 5-liste coloriable, G l'est aussi. On peut donc supposer que G est presque triagulé.



Un graphe est presque triangulaire si chaque face (sauf éventuellement la face externe) est un triangle.

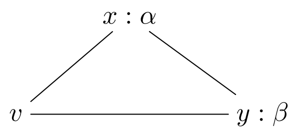
On va montrer la propriété suivante par récurrence sur le nombre de sommets.

Proposition 6.10
On considère graphe presque triangulé dont le cycle de la face externe est B. Soit $\{x, y\}$ une arête de B.

- x colorié avec α ;
- y colorié avec β $(\alpha \neq \beta)$;
- chaque sommet de $B \setminus \{x, y\}$ a une liste de 3 couleurs ;
- chaque autre sommet a une liste de 5 couleurs.

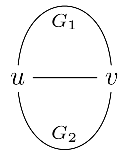
Alors on peut colorier G en piochant dans les listes.

Démonstration
Pour $n = 3$.

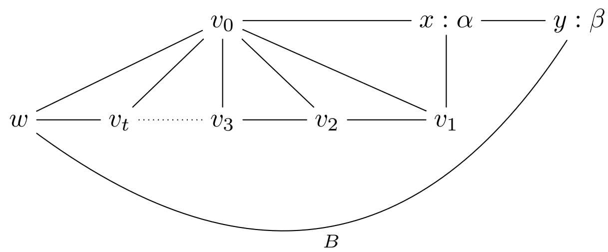


$C(v) \setminus \{\alpha, \beta\} \neq \emptyset$ et donc on peut colorier v.
On fait la récurrence pour $n > 3$.

1. Si B possède une corde $\{u, v\}$,



   on colore G_1 par hypothèse de récurrence puis on donne des couleurs α' et β' à u et v. On colore ensuite G_2 par hypothèse de récurrence.
2. Si B ne possède pas de corde.



   Soit v_0 le voisin de x sur B qui n'est pas y. Les voisins de v_0 sont dans l'ordre $x, v_1, v_2, \dots, v_t, w \in B$ (les v_i sont à l'intérieur de B car B est sans corde).
   Soient $\gamma, \delta \in C(v_0) \setminus \{\alpha\}$. Soit $G' = G \setminus \{v_0\}$. On considère le bord $B' : yxv_1 \dots v_t w$. A chaque v_i on associe un sous-ensemble de taille 3 de $C(v_i) \setminus \{\gamma, \delta\}$.
   Par hypothèse de récurrence on peut colorier G' en piochant dans les listes. On peut colorier v_0 avec une couleur de $\{\gamma, \delta\}$ moins la couleur de w.

7 Couplage

Définition 7.1
Soit $G = (V, E)$ un graphe. Un couplage est un ensemble d'arêtes, $C \subset E$, tel que deux arêtes quelconques de C n'ont pas d'extrémité en commun.

Notations. Pour $v \in V$, on note

$$\Gamma(v) = \{u \in V \mid \{u, v\} \in E\}$$

le voisinage de v. Pour $W \subset V$ on définit

$$\Gamma(W) = \{u \in V \mid \exists w \in W, \{u, w\} \in E\} = \bigcup_{w \in W} \Gamma(w).$$

Définition 7.2
Un graphe $G = (V, E)$ est biparti s'il existe V_1 et V_2 tels que $V = V_1 \sqcup V_2$ et $E \subset \{\{v_1, v_2\} \mid v_1 \in V_1, v_2 \in V_2\}$.

Soit $G = (V, E)$ un graphe biparti avec $V = X \sqcup Y$. À quelle condition existe-t-il un couplage incident à tous les éléments de X ? Nécessairement, pour tout $W \subset X$ on a $|\Gamma(W)| \geq |W|$. La réciproque est vraie :

Théorème 7.3 (Hall)
Le graphe possède un couplage incident à tous les éléments de X si, et seulement si, pour tout $W \subset X$, on a $|\Gamma(W)| \geq |W|$.

Démonstration
Par récurrence sur $|X|$. Si $|X|$ c'est vérifié, on prend $C = \{x, y\}$ avec $y \in \Gamma(x)$.
Supposons $|X| > 1$. L'un des deux cas suivant se présente :

1. Quelque soit $X' \subsetneq X$ non vide, $|\Gamma(X')| > |X'|$. Soit $\{x, y\} \in E$. On considère le graphe $\widetilde{G} = G \setminus \{x, y\}$ (on enlève les deux sommets x et y). $\widetilde{G}$ est un graphe biparti sur $\widetilde{X} \sqcup \widetilde{Y}$ où $\widetilde{X} = X \setminus \{x\}, \widetilde{Y} = Y \setminus \{y\}$.
   Soit $X' \subset \widetilde{X}$, par hypothèse
   $$|\Gamma_G(X')| > |X'|$$
   de plus
   $$\Gamma_{\widetilde{G}}(X') = \Gamma_G(X') \setminus \{y\}$$
   et donc
   $$\left|\Gamma_{\widetilde{G}}(X')\right| \geq |X'|$$
   et par hypothèse de récurrence, il existe un couplage $\widetilde{C}$ de $\widetilde{G}$ incident à tous les éléments de $\widetilde{X}$. Donc $C = \widetilde{C} \cup \{x, y\}$ est un couplage de G incident à tous les éléments de X.
2. Il existe $X' \subsetneq X$ non vide tel que
   $$|\Gamma(X')| = |X'| .$$
   Soit G' le graphe biparti sur $X' \sqcup Y$. G' vérifie la condition car G la vérifie. Par hypothèse de récurrence, il existe un couplage, C', incident à tous les sommets de X'.
   Soit Y' les sommets de Y incidents à C'. Soit $G'' = G \setminus (X' \cup Y')$. Soit $X'' \sqcup Y''$ les sommets de G''. Soit $W \subset X''$ on veut montrer que
   $$|\Gamma_{G''}(W)| \geq |W| .$$
   Or
   $$|\Gamma_G(W \sqcup X')| \geq |W \sqcup X'|$$
   et donc
   $$|\Gamma_{G''}(W)| \geq |W \sqcup X'| - |Y'| = |W| .$$
   Par hypothèse de récurrence, G'' possède un couplage incident à tous les éléments de X'', C''. Donc $C' \cup C''$ constitue un couplage incident à tous les éléments de X.

Chapitre 3

Probabilités et preuves probabilistes

1 Preuves par dénombrement

Mélange des cartes par la méthode de queue d'aronde.

Procédé.

1. Couper le paquet en deux partes de même taille.
2. Intercaler les cartes des deux paquets.

Si on a un jeu de 52 cartes et qu'on fait cette manipulation quatre fois, obtient-on un ordre « aléatoire » ? La réponse est *non* parce qu'on ne peut même pas obtenir tous les ordres possibles.

Il y a 52! ordres des cartes possibles. Pourtant, avec la manipulation précédente on peut obtenir après une itération : $\binom{52}{26}$ ordres possibles. Après quatre itérations, on a donc $\binom{52}{26}^4 < 52!$.

Fonctions booléennes. Une fonction booléenne à n variables est une application $\{0,1\}^n \to \{0,1\}$.

Une formule booléenne est une expression bien formée sur $\{x_1, \ldots, x_n, \wedge, \vee, \neg, (,)\}$.

Une formule booléenne calcule une fonction booléenne. Toute fonction booléenne peut être représentée par une formule $f : \{0,1\}^n \to \{0,1\}$ avec

$$f(x_1, \ldots, x_n) = \bigvee_{\substack{(\varepsilon_1,\ldots,\varepsilon_n)\in\{0,1\}^n \\ f(\varepsilon_1,\ldots,\varepsilon_n)=1}} \bigwedge_{i=1}^{n} s_i x_i$$

avec $s_i x_i = x_i$ si $\varepsilon_i = 1$ et $s_i x_i = \neg x_i$ si $\varepsilon_i = 0$.

Par exemple, avec

$$\begin{aligned} f = \{0,1\}^2 &\to \{0,1\} \\ (0,0) &\mapsto 0 \\ (0,1) &\mapsto 1 \\ (1,0) &\mapsto 0 \\ (1,1) &\mapsto 1 \end{aligned}$$

on a la formule

$$f(x_1, x_2) = (\neg x_1 \wedge x_2) \vee (x_1 \wedge x_2).$$

Taille des formule. La formule ainsi obtenue a une longueur en $O(n2^n)$. Notons $L(f) = \min \mathrm{taille}(E)$ où E calcule f. On se demande quel est le maximum de $L(f)$ pour f à n variables.

Le nombre d'expressions de longueur m est inférieur à $(n+5)^m$. Le nombre de fonctions booléennes à n variables est 2^{2^n}.

Pour n tel que $2^{2^n} > (n+5)^m$ on a $L_n > m$. On a alors

$$2^n > m \log_2(n+5)$$

c'est-à-dire

$$L_n \geq \frac{2^n}{\log_2(n+5)}.$$

1.1 Espace probabilisé fini

Définition 1.1
Un *espace probabilisé fini* est un couple (Ω, P) avec Ω et $P : \mathcal{P}(\Omega) \to [0,1]$ tel que

1. $P(\emptyset) = 0$;
2. $P(\Omega) = 1$;
3. $P(A \cup B) = P(A) + P(B)$ pour $A \cap B = \emptyset$.

Ω est l'ensemble de tous les résultats d'une expérience aléatoire. Les éléments de Ω sont les *événements élémentaires*. Les parties de Ω sont les *événements*. $P(A)$ est la *probabilité* de l'événement A.

Remarque. Comme Ω est fini, pour définir P il suffit de donner $P(\{\omega\})$ pour tout $\omega \in \Omega$.

Exemple. Le cas où tous les événements sont équiprobable est celui où $P(A) = |A| \,/\, |\Omega|$.

Cas d'un espace probabilisé infini. On regarde l'expérience : tirer cinq nombres dans $[0,1]$. Quelle est la probabilité que deux d'entre eux soient à distance inférieure à 0.1 ?

Ici, un événement élémentaire est du type $\{x_1 = 0.17, x_2 = 0.2, x_3 = 0.3, x_4 = 0.9, x_5 = 0.52\}$ et sa probabilité est nulle. Il faut donc définir P autrement.

Exemples d'espace probabilisés finis. On regarde les chaines, C_n, de longueur n de 0 et 1 (pile ou face). Toute les possibilités sont équiprobables. La probabilité d'avoir exactement 10 piles est

$$\frac{\binom{100}{10}}{2^{100}}.$$

On considère S_n, l'ensemble des permutations de $[n]$ avec la probabilité uniforme. Dans un jeu de 52 cartes, quelle est la probabilité que le roi de pique sous au-dessus de la dame de cœur ? Un ordre est une permutation $\pi \in S_{52}$. On peut prendre 1 le roi de pique et 2 la dame de cœur. Il y a une bijection entre $\{\pi \mid \pi(1) < \pi(2)\}$ et son complémentaire. Donc la probabilité est égale à 1/2.

On regarde G_n, l'ensemble des graphes à n sommets (simples, sans bouclettes, non orientés) muni de la probabilité uniforme. On veut connaître

$$\lim_{n\to\infty} P[G \text{ à } n \text{ sommets est biparti}].$$

On pose $V = [n]$ et on prend $U \subset V$ et on considère l'événement, B_U, « G est biparti selon U », *i.e.* « $E \subset U \times (V - U)$ ». On a

$$P[B_U] = \left(\frac{1}{2}\right)^{\binom{n}{2} - |U| \cdot |V-U|} \leq \frac{2^{n^2/4}}{2^{\binom{n}{2}}}.$$

Finalement, la probabilité que G soit biparti, c'est la probabilité qu'il existe U tel que G est biparti selon U. C'est donc majoré par

$$\sum_{U \subset V} P[B_U] \leq 2^n \frac{2^{n^2/4}}{2^{\binom{n}{2}}} \to 0.$$

1.2 Indépendance

Définition 1.2
Deux événements A et B sont indépendants si $P(A \cap B) = P(A)P(B)$.

Exemples.

1. Dans C_{10} on regarde A l'événement « au moins 3 piles parmi les 5 premiers lancers » et B « exactement 2 faces dans les quatre derniers ».
2. Dans G^{20}, A : « au moins un triangle sur les sommets $\{1, \ldots, 7\}$ » et B : « pas de cycle de longueur impaire sur $\{11, 12, \ldots, 20\}$ ».
3. Dans S_n, A : « $\pi(1) = 1$ » et B : « $\pi(2) = 2$ ».

A et B sont-ils indépendants dans chacun des cas ? Ils le sont sauf pour le dernier cas.

Définition 1.3
Soient $A_1, \ldots, A_p$ des événements. Ils sont indépendants si pour tout $I \subset [p]$ on a

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i).$$

Exemple, tournoi. On regarde K_n on chaque arête a une orientation. Par exemple :

$$\begin{tikzcd}
1 \arrow[r] & 2 \arrow[dl, bend left=80] \\
4 \arrow[u] & 3 \arrow[l] \arrow[u] \arrow[ul]
\end{tikzcd}$$

Supposons que l'on oriente chaque arête indépendamment avec probabilité $1/2$. Montrons qu'il existe, pour n assez grand, un tournoi où chaque triplet de joueurs est battu par un même quatrième joueur.

La méthode probabiliste (en combinatoire) consiste à montrer qu'il existe un objet avec la propriété considérée et qui est de probabilité strictement positive.

Pour a, b, c, d distincts, fixés, la probabilité que d batte a, b et c est de $1/8$.

Soient a, b, c distincts, fixés. La probabilité pour que pour tout d on a pas d qui bat a, b, c est par indépendance, $(\frac{7}{8})^{n-3}$.

Ainsi, la probabilité pour qu'il existe a, b, c tel qu'aucun d ne convienne est majoré par la somme des probabilités selon le choix de a, b, c. Or cette somme est égale à

$$\binom{n}{3}\left(\frac{7}{8}\right)^{n-3} < 1$$

pour n assez grand.

1.3 Variable aléatoire

DÉFINITION 1.4
Une *variable aléatoire* est une fonction $f : \Omega \to \mathbf{R}$.

EXEMPLES.

1. Dans C_n, f la fonction qui donne le nombre de 1 dans la chaîne.
2. Dans S_n, g le nombre de records de $\pi \in S_n$. C'est-à-dire

$$g = \left|\{i \in [n] \mid \forall i' < i,\ \pi(i') < \pi(i)\}\right|.$$

DÉFINITION 1.5
Soit f une variable aléatoire sur (Ω, P). L'espérance de f est

$$\mathbf{E}[f] = \sum_{\omega \in \Omega} f(\omega) P(\{\omega\}).$$

REMARQUE. Quand l'espace est équiprobable on a

$$\mathbf{E}[f] = \frac{1}{|\Omega|} \sum_{\omega \in \Omega} f(\omega).$$

CALCUL DE $\mathbf{E}[f]$. Dans le premier exemple, on a

$$\mathbf{E}[f] = \frac{1}{2^n} \sum_{\omega \in \{0,1\}^n} \left|\omega^{-1}(1)\right| = \frac{1}{2^n} \sum_{k=0}^{n} \binom{n}{k} = \frac{1}{2^n} n 2^{n-1} = \frac{n}{2}.$$

DÉFINITION 1.6
Soit $A \subset \Omega$. La fonction indicatrice de A est la fonction :

$$\mathbb{1}_A(\omega) = \begin{cases} 1 \text{ si } \omega \in A \\ 0 \text{ sinon} \end{cases}$$

PROPOSITION 1.7
On a

$$\mathbf{E}[\mathbb{1}_A] = P(A).$$

DÉMONSTRATION

$$\begin{aligned} \mathbf{E}[\mathbb{1}_A] &= \sum_{\omega \in \Omega} P(\omega) \mathbb{1}_A(\omega) \\ &= \sum_{\omega \in A} P(\omega) = P(A). \end{aligned}$$

THÉORÈME 1.8 (Linéarité de l'espérance)
Soient f, g deux variables aléatoires sur (Ω, P) et soit $\alpha \in \mathbf{R}$.

$$\mathbf{E}[f + g] = \mathbf{E}[f] + \mathbf{E}[g]$$
$$\mathbf{E}[\alpha f] = \alpha \mathbf{E}[f].$$

Calcul de $\mathbf{E}[g]$. $g(\pi)$ est le nombre de records de π. Si on pose A_i l'événement « i est un record » alors $g = \sum \mathbb{1}_{A_i}$.

$$\begin{aligned}
\mathbf{E}[g] &= \mathbf{E}[\sum \mathbb{1}_{A_i}] \\
&= \sum_{i=1}^{n} P(A_i) \\
P(A_i) &= \frac{1}{i} \\
\mathbf{E}[g] &= \sum_{i=1}^{n} \frac{1}{i}.
\end{aligned}$$

2 Applications de la méthode probabiliste

2.1 Grands graphes bipartis

Soit $G = (V, E)$ un graphe. Il s'agit de trouver un sous-graphe partiel biparti, contenant beaucoup d'arêtes.

Proposition 2.1
Il existe A et B tel que $V = A \sqcup B$ et

$$E(A, B) = \{\{u, v\} \in E \,|\, u \in A, V \in B\}$$

vérifie $|E(A, B)| > |E| /2$.

Démonstration
On choisit A au hasard avec $|A| = |V| /2$, $A \sim \mathcal{U}(\binom{V}{|V|/2})$. On pose $B = V - A$. Il s'agit d'estimer $|E(A, B)|$.
Notons C_e l'événement « l'arête e vérifie $e \in E(A, B)$ ». Soit $e = \{u, v\}$ est fixé. La probabilité que C_e soit vérifiée est

$$\mathbf{P}(C_e) = 2\frac{\binom{2n-1}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-1}.$$

Comme

$$|E(A, B)| = \sum_{e \in E} \mathbb{1}_{C_e}$$

on a

$$\begin{aligned}
\mathbf{E}[|E(A, B)|] &= \sum_{e \in E} \mathbf{E}[\mathbb{1}_{C_e}] \\
&= \sum_{e \in E} \mathbf{P}(C_e) \\
&= |E| \frac{n}{2n-1} > \frac{|E|}{2}.
\end{aligned}$$

2.2 Grand graphe sans cliques

Définition 2.2
Soit $G = (V, E)$ un graphe, $V' \subset V$ est une *clique* si V' induit un sous-graphe complet.

Graphes sans triangle. Soit $T(n)$ le nombre maximum d'arêtes pour les sous-graphes à n sommets sans triangle.

On aimerait une description de $T(n)$ et des graphes sans triangles à n sommets et $T(n)$ arêtes.

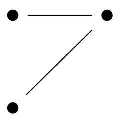
1. Pour C_n avec $n > 3$ il y a n arêtes.
2. Les arbres de tailles $n > 2$ ont $n - 1$ arêtes.
3. Les graphes bipartis complets. En particulier, $K_{\lfloor n/2 \rfloor \lceil n/2 \rceil}$ a $\lfloor n/2 \rfloor \lceil n/2 \rceil$ arêtes. Donc $T(n) \geq \lfloor n^2/4 \rfloor$.

On va montrer que $T(n) = \lfloor n^2/4 \rfloor$ et tout graphe sans triangle avec ce nombre d'arêtes est isomorphe à $K_{\lfloor n/2 \rfloor \lceil n/2 \rceil}$. Pour les premières valeurs de n on a :

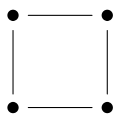
1. Pour $T(1) = 0$:

2. Pour $T(2) = 1$:

3. Pour $T(3) = 2$:



4. Pour $T(4) = 4$:



Montrons par récurrence sur n que

$$T(n) \leq \frac{n^2}{4}.$$

Démonstration

Soit $G = (V, E)$ sans triangle à $n + 2$ sommets. Soit $e = \{x, y\}$ une arête.
Soit $G' = G \setminus e$. Soient :

$$\begin{aligned} V_x &= \{u \in V' \mid \{u, x\} \in E\} \\ V_y &= \{u \in V' \mid \{u, y\} \in E\} \\ E_x &= E(\{x\}, V') \\ E_y &= E(\{y\}, V') \end{aligned}$$

Puisqu'il n'y a pas de triangle, $V_x \cap V_y = \emptyset$. On a alors

$$\begin{aligned} |E| &= |E'| + |E_x \cup E_y| + 1 \\ &\leq |E'| + |V'| + 1 \\ &\leq \frac{n^2}{4} + n + 1 = \frac{(n+2)^2}{4} \end{aligned}$$

Démonstration

Soit $G = (V, E)$ un graphe sans triangle à $\lfloor \frac{n^2}{4} \rfloor$ arêtes et n sommets. Montrons par récurrence sur n que G est isomorphe à $K_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}$.
La propriété est vraie pour $n \in \{2, 3\}$. Montrons que si c'est vrai pour n, ça l'est pour $n + 2$.
Soit $G = (V, E)$ sans triangle à $n + 2$ sommets et avec $\lfloor \frac{(n+2)^2}{4} \rfloor$ arêtes. Soit $e = \{x, y\} \in E$ et soit $G' = G \setminus \{x, y\}$. $G' = (V', E')$ a n sommets, est sans triangle et pour tout $u \in V'$, on a pas $\{u, x\} \in E$ et $\{u, y\} \in E$. Mais au moins l'une des deux appartenance est vraie, sinon on pourrait rajouter une arête à G.

Donc

$$|E'| = |E| - (n+1) = \left\lfloor \frac{n^2}{4} \right\rfloor$$

et par hypothèse de récurrence, G' est isomorphe à $K_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}$. Comme G est sans triangle, Γ_x est la partie gauche et Γ_y est la partie droite (ou inversement) de $K_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}$. Donc en mettant x à droite et y à gauche, on a que G est biparti complet avec le bon nombre de sommets.

Définition 2.3
Soit $G = (V, E)$ un graphe. $I \subset V$ est *indépendant* si pour tous $u, v \in I$, $\{u, v\} \notin E$.

Remarque. I est indépendant dans G si, et seulement si, I est une clique dans $\overline{G}$.

Le théorème précédent dit que s'il y a beaucoup d'arêtes alors il existe un triangle. S'il y a beaucoup d'arêtes, il existe K_3 en sous graphe ; s'il y en a peu, il existe un ensemble indépendant de taille 3.

Théorème 2.4 (Thuram)
Soit $G = (V, E)$ un graphe avec $n = |V|$ et $m = |E|$.

$$\alpha(G) \geq \frac{n^2}{2m + n}$$

Avec $\alpha(G)$ la taille maximale des ensembles indépendants.

Lemme 2.5
Pour $G = (V, E)$ on a

$$\alpha(G) \geq \sum_{v \in V} \frac{1}{\deg(v) + 1}.$$

Démonstration
Soit π une permutation aléatoire (uniforme) de V. Soit

$$M(\pi) = \{u \in V \mid \forall v \in V,\ \{u, v\} \in E \implies \pi(v) > \pi(u)\}.$$

$M(\pi)$ est un ensemble indépendant. En effet, si $u, v \in M(\pi)$ alors on a soit $\pi(u) < \pi(v)$ soit $\pi(v) < \pi(u)$ et donc $\{u, v\} \notin E$.
Soit A_v l'événement « $v \in M(\pi)$ ». A_v est vérifié si, et seulement si, pour tout $v' \in \Gamma(v)$, $\pi(v') > \pi(v)$. Soit $d = \deg(v)$, on a :

$$\begin{aligned} \mathbf{P}(A_v) &= \frac{\binom{n}{1+d} d!(n-(1+d))!}{\binom{n}{1+d}(d+1)!(n-(1+d))!} \\ &= \frac{1}{d+1} \end{aligned}$$

Comme $|M(\pi)| = \sum_{v \in V} \mathbb{1}_{A_v}$ on a

$$\begin{aligned} \mathbf{E}[|M(\pi)|] &= \sum_{v \in V} \mathbf{P}(A_v) \\ &= \sum_{v \in V} \frac{1}{\deg(v)+1}. \end{aligned}$$

Donc il existe π tel que

$$M(\pi) \geq \mathbf{E}[M(\pi)] = \sum \frac{1}{\deg(v)+1}.$$

Démonstration (Théorème)
On sait que $\sum \deg(v) = 2|E| = 2n$.
Si $x+y = s$ sont fixés alors $1/(x+1)+1/(y+1)$ est minimal pour $x = s/2$. Donc $\sum 1/(\deg(v)+1)$ est supérieure à la valeur obtenue pour $\deg(v) = 2m/n$ ce qui donne

$$\alpha(v) \geq \mathbf{E}[M(\pi)] \geq n\frac{1}{\frac{2m}{n}+1} = \frac{n^2}{2m+n}.$$

2.3 Nombre de points d'intersection de niveau au plus k

On considère $D_1, \ldots, D_n$, n droites dans le plan en position générale (dont 2 ne sont pas parallèles et 3 ne sont pas concourantes). Soit $o \notin \bigcup D_i$ fixé.

Définition 2.6
Soit v un point d'intersection, $v \in D_i \cap D_j$. Le niveau de v est le nombre de droites intersectant $]o, v[$.

Théorème 2.7
Il y a au plus $3(k+1)n$ points de niveau au plus k.

Démonstration
Par récurrence sur k.

- Au niveau 0 il y a au plus n points d'intersection.
- Soit $0 < p < 1$ à choisir. On choisit $R \subset \{D_1, \ldots, D_n\}$ un sous-ensemble des droites où chaque droite est choisie avec probabilité p. On pose $f(R)$ le nombre de points de niveau 0 de $\mathcal{A}(R)$ (l'arrangement des droites R). On va analyser $f(R)$ de deux façons différentes. Pour $v = D_i \cap D_j$, notons A_v l'événement « v est de niveau 0 dans $\mathcal{A}(R)$ ». A_v est vérifié si, et seulement si, les deux droites définissant v sont dans R et les droites intersectant $]o, v[$ ne sont pas dans R.
  - On a $f(R) \leq |R|$, donc
  $$\mathbf{E}[f(R)] \leq \mathbf{E}[|R|] \leq np$$
  - On a
  $$f(R) = \sum_{v \in I_D} \mathbb{1}_{A_v}$$
  et donc
  $$\mathbf{E}[f(R)] = \sum_{v \in I_D} \mathbf{P}(A_v) \geq \sum_{v,\, l(v) \leq k} p^2(1-p)^k$$
  avec $l(v)$ le niveau de v.

  Si N_k est le nombre de points de niveaux inférieurs à k alors
  $$np \geq \mathbf{E}[f(R)] \geq N_k p^2(1-p)^k$$
  d'où
  $$N_k \leq \frac{n}{p(1-p)^k}.$$
  Pour $p = 1/(k+1)$ (presque minimal) on a
  $$\frac{1}{p(1-p)^k} \leq e(k+1) \leq k(k+1)$$
  d'où
  $$N_k \leq 3(k+1)n.$$

2.4 Nombre d'arbres sur $[n]$

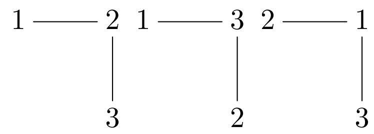
1. Pour $n = 1$ on a

$$1$$

2. Pour $n = 2$ on a

$$1 \text{ --- } 2$$

3. Pour $n = 3$ on a

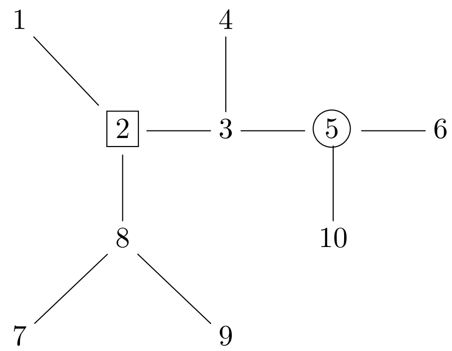


Si on note $T(K_n)$ le nombre d'arbres couvrants de K_n.

Théorème 2.8 (Cayley)
Pour $n \geq 2$,

$$T(K_n) = n^{n-2}.$$

On prend un arbre sur $[n]$. On distingue 2 sommets (qui peuvent être confondus), un encerclé et l'autre encadré. Un tel arbre est un *vertébré*.



Si V_n est l'ensemble des vertébrés sur $[n]$ alors

Lemme 2.9
V_n est en bijection avec $V^V = [n]^{[n]}$.

En conséquence, comme $n^n = T(K_n)n^2$ on a le résultat voulu.

Démonstration
En plusieurs étapes :

1. On regarde du cercle à l'encadré les sommets, c'est la colonne vertébrale C. On définit une permutation de C en prenant le chemin du cercle au rectangle comme liste image et les sommets atteints dans l'ordre croissant comme liste antécédente.
   Pour les sommets en dehors de C, on définit une application de $V \setminus C \to C$ de la manière suivante : on oriente les arêtes en dehors vers la colonne vertébrale, à chaque sommet on associe le sommet de l'extrémité orientée vers C.
   On a par recollement une application de $V \to V$.
2. Montrons que cette association est inversible. Soit $\theta \in V^V$, montrons qu'il existe un vertébré qui définit Θ.
   Soit $G = ([n], E)$ où
   $$E = \{(i, \theta(i) \mid i \in [n]\}.$$
   Comme θ est une application, pour tout v on a $\deg^+(v) = 1$. Les éléments des cycles limites définissent la colonne vertébrale et les autres éléments sont associés en fonction de leur image.