2M226 - Combinatoire et Graphes

Arnau Padrol

26 juillet 2018

Table des matières

I Combinatoire énumérative **3**

1 Rappels et notation **5**
1.1 Ensembles 5
1.2 Applications 7
1.3 Relations binaires 8
1.3.1 Relations d'équivalence et partitions 8
1.3.2 Relations d'ordre 10
1.4 Entiers naturels 10
1.5 Cardinal d'un ensemble fini 11
1.5.1 Principe de bijection 12
1.5.2 Principe des tiroirs 13
1.6 Équipotence et ensembles infinis dénombrables 14

2 Dénombrement **17**
2.1 Principes de dénombrement 17
2.1.1 Principe d'addition 17
2.1.2 Principe des bergers 18
2.1.3 Principe de multiplication 19
2.2 Comptage des applications 19
2.2.1 Le nombre d'applications 20
2.2.2 Le nombre d'injections 21
2.2.3 Le nombre de bijections 22
2.2.4 Une estimation de la fonction factorielle 22
2.2.5 Surjections et partitions 24
2.3 Nombres binomiaux 25
2.3.1 L'ensemble de parties de taille k 25
2.3.2 Multi-ensembles 28
2.3.3 Formule du binôme 29
2.4 Les nombres multinomiaux 30
2.4.1 Une estimation de $\binom{n}{k}$ 32
2.4.2 La "forme" de l'ensemble des coefficients binomiaux 33

2.5 Formule du crible . . . 35
2.5.1 Le nombre de surjections, revisité . . . 36

3 Fonctions génératrices 39
3.1 L'anneau des séries formelles . . . 39
3.1.1 Rappel : L'anneau des polynômes . . . 39
3.1.2 Séries formelles . . . 39
3.1.3 Une justification pour la notation . . . 41
3.1.4 Inverse multiplicatif . . . 41
3.2 Théorème du binôme pour des exposants négatifs . . . 43
3.3 Équations de récurrence linéaires . . . 46
3.3.1 La suite de Fibonacci . . . 46
3.3.2 Récurrences linéaires homogènes à coefficients constants . . . 48

II Graphes 49

4 Introduction à la théorie de graphes 51
4.1 Graphes et isomorphismes . . . 51
4.1.1 Isomorphisme . . . 52
4.2 Bestiaire . . . 54
4.3 Degrés . . . 55
4.3.1 Le lemme des poignées de main . . . 56
4.3.2 Matrices associées à un graphe . . . 56
4.3.3 Le théorème d'Havel et Hakimi . . . 58
4.4 Théorie extrémale des graphes . . . 60
4.4.1 Sous-graphes . . . 60
4.4.2 Théorème de Turán . . . 61
4.4.3 Graphe complémentaire et stables . . . 63
4.5 Théorie de Ramsey . . . 64

5 Chaînes, parcours, cycles et tours 67
5.1 Chaînes, parcours . . . 67
5.1.1 Connexité . . . 68
5.2 Distance . . . 69
5.2.1 Graphes valués et Algorithme de Dijkstra . . . 70
5.3 Tours et parcours eulériens (et hamiltoniens) . . . 72
5.3.1 Graphes eulériens . . . 72
5.3.2 Graphes hamiltoniens . . . 74
5.4 Arbres . . . 74

6 Coloration, graphes bipartis et couplages **79**
6.1 Colorations 79
6.1.1 Graphes bipartis 81
6.2 Couplages 81

7 Planarité **85**
7.1 Dessiner des graphes dans le plan 85
7.2 Formule d'Euler 86

Première partie

Combinatoire énumérative

Chapitre 1

Rappels et notation

1.1 Ensembles

Nous allons travailler avec une définition intuitive et informelle de la notion d'ensemble. Les fondations mathématiques de la **théorie des ensembles** sont subtiles, et une axiomatique rigoureuse ne permet pas la définition d'objets comme **l'ensemble de tous les ensembles** qui donnent lieu à paradoxes (voir Zermelo–Fraenkel). Pour les ensembles étudiés dans ce cours, dont la plupart sont finis, il n'y a pas de risque de paradoxe, et la notion intuitive d'ensemble est largement suffisante.

Définition 1.1. Un **ensemble** est une "collection d'objets", appelés **éléments** de E. On note $\boldsymbol{x \in E}$, et on dit que x appartient à l'ensemble E, si x est un élément de E. On note $\boldsymbol{x \notin E}$ sinon. L'ensemble qui ne contient aucun élément est appelé **ensemble vide** et est noté $\varnothing$.

On utilise les symboles '{' et '}' pour présenter un ensemble. Par exemple, l'ensemble formé des éléments a, b et c s'écrit $\{a, b, c\}$. L'ordre des éléments d'un ensemble n'a aucune aucune importance ($\{a, b\} = \{b, a\}$), ni les répétitions non plus ($\{a, a, b\} = \{a, b\}$). On écrit $\{x \in E : \mathcal{P}\}$ pour dénoter l'ensemble des éléments x de E possédant la propriété $\mathcal{P}$. On utilise aussi cette notation pour construire des nouveaux ensembles à partir d'ensembles connus. Par exemple, l'ensemble des carrés des entiers naturels s'écrit

$$\{0, 1, 4, 9, \ldots\} = \left\{n \in \mathbb{N} : \text{ existe } i \text{ tel que } i^2 = n\right\} = \left\{i^2 : \ i \in \mathbb{N}\right\}.$$

Si A et B sont des ensembles, on note $\boldsymbol{A \subseteq B}$, et on dit que A est un **sous-ensemble** de B, si chaque élément de A appartient également à B. On dit aussi que A est une **partie** de B, ou que A est **inclus** dans B. Deux ensembles sont égaux, ce qu'on note $\boldsymbol{A = B}$, si et seulement si $A \subseteq B$ et $B \subseteq A$.

Opérations ensemblistes

Soient A, B et E des ensembles.

- La **(ré)union** de A et B est l'ensemble

$$A \cup B = \{x : x \in A \text{ ou } x \in B\}.$$

Pour la réunion de plusieurs ensembles, on utilise aussi la notation

$$\bigcup_{i=1}^{n} A_i = \bigcup_{1 \le i \le n} A_i = \bigcup_{i \in [1,n]} A_i = A_1 \cup A_2 \cup \cdots \cup A_n.$$

- L'**intersection :** de A et B est l'ensemble

$$A \cap B = \{x : x \in A \text{ et } x \in B\}.$$

Si $A \cap B = \varnothing$, alors A et B sont **disjoints**.

Pour l'intersection de plusieurs ensembles, on utilise aussi la notation

$$\bigcap_{i=1}^{n} A_i = \bigcap_{1 \le i \le n} A_i = \bigcap_{i \in [1,n]} A_i = A_1 \cap A_2 \cap \cdots \cap A_n.$$

Les opérations union et intersection sont *associatives*, *commutatives* et *distributives l'une par rapport à l'autre.*

- La **différence** entre A et B est l'ensemble A **privé** de B :

$$A \setminus B = \{x : x \in A \text{ et } x \notin B\}.$$

Si $A \subseteq E$, le **complémentaire** de A dans E est $\bar{A} = E \setminus A$.

- Le **produit cartésien** de A et B est

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Les **couples** (a, b) sont des paires *ordonnées*. Il ne faut pas confondre la paire $\{a, b\}$ avec le couple (a, b) : $(a, b) = (b, a)$ si et seulement si $a = b$.

Le produit cartésien de plusieurs ensembles on utilise aussi la notation

$$\begin{aligned}\prod_{i=1}^{n} A_i = \prod_{1 \le i \le n} A_i = \prod_{i \in [1,n]} A_i &= A_1 \times A_2 \times \cdots \times A_n \\ &= \{(a_1, \ldots, a_n) : a_i \in A_i \text{ pour tout } i \in [1, n]\}.\end{aligned}$$

Ses éléments sont appelés des ***n*-uplets**.

Si tous les A_i sont égaux à A, on utilise aussi la notation A^n (comme par exemple dans $\mathbb{R}^n$).

- L'**ensemble des parties** de E est

$$\mathcal{P}(E) = \{A : A \subseteq E\}.$$

Par exemple, $\mathcal{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$.

1.2 Applications

Soient E et F des ensembles. Une **application** de E dans F est la donnée, pour chaque élément x de E, d'un élément $f(x)$ de F. On formalise ceci comme suit :

Définition 1.2. Une **application** (ou **fonction**) f de E dans F est une partie de $E \times F$ telle que pour tout $x \in E$, l'ensemble $\{y \in F : (x,y) \in f\}$ contient exactement un élément. Si $(x,y) \in f$, on note $y = f(x)$ ou $x \mapsto y$ et on dit que y est l'**image** de x par f, et que x est un **antécédent** de y par f. E est appelé l'**ensemble de départ** de f, et F l'**ensemble d'arrivée**.

Définition 1.3. On écrit $f : E \to F$ si f est une application de E dans F. Si $A \subseteq E$, l'**image (directe)** de A par f est

$$f(A) = \{f(x) : x \in A\}.$$

Si $B \subseteq F$, l'**image réciproque** de B est

$$f^{-1}(B) = \{x \in E : f(x) \in B\}.$$

Définition 1.4. Une application $f : E \to F$ est dite :

- **injective** si

$$\forall x, y \in E,\ f(x) = f(y) \Rightarrow x = y,$$

équivalemment, si $x \neq y \Rightarrow f(x) \neq f(y)$;

- **surjective** si

$$\forall y \in F,\ \exists x \in E,\ y = f(x),$$

c'est-à-dire, si $f(E) = F$;

- **bijective** si elle est à la fois injective et surjective :

$$\forall y \in F,\ \exists! x \in E,\ y = f(x).$$

Une application qui est injective, surjective ou bijective est appelée une **injection**, **surjection** ou **bijection**, respectivement.

Soient $f : E \to F$ et $g : F \to G$ applications. On définit l'**application composée** de f et g

$$\begin{aligned} g \circ f : E &\to G \\ x &\mapsto g(f(x)) \end{aligned}$$

Nous laissons la preuve du résultat suivant comme un exercice au lecteur.

Lemme 1.5. *Si $f : E \to F$ et $g : F \to G$ sont injectives/surjectives/bijectives, alors $g \circ f$ est aussi injective/surjective/bijective.*

L'application $\mathrm{id}_E : E \to E$ telle que $x \mapsto x$ est appelée **fonction identité**. Si $f : E \to F$ est bijective, alors il existe une unique fonction $f^{-1} : F \to E$, appelée **fonction inverse de f** telle que $f^{-1} \circ f = \mathrm{id}_E$ et $f \circ f^{-1} = \mathrm{id}_F$. C'est à dire $f^{-1}(y) = x$ si et seulement si $x = f(y)$. La fonction $f^{-1} : F \to E$ est aussi une bijection.

1.3 Relations binaires

Soit E un ensemble. Une **relation binaire** sur E est une partie $\mathcal{R}$ de $E \times E$. Lorsque $(x, y) \in \mathcal{R}$ on dit que x et y **sont en relation** par $\mathcal{R}$, et on écrit $x\mathcal{R}y$.

Définition 1.6. Une relation binaire $\mathcal{R}$ sur E est

- **réflexive** : si pour tout $x \in E$, on a $x\mathcal{R}x$;
- **symétrique** : si pour tout $(x, y) \in E^2$, on a $x\mathcal{R}y$ implique $y\mathcal{R}x$;
- **antisymétrique** : si pour tout $(x, y) \in E^2$, on a ($x\mathcal{R}y$ et $y\mathcal{R}x$) impliquent $x = y$;
- et **transitive** : si pour tout $(x, y, z) \in E^3$, on a ($x\mathcal{R}y$ et $y\mathcal{R}z$) impliquent $x\mathcal{R}z$.

1.3.1 Relations d'équivalence et partitions

Définition 1.7. Une relation binaire $\mathcal{R}$ sur E est une **relation d'équivalence** si elle est réflexive, symétrique et transitive.

Exemples 1.8. Lest relations suivantes sont des relations d'équivalence :

- l'égalité, définie par $x\mathcal{R}y$ si $x = y$;
- Si $f : X \to Y$ est une application, la relation définie par $x\mathcal{R}y$ si $f(x) = f(y)$;

- $\mathcal{R} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : 2 \text{ divise } x - y\}$;
- la relation $\mathcal{R}$ sur $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ donnée par $(a, b)\mathcal{R}(c, d)$ si et seulement si $ad = cb$.

Définition 1.9. Soit $\mathcal{R}$ une relation d'équivalence sur l'ensemble E. Pour tout $x \in E$ la **classe d'équivalence** de x est l'ensemble $\mathcal{R}[x] = \{y \in E : x\mathcal{R}y\}$. L'ensemble de toutes les classes d'équivalence est l'**ensemble quotient** de E par $\mathcal{R}$, et est noté $E/\mathcal{R}$. On a $E/\mathcal{R} \subseteq \mathcal{P}(E)$.

Définition 1.10. Une **partition** d'un ensemble E est une famille $(A_i)_{i\in I}$ de sous-ensembles de E, telle que :

(i) les ensembles A_i **recouvrent** E : $\bigcup_{i\in I} A_i = E$;

(ii) sont non-vides : $\forall i \in I$, $A_i \neq \varnothing$;

(iii) et deux-à-deux disjoints :$\forall i \in I$, $\forall j \in I$, $i \neq j \Rightarrow A_i \cap A_j = \varnothing$.

Proposition 1.11.

1. *Si $\mathcal{R}$ est une relation d'équivalence sur E, alors $E/\mathcal{R}$ est une partition de E.*
2. *Pour toute partition $(A_i)_{i\in I}$ de E, il existe une unique relation d'équivalence $\mathcal{R}$ telle que $E/\mathcal{R} = \{A_i : i \in I\}$. En particulier, $E/\mathcal{R}$ détermine entièrement $\mathcal{R}$.*

Démonstration.

1. Comme $\mathcal{R}$ est réflexive, $\forall x \in E$, $x\mathcal{R}x$, et donc $x \in \mathcal{R}[x]$. Ceci implique que $E \subseteq \bigcup_{\mathcal{R}[x]\in E/\mathcal{R}} \mathcal{R}[x]$ et que $\forall x \in E$, $\mathcal{R}[x] \neq \varnothing$.

   Il reste a montrer que, si $\mathcal{R}[x]$ et $\mathcal{R}[y]$ ne sont pas disjoints, alors $\mathcal{R}[x] = \mathcal{R}[y]$. En effet, si $z \in \mathcal{R}[x] \cap \mathcal{R}[y]$, alors $x\mathcal{R}z$ et $y\mathcal{R}z$. Par transitivité (et symétrie), $x\mathcal{R}y$, et donc $\mathcal{R}[x] = \mathcal{R}[y]$.

2. Soit $(A_i)_{i\in I}$ une partition de E. On définit une relation binaire $\mathcal{R}$ sur E de la manière suivante : $x\mathcal{R}y$ si et seulement s'il existe $i \in I$ tel que $x, y \in A_i$. C'est facile à vérifier que cette relation est réflexive, transitive et symétrique.

cqfd.

1.3.2 Relations d'ordre

Définition 1.12. Une relation binaire $\mathcal{R}$ sur E est une **relation d'ordre (partiel)** si elle est réflexive, antisymétrique et transitive.

On utilise d'habitude le symbole $\preceq$ pour noter une relation d'ordre. On en dérive deux autres relations binaires très naturelles. L'inégalité inverse $x \succeq y$, définie par $x \succeq y$ si et seulement si $y \preceq x$, qui est aussi une relation d'ordre ; et l'inégalité stricte $x \prec y$, définie par $x \prec y$ si et seulement si $x \preceq y$ et $x \neq y$ (par contre, ceci n'est pas une relation d'ordre).

Si pour tout couple d'éléments $x, y \in E$ on a soit $x \preceq y$, soit $y \preceq x$, on dit que la relation est une **relation d'ordre total**.

Un couple $(E, \preceq)$, où E est un ensemble muni d'une relation d'ordre $\preceq$, est appelé un **ensemble partiellement ordonné**.

Exemples 1.13. Voici quelques ensembles partiellement ordonnés :

- $(\mathbb{N}, \leq)$ où $x \leq y$ si $y - x \in \mathbb{N}$, (et de façon similaire $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$) ;
- $(\mathbb{N}, |)$, où $a \mid b$ si $\exists k \in \mathbb{N}$ tel que $bk = a$;
- $(\mathcal{P}(X), \subseteq)$

Soit $(X, \preceq)$ un ensemble partiellement ordonné. Un élément $a \in X$ est le **plus grand élément** de X si par tout $x \in X$, on a $x \preceq a$; et un **élément maximal** s'il n'existe pas de $y \in X$ tel que $a \prec y$. On définit de la même manière le **plus petit élément** et un **élément minimal**.

Il y a ensembles sans élément maximal, par exemple $(\mathbb{N}, \leq)$. Si le plus grand élément existe, alors il est maximal, mais la réciproque n'est pas vraie. Par exemple, l'ensemble $([1, 5], |)$ a plusieurs éléments maximaux : $\{3, 4, 5\}$.

1.4 Entiers naturels

On note $\mathbb{N} = \{0, 1, 2, \ldots\}$ l'ensemble des **entiers naturels**. On note les entiers naturels privés de zéro par $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. Pour $a, b \in \mathbb{N}$, on définit l'intervalle $[a, b] = \{n \in \mathbb{N} : a \leq n \text{ et } n \leq b\}$ (si $a > b$, alors $[a, b] = \varnothing$). Par construction [1], l'ensemble $\mathbb{N}$ a la propriété suivante (qu'on prend comme un axiome) :

Remarque 1.14 (Propriété fondamentale des entiers naturels)**.** Toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

On dit aussi que $(\mathbb{N}, \leq)$ est **bien ordonné**.

1. Celle-ci est hors-programme.

Proposition 1.15 (Principe de récurrence)**.** *Soit $\mathcal{P}(n)$ une proposition dépendant d'un entier n de $\mathbb{N}$. Si la proposition $\mathcal{P}(0)$ est vraie, et si on a la propriété :*

$$\forall n \in \mathbb{N}, \mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$$

alors, pour tout n de $\mathbb{N}$, la proposition $\mathcal{P}(n)$ est vraie.

Démonstration. Soit E l'ensemble des entiers n de $\mathbb{N}$ tels que la proposition $\mathcal{P}(n)$ est fausse. On va montrer que $E = \varnothing$. Supposons le contraire. Si $E \neq \varnothing$, alors il admet un plus petit élément n_0. Comme $\mathcal{P}(0)$ est vraie, $n_0 \neq 0$ et $n_0 - 1 \in \mathbb{N}$. Par minimalité de n_0, $\mathcal{P}(n_0 - 1)$ est vraie, d'où $\mathcal{P}(n_0 - 1 + 1) = \mathcal{P}(n_0)$ est vraie, et $n_0 \notin E$, ce qui est une contradiction. **cqfd.**

On utilise souvent le même principe pour montrer qu'une propriété $\mathcal{P}(n)$ est valide pour tous les entiers $n \geq k$. Dans ce cas là, il faut montrer que $\mathcal{P}(k)$ est vraie et que pour tout $n \geq k$, $\mathcal{P}(n) \Rightarrow \mathcal{P}(n+1)$. (On déduit ce principe du principe de récurrence en utilisant la propriété $\mathcal{P}'(n)$ qui est vraie si et seulement si $\mathcal{P}(n+k)$ est vraie.)

1.5 Cardinal d'un ensemble fini

Un ensemble E est dit **fini** s'il est vide ou s'il existent un entier $n \in \mathbb{N}$ et une bijection $f : E \to [1, n]$. Notez que, à priori, ce nombre n pourrait ne pas être unique. Dans cette section, nous allons montrer qu'un tel nombre est toujours unique, et nous allons l'appeler le **cardinal** de E.

Théorème 1.16. *Soient $n, m \in \mathbb{N}^*$. Il existe une injection de $[1, n]$ dans $[1, m]$ si et seulement si $n \leq m$.*

Démonstration. Si $n \leq m$, alors l'application $i \mapsto i$ est une fonction injective de $[1, n]$ dans $[1, m]$, ce qui montre l'implication directe.

Pour la réciproque, on montre par récurrence la propriété $\mathcal{P}(n)$ suivante :

$\mathcal{P}(n)$: pour tout $m \geq 1$, s'il existe une injection de $[1, n]$ dans $[1, m]$ alors $n \leq m$.

Initialisation : Pour $n = 1$, la propriété $\mathcal{P}(1)$ est vraie, car $m \geq n = 1$ par hypothèse.

Hérédité : Supposons la propriété $\mathcal{P}(n)$ vraie pour $n \geq 1$, et montrons que $\mathcal{P}(n+1)$ est vraie aussi.

Supposons qu'il existe une application injective $f : [1, n+1] \to [1, m]$. Notons qu'on a forcement $m \geq 2$, car $[1, n+1]$ contient au moins deux éléments distincts, et leurs images sont deux éléments distincts par l'injectivité de f. On en déduit que $m - 1 \in \mathbb{N}^*$.

- Si $f(n+1) = m$, alors l'application

$$\begin{aligned} f\big|_{[1,n]} : [1,n] &\to [1,m-1] \\ i &\mapsto f(i) \end{aligned}$$

est une injection de $[1,n]$ dans $[1,m-1]$. D'après l'hypothèse de récurrence on a que $n \leq m-1$, et donc que $n+1 \leq m$.

- Si $f(n+1) = k \neq m$. On considère l'application $\sigma : [1,m] \to [1,m]$ définie par

$$\begin{cases} \sigma(m) = k \\ \sigma(k) = m \\ \sigma(i) = i \text{ autrement} \end{cases}$$

qui est une bijection.

L'application $g = \sigma \circ f$ est alors injective de $[1,n+1]$ dans $[1,m]$ (voir Lemme 1.5), et telle que $g(n+1) = m$. On se ramène au cas précédent. **cqfd.**

Corollaire 1.17. *Si, pour $n, m \in \mathbb{N}^*$, il existent des bijections $f : E \to [1,n]$ et $g : E \to [1,m]$, alors $n = m$.*

Démonstration. Les applications $f \circ g^{-1} : [1,m] \to [1,n]$ et $g \circ f^{-1} : [1,n] \to [1,m]$ sont aussi des bijections (voir Lemme 1.5). Du Théorème 1.16 on en déduit que $n \leq m$ et qie $n \geq m$, et donc que $n = m$. **cqfd.**

Définition 1.18. Si E est un ensemble fini en bijection avec l'intervalle $[1,n]$, on dit que le **cardinal** de E est n, ou que le **nombre d'éléments** dans E est n, ce qu'on note $\boldsymbol{|E| = n}$. Lorsque E est vide, on posera $|E| = 0$.

1.5.1 Principe de bijection

Proposition 1.19 (Principe de bijection)**.** *Si E et F sont en bijection, alors $|E| = |F|$.*

Démonstration. Soit $f : E \to F$ une bijection. Soient $m = |F|$ et $g : F \to [1,m]$ une bijection. alors $g \circ f : E \to [1,m]$ est aussi une bijection. Par unicité du cardinal, $|E| = |F|$. **cqfd.**

Ce principe simple est très utile ! Il donne lieu aux preuves bijectives, une technique que nous allons utiliser à plusieurs reprises dans la suite.

1.5.2 Principe des tiroirs

Quelques conséquences du Théorème 1.16.

Corollaire 1.20 (Principe des tiroirs)**.** *Pour des ensembles finis E et F, il existe une injection de E dans F si et seulement si $|E| \leq |F|$.*

En particulier, si $|E| > |F|$ alors il n'y a pas d'injection de E dans F, et pour toute application $f : E \to F$ il existe au moins un élément $y \in F$ tel que $|f^{-1}(\{y\})| \geq 2$.

Démonstration. Soit $f : E \to F$ une injection. Notons $n = |E|$ et $m = |F|$. Par définition, il existent des bijections $g : E \to [1, n]$ et $h : F \to [1, m]$. Alors $h \circ f \circ g^{-1} : [1, n] \to [1, m]$ est aussi une injection, et donc $n \leq m$. **cqfd.**

Ce résultat est traditionnellement énoncé comme suit : *Si m objets sont répartis dans n tiroirs, et $m > n$, alors il existe au moins un tiroir contenant au moins deux objets.*

Il est très utile pour montrer l'existence des éléments avec des propriétés particulières. Voici quelques exemples d'applications du principe.

Exemple 1.21. Soit $n \in \mathbb{N}^*$. Montrer que si A est un sous-ensemble de $[1, 2n]$ de taille $n + 1$, alors A contient deux nombres premiers entre eux.

Démonstration. Ici, les $n + 1$ entiers de A jouent le rôle des *objets*, et les *tiroirs* sont les n intervalles de la forme $[2i - 1, 2i]$ avec $1 \leq i \leq n$. Le principe des tiroirs certifie qu'il y a deux nombres consécutifs dans A, et deux nombres consécutifs sont toujours premiers entre eux. **cqfd.**

Exemple 1.22. Soit $n \in \mathbb{N}^*$. Montrer que si A est un sous-ensemble de $[1, 2n]$ de taille $n + 1$, alors A contient deux nombres a et b tels que $a \mid b$.

Démonstration. Comme dans l'exemple précédent, les $n + 1$ entiers de A sont les *objets*. Pour définir les *tiroirs*, il faut écrire chaque nombre $a_1, \ldots, a_{n+1}$ de A sous la forme $a_i = 2^{u_i} v_i$, où v_i est impair. Notons que v_i ne peut prendre que n valeurs possibles, qui joueront le rôle des *tiroirs*. Il existe donc un $v \in \mathbb{N}^*$ tel que A contient deux nombres de la forme $2^{u_i} v$ et $2^{u_j} v$, pour quelques $u_i, u_j \in \mathbb{N}$. Celui avec la valeur de u_i plus petite divise l'autre. **cqfd.**

Il y a des versions plus fortes de ce principe, que nous allons traiter dans les exercices.

Nous finissons avec une dernière conséquence du Théorème 1.16 :

Corollaire 1.23 (Principe d'inclusion)**.** *Soit F une partie d'un ensemble fini E. Alors $|F| \leq |E|$, et $|F| = |E|$ si et seulement si $F = E$.*

Démonstration. La restriction de l'application identité sur F, $\mathrm{id}\big|_F : F \to E$, est injective, et donc $|F| \leq |E|$.

Supposons que $|F| = |E|$. Si $E \neq F$, alors il existe $e \in E$ tel que $e \notin F$. Alors $F \subseteq E \setminus \{e\}$ et $|F| \leq |E \setminus \{e\}|$. C'est facile à voir que $|E \setminus \{e\}| = |E| - 1$, ce qui amène à une contradiction qui finit la preuve. **cqfd.**

1.6 Équipotence et ensembles infinis dénombrables

Un ensemble est dit **infini** s'il n'est pas fini, comme par exemple l'ensemble des entiers naturels $\mathbb{N}$. Nous voulons classifier les ensembles qui ont la même "taille" que $\mathbb{N}$. Comment peut-on comparer la "taille" des ensembles infinis ? On prend le principe de bijection comme base, et on compare des ensembles avec des fonctions.

Définition 1.24. Soient E et F des ensembles. On dit qu'ils sont **équipotents** s'il existe une bijection entre E et F.

On aurait pu se baser sur le principe d'inclusion, et dire que E est plus petit que F lorsqu'il existe une injection de E dans F. Le théorème suivant montre que ces deux notations sont compatibles. La preuve ne fait pas partie du programme du cours.

Théorème 1.25 (Cantor-Bernstein)**.** *Soient E et F deux ensembles. S'il existe une injection de E dans F et une injection de F dans E, alors il existe une bijection de E dans F.*

Définition 1.26. On dit qu'un ensemble est **infini dénombrable** s'il est équipotent à $\mathbb{N}$.

Certains ensembles classiques sont dénombrables :

Proposition 1.27. *$\mathbb{N}^*$, $2\mathbb{N} = \{0, 2, 4, \ldots\}$, $\mathbb{Z}$ et $\mathbb{N} \times \mathbb{N}$ sont des ensembles infinis dénombrables.*

Démonstration. $\mathbb{N}^*$ est dénombrable car l'application

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N}^* \\ x &\mapsto x + 1 \end{aligned}$$

est bijective.

$2\mathbb{N}$ est dénombrable car l'application

$$\begin{aligned} f : \mathbb{N} &\to 2\mathbb{N} \\ x &\mapsto 2x \end{aligned}$$

est bijective.

$\mathbb{Z}$ est dénombrable car l'application

$$g : \mathbb{Z} \to \mathbb{N}$$
$$x \mapsto \begin{cases} 2x \text{ si } x \geq 0, \\ -2x + 1 \text{ si } x < 0. \end{cases}$$

est bijective.

$\mathbb{N} \times \mathbb{N}$ est dénombrable car l'application

$$h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}^*$$
$$(x, y) \mapsto 2^x(2y + 1)$$

est bijective.

Nous laissons la vérification de la bijectivité de ces fonctions au lecteur. **cqfd.**

Proposition 1.28. *Tout sous-ensemble $E \subseteq \mathbb{N}$ est soit fini, soit infini dénombrable.*

Démonstration. Supposons que $E \subseteq \mathbb{N}$ n'est pas fini. On construit par récurrence une fonction $f : \mathbb{N} \to E$. On prend $f(0) = \min E$, $f(1) = \min E \backslash \{f(0)\}$, et de façon récurrente $f(n) = \min E \setminus \{f(0), \ldots, f(n-1)\}$. Notez que f est une application bien définie car tout sous-ensemble non-vide de E a un élément minimal, et $E \setminus \{f(0), \ldots, f(n-1)\}$ est non-vide car E est infini.

Montrons que f est une bijection. Par construction, f est injective, car si $n < m$, alors $f(m) \in E \backslash \{f(0), \ldots, f(n), \ldots, f(m-1)\}$ et donc $f(n) \neq f(m)$. Pour montrer que f est aussi surjective, nous supposons le contraire. C'est-à-dire qu'il existe $n \in E \setminus \{f(0), f(1), \ldots\}$. Soit $S = \{i : f(i) > n\}$, qui est un ensemble non-vide et donc a un plus petit élément k. Ceci veut dire que $f(0) < \cdots < f(k-1) < n < f(k)$, ce qui contredit l'élection de $f(k)$ comme le plus petit élément de $E \setminus \{f(0), \ldots, f(k-1)\}$. **cqfd.**

Proposition 1.29. *$\mathbb{Q}$ est infini dénombrable.*

Démonstration. L'application identité est une injection de $\mathbb{N}$ dans $\mathbb{Q}$, ce qui montre que $\mathbb{Q}$ est infini. L'application $\frac{p}{q} \mapsto (p, q)$, où $\frac{p}{q}$ est irréductible et $q > 0$, est une injection de $\mathbb{Q}$ dans $\mathbb{Z} \times \mathbb{N}^*$. Si on la composée avec l'application h de la preuve de la Proposition 1.27, on obtient une injection de $\mathbb{Q}$ dans $\mathbb{N}$. C'est donc une bijection avec un sous-ensemble de $\mathbb{N}$. De la proposition précédente, $\mathbb{Q}$ est infini dénombrable. **cqfd.**

Mais il existe des cardinaux infinis plus grands. Par exemple, le Théorème de Cantor nous montre que $\mathcal{P}(\mathbb{N})$ n'est pas dénombrable.

Théorème 1.30 (Cantor)**.** *Soit E un ensemble, alors E et $\mathcal{P}(E)$ ne sont pas équipotents.*

Démonstration. Supposons par l'absurde qu'il existe une surjection $f : E \to \mathcal{P}(E)$. Soit $A = \{x \in E : x \notin f(x)\} \in \mathcal{P}(E)$. Comme f est surjective, il existe $a \in E$ tel que $f(a) = A$. Alors,

$$a \in A \Leftrightarrow a \notin f(a) \Leftrightarrow a \notin A$$

ce qui est une contradiction. **cqfd.**

En exercice, nous allons en déduire que $\mathbb{R}$ n'est pas dénombrable non-plus.

Chapitre 2

Dénombrement

2.1 Principes de dénombrement

L'objet général de la combinatoire énumérative est de "calculer" le cardinal des ensembles particuliers. La plupart du temps, l'ensemble considéré dépend d'un ou plusieurs paramètres, et il s'agit d'exprimer ce cardinal comme fonction de ces paramètres.

Nous allons commencer avec des principes très simples qui décrivent les cardinaux obtenus avec des opérations ensemblistes. Ceci nous permettra de réduire des problèmes de dénombrement complexes à des cas plus simples.

2.1.1 Principe d'addition

Proposition 2.1 (Principe d'addition)**.** *Si E et F sont des ensembles finis disjoints ($E \cap F = \varnothing$), alors $|E \cup F| = |E| + |F|$.*

Démonstration. Si $E = \varnothing$ ou $F = \varnothing$, le résultat est immédiat. Supposons, $E, F \neq \varnothing$, et posons $|E| = n \geq 1$ et $|F| = m \geq 1$. Par définition, il existent des bijections $f : E \to [1, n]$ et $g : F \to [1, m]$. L'application

$$h : E \cup F \to [1, n+m]$$
$$x \to \begin{cases} f(x), \text{ si } x \in E, \\ g(x) + n, \text{ si } x \in F. \end{cases}$$

est clairement une bijection (vérifiez-le !). On en déduit que $|E \cup F| = n + m = |E| + |F|$. **cqfd.**

Et si on raisonne par récurrence sur n, on en obtient le résultat suivant :

Corollaire 2.2. *Soient $E_1, \ldots, E_n$ des ensembles finis deux à deux disjoints. Alors,*

$$\left|\bigcup_{i=1}^{n} E_i\right| = \sum_{i=1}^{n} |E_i|.$$

On peut dire aussi quelque chose si les ensembles ne sont pas disjoints. Traiter la réunion de trois ou plus ensembles pas forcement disjoints est plus compliqué, et nous le ferons dans la Section 2.5

Corollaire 2.3. *Soient E et F ensembles finis. Alors $|E \cup F| = |E| + |F| - |E \cap F|$.*

Démonstration. Soit $G = E \cap F$. Alors $E \setminus G$, $F \setminus G$ et G sont disjoints, donc

$$\begin{aligned} |E \cup F| &= |E \setminus G| + |F \setminus G| + |G| = |E \setminus G| + |G| + |F \setminus G| + |G| - |G| \\ &= |E| + |F| - |E \cap F|. \end{aligned}$$

Où on a utilisé que $|E| = |G| + |E \setminus G|$ et $|F| = |G| + |F \setminus G|$. **cqfd.**

2.1.2 Principe des bergers

On va formaliser le principe des bergers qui informellement dit : *Pour compter les moutons il suffit de compter les pattes et diviser par* 4. Malgré sa simplicité, il s'agit d'un principe très utile, et que nous allons exploiter très souvent.

Proposition 2.4. *Soient E et F deux ensembles finis et $f : E \to F$. Alors $|E| = \sum_{y \in F} |f^{-1}(y)|$.*

Démonstration. Les ensembles $f^{-1}(y)$ recouvrent E ($E = \bigcup_{y \in F} f^{-1}(y)$), et sont deux-à-deux disjoints ($f^{-1}(y) \cap f^{-1}(z) = \varnothing$ si $y \neq z$). On déduit l'égalité du principe d'addition. **cqfd.**

Corollaire 2.5. *Si $f : E \to F$ est surjective, alors $|F| \geq |E|$.*

Démonstration. Si $f : E \to F$ est surjective, alors $|f^{-1}(y)| \geq 1$ pour tout $y \in F$, et donc $|E| = \sum_{y \in F} |f^{-1}(y)| \geq \sum_{y \in F} 1 = |F|$. **cqfd.**

Corollaire 2.6 (Principe des bergers)**.** *Soient E et F deux ensembles finis et $f : E \to F$. S'il existe $p \in \mathbb{N}^*$ tel que $|f^{-1}(y)| = p$ pour tout $y \in F$, alors $|E| = p \cdot |F|$.*

2.1.3 Principe de multiplication

Proposition 2.7 (Principe de multiplication)**.** *Soient E et F ensembles finis, alors $|E \times F| = |E| \cdot |F|$.*

Démonstration. Considérons l'application

$$\begin{aligned} f : E \times F &\to F \\ (x, y) &\mapsto y. \end{aligned}$$

Alors $|f^{-1}(y)| = |E|$ pour tout $y \in F$. Du principe des bergers on en déduit $|E \times F| = |E|\,|F|$. **cqfd.**

Corollaire 2.8. *Soient $E_1, \ldots, E_n$ des ensembles finis. Alors*

$$|E_1 \times E_2 \times \cdots \times E_n| = |E_1| \cdot |E_2| \cdot \cdots \cdot |E_n|.$$

Ce résultat se visualise très bien sous la forme d'arbre de décision. Pour choisir un élément de $E_1 \times E_2 \times \cdots \times E_n$, il faut d'abord choisir un élément de E_1, pour lequel on a $|E_1|$ options ; après, pour chaque choix, il faut choisir un élément de E_2, pour lequel on a $|E_2|$ options, etc.

Corollaire 2.9. *Si E est un ensemble fini, alors $|E^n| = |E|^n$.*

C'est-à-dire, le nombre de mots de taille n sur un alphabet A avec k lettres est k^n.

Exemples 2.10.

- Combien de (possibles) mots de cinq lettres existe-t-il (en utilisant l'alphabet usuel de 26 lettres et prenant en compte les mots sans sens) ?

  26^5*, car un mot de cinq lettres est un* 5*-uplet d'éléments de* $\{a, b, c, d, \ldots, z\}$.

- Combien de nombres y-à-t'il avec au plus 3 chiffres (décimales) ?

  10^3*, car ils sont en bijection avec les* 5*-uplets d'éléments de* $[0, 9]$.

- Combien de nombres y-à-t'il avec au plus 3 chiffres, étant toutes paires ?

  5^3*, car ils sont en bijection avec les* 5*-uplets d'éléments de* $\{0, 2, 4, 6, 8\}$.

2.2 Comptage des applications

Nous allons appliquer ces techniques au dénombrement des applications (de divers types) entre deux ensembles finis.

2.2.1 Le nombre d'applications

Soient E et F des ensembles finis non-vides, et $\boldsymbol{\mathcal{F}(E,F)}= \{f : E \to F\}$ l'ensemble des applications de E dans F.

Observation 2.11. $|\mathcal{F}(\varnothing, F)| = 1$ pour tout ensemble F, mais si $E \neq \varnothing$ alors $|\mathcal{F}(E, \varnothing)| = 0$.

Proposition 2.12. $|\mathcal{F}(E,F)| = |F|^{|E|}$.

Démonstration. Soit $n = |E|$. On montre que les ensembles $\mathcal{F}(E,F)$ et F^n sont en bijection. En effet, posons $E = \{x_1, \ldots, x_n\}$, alors

$$\begin{aligned} \phi : \mathcal{F}(E,F) &\to F^n \\ f &\mapsto (f(x_1), \ldots, f(x_n)) \end{aligned}$$

est une bijection. D'où $|\mathcal{F}(E,F)| = \left|F^{|E|}\right| = |F|^{|E|}$. **cqfd.**

L'ensemble $\mathcal{F}(E,F)$ est parfois noté tout simplement F^E.

Théorème 2.13. *Soit E un ensemble fini. Le nombre de sous-ensembles de E est*

$$|\mathcal{P}(E)| = 2^{|E|}.$$

Pour la preuve, nous avons besoin du concept de **fonction caractéristique** d'une partie A de E. C'est l'application $f_A : E \to \{0,1\}$ telle que

$$f_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} .$$

Démonstration. L'application

$$\begin{aligned} \phi : \mathcal{P}(E) &\to \mathcal{F}(E, \{0,1\}) \\ A &\mapsto f_A \end{aligned}$$

est une bijection (vérifiez-le !). Du principe de bijection

$$|\mathcal{P}(E)| = |\mathcal{F}(E, \{0,1\})| = |\{0,1\}|^{|E|} = 2^{|E|}.$$ **cqfd.**

2.2.2 Le nombre d'injections

On rappelle d'abord la définition de la fonction factorielle, qui apparaîtra dans nos formules.

Définition 2.14. La **factorielle** de l'entier naturel $n \in \mathbb{N}$ est le nombre $n! \in \mathbb{N}$ défini par la formule :

$$n! = \prod_{1 \leq i \leq n} i = \begin{cases} 1 & \text{si } n = 0, \\ n \cdot (n-1)! & \text{sinon.} \end{cases}$$

Soit $\mathcal{F}_{inj}(E, F)$ l'ensemble des injections de E dans F.

Proposition 2.15. *Soient E, F ensembles finis, de cardinaux respectifs $|E| = k \geq 1$ et $|F| = n \geq 1$. Le nombre d'injections de E dans F est exactement :*

$$|\mathcal{F}_{inj}(E, F)| = n(n-1)\cdots(n-k+1) = \prod_{i=0}^{n-1}(n-i) = \begin{cases} 0 & \textit{si } n < k, \\ \frac{n!}{(n-k)!} & \textit{si } n \geq k. \end{cases}$$

Démonstration. Soient $E = \{x_1, \ldots, x_k\}$ et $F = \{y_1, \ldots, y_n\}$. On fait la preuve par récurrence sur k.

Initialisation : Si $k = 1$, $E = \{x_1\}$ et il y a n fonctions injectives de E dans F, qui représentent les n possibles valeurs de $f(x_1)$.

Hérédité : Supposons $k \geq 2$. On considère l'application

$$\begin{aligned} \phi : \mathcal{F}_{inj}(E, F) &\to \mathcal{F}_{inj}(E \setminus \{x_k\}, F) \\ f &\mapsto f\big|_{E\setminus\{x_k\}} \end{aligned}$$

où $f\big|_{E\setminus\{x_k\}}$ est la restriction de f sur $E \setminus \{x_k\}$.

On observe que l'image réciproque d'une fonction de $\mathcal{F}_{inj}(E \setminus \{x_k\}, F)$ par ϕ a cardinal $n - (k-1)$, qui correspond aux $n - (k-1)$ possibles éléments de F qui no sont dans l'image de $x_1, \ldots, x_{k-1}$. Du principe des bergers, et par récurrence

$$|\mathcal{F}_{inj}(E, F)| = |\mathcal{F}_{inj}(E \setminus \{x_k\}, F)| \cdot (n-k+1) = (n(n-1)\cdots(n-k+2))(n-k+1)$$

cqfd.

Les injections de $[1, k]$ dans F sont en bijection avec les ***k*-arrangements** d'éléments de F. Un k-arrangement d'éléments de F est un k-uplet $(a_1, \ldots, a_k) \in F^k$ tel que $a_i \neq a_j$ pour tout $1 \leq i < j \leq k$. C'est à dire, des mots de longueur k sur l'alphabet F qui ne contiennent pas des lettres répétées. intuitive, on a n choix pour le premier élément, $n-1$ choix pour le deuxième une fois le premier a été fixé, et ainsi jusqu'à $n - (k-1)$ choix pour le dernier.

2.2.3 Le nombre de bijections

Le nombre de bijections découle très facilement du nombre d'injections. On a tout simplement besoin du lemme suivant.

Lemme 2.16. *Si $|E| = |F|$ pour des ensembles finis E et F, alors les propriétés suivantes sont équivalentes pour une application $f : E \to F$:*
(i) f est injective,
(ii) f est surjective,
(iii) f est bijective.

Remarque 2.17. Ce lemme est caractéristique des ensembles finis.

Corollaire 2.18. *Soient E et F des ensembles finis de cardinal n. Le nombre de bijections de E dans F est $n!$.*

Une application bijective d'un ensemble fini E dans lui-même est appelée une **permutation** de l'ensemble E. (L'ensemble de bijections de $[1, n]$ das lui-même forme un groupe très important, le groupe symétrique S_n, voir UE 2M175.)

2.2.4 Une estimation de la fonction factorielle

Il est souvent très utile d'encadrer des fonctions compliquées par des fonctions "plus simples". On va essayer de comprendre la croissance de la fonction factorielle lorsque $n \to \infty$.

Une première approximation donne que

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

car

$$n! = \prod_{i=2}^{n} i \leq \prod_{i=2}^{n} n = n^{n-1}; \qquad n! = \prod_{i=2}^{n} i \geq \prod_{i=2}^{n} 2 = 2^{n-1}.$$

Voici une estimation un peu plus précise de la fonction factorielle. On a besoin du résultat suivant :

Lemme 2.19 (Inégalité entre moyennes arithmétique et géométrique)**.** *Soient a, b des réels ≥ 0. Alors*

$$\frac{a+b}{2} \leq \sqrt{ab},$$

avec égalité si et seulement si $a = b$.

Démonstration. Suit de

$$0 \leq (\sqrt{a} - \sqrt{b})^2 = a + b - 2\sqrt{ab}.$$

cqfd.

Théorème 2.20. *Pour tout $n \geq 1$,*

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

Démonstration. On considère les produits de la forme $i(n+1-i)$. Dans $\prod_{i=1}^{n} i(n+1-i)$, chaque $i \in [1, n]$ apparaît deux fois, et donc ce produit est égal à $(n!)^2$. En prenant la racine carrée :

$$\prod_{i=1}^{n} \sqrt{i(n+1-i)} = n!.$$

Si on applique l'inégalité arithmétique-géométrique, on obtient

$$\sqrt{i(n+1-i)} \leq \frac{i+n+1-i}{2} = \frac{n+1}{2}.$$

D'où

$$n! = \prod_{i=1}^{n} \sqrt{i(n+1-i)} \leq \prod_{i=1}^{n} \frac{n+1}{2} = \left(\frac{n+1}{2}\right)^n.$$

Pour le minorant, il suffit de montrer que $i(n+1-i) \geq n$ pour tout $i \in [1, n]$. Si $i = 1$ ou $i = n$, ceci est vrai avec égalité. Si $i \neq 1, n$, alors on a un produit de deux nombres, le plus grand desquels vaut au moins $\frac{n}{2}$, et le plus petit au moins 2. D'où $i(n+1-i) \geq 2\frac{n}{2} = n$, et

$$n! = \prod_{i=1}^{n} \sqrt{i(n+1-i)} \geq \prod_{i=1}^{n} \sqrt{n} = n^{n/2}.$$

cqfd.

Ces inégalités peuvent être raffinés et faites plus précises. En fait, on peut faire une estimation asymptotique très précise, grâce à la formule de Stirling, que nous n'allons pas démontrer.

Théorème 2.21 (Formule de Stirling)**.**

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.$$

C'est à dire

$$\lim_{n\to\infty} \frac{n!}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} = 1.$$

2.2.5 Surjections et partitions

Soit $\boldsymbol{S(n,k)}$ le nombre de partitions d'un ensemble E de cardinal n en k parties. Les nombres $S(n,k)$ sont appelés les **nombres de Stirling** (de deuxième type). (On peut parfois trouver la notation $\left\{ {n \atop k} \right\}$ ou $S_{n,k}$ pour $S(n,k)$.)

Observation 2.22.

$$S(n,1) = 1, \qquad S(n,2) = 2^{n-1} - 1, \qquad S(n,n-1) = \binom{n}{2}, \qquad S(n,n) = 1.$$

Démonstration. Il y a une seule partition de E en une partie ou $|E|$ parties, elles sont $\{E\}$ et $\{\{e\} : e \in E\}$ respectivement. Chaque partition en 2 parties consiste en une paire de parties non-vides complémentaires $\{A, E \setminus A\}$. Il y a $2^n - 2$ parties non-vides, et chaque partition est comptée deux fois, d'où $S(n,2) = \frac{2^n-2}{2} = 2^{n-1} - 1$. Finalement, une partition en $n-1$ parties est toujours formée d'une paire et le reste sont des singletons. On en déduit que $S(n,n-1)$ coïncide avec le nombre de paires $\binom{n}{2}$. **cqfd.**

Les surjections et les partitions sont fortement liées.

Proposition 2.23. *Soient E et F des ensembles finis non-vides de cardinaux respectifs n et k, avec $n \geq k$. Le cardinal de l'ensemble de surjections $\mathcal{F}_{surj}(E,F)$ est*

$$|\mathcal{F}_{surj}(E,F)| = k! \cdot S(n,k).$$

Démonstration. À toute surjection $f : E \to F = \{y_1, \ldots, y_k\}$ on fait correspondre une partition de E en k classes distinctes : $f^{-1}(y_1), \ldots, f^{-1}(y_k)$. Il y a $k!$ surjections (qui correspondent aux $k!$ permutations de F) qui donnent la même partition. On obtient le résultat du principe des bergers. **cqfd.**

Théorème 2.24. *Soit $n, k \in \mathbb{N}$ tels que $1 \leq k \leq n$, on a :*

$$S(n,k) = \begin{cases} 1 \quad si\ k \in \{1,n\}, \\ S(n-1,k-1) + kS(n-1,k) \quad si\ 2 \leq k \leq n-1. \end{cases}$$

Démonstration. On considère des partitions de $E = [1,n]$. Le résultat est trivial pour $k = 1$ ou $k = n$, car il y a une seule partition de $[1,n]$ en 1 ou n parties. Pour $2 \leq k \leq n-1$, on considère deux types de partitions :

- les partitions où une des parties est le singleton $\{n\}$. Il y a $S(n-1,k-1)$ partitions de ce type, qui correspondent aux possibles partitions de $[1,n-1]$ en k parties.

- les partitions $[1,n] = A_1 \cup \cdots \cup A_k$ où la classe A_i qui contient n contient au moins un autre élément (dans la preuve, appelons-lez partitions de type 2). Alors $[1,n-1] = \tilde{A}_1 \cup \cdots \cup \tilde{A}_k$, où $\tilde{A}_i = A_i \setminus \{n\}$. Il y a k partitions de type 2 de $[1,n]$ qui donnent lieu à la même partition de $[1,n-1]$ (une pour chaque possible A_i qui pourrait contenir n). Du principe des bergers on a qu'il y a $kS(n-1,k)$ partitions de type 2. **cqfd.**

Cette récurrence nous permet calculer les nombres de Stirling de deuxième type (et donc le nombre de surjections aussi).

n	$S(n,1)$	$S(n,2)$	$S(n,3)$	$S(n,4)$	$S(n,5)$	$S(n,6)$	$S(n,7)$
1	1						
2	1	1					
3	1	3	1				
4	1	7	6	1			
5	1	15	25	10	1		
6	1	31	90	65	15	1	
7	1	63	301	350	140	21	1

2.3 Nombres binomiaux

2.3.1 L'ensemble de parties de taille k

Soit E un ensemble fini, on note $\boldsymbol{\mathcal{P}_k(E)}$ l'ensemble de parties de E de cardinal k, qu'on appelle ses ***k*-parties** ou parfois ses ***k*-combinaisons**.

Définition 2.25. On note $\binom{n}{k}$, le **nombre ou coefficient binomial** (lu "k parmi n"), le nombre de parties à k éléments d'un ensemble de cardinal n :

$$\binom{n}{k} = |\mathcal{P}_k([1,n])|.$$

Ce nombre est parfois noté C_n^k (lu "combinaison de k parmi n").

Nous pouvons montrer de façon combinatoire plusieurs propriétés des nombres binomiaux. En particulier, quelques de ces observations combinatoires vont nous permettre calculer les nombre binomiaux.

Proposition 2.26. *Pour $n \in \mathbb{N}$ et $0 \leq k \leq n$,*

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

Démonstration. L'application

$$\begin{aligned}\phi : \mathcal{P}_k([1,n]) &\to \mathcal{P}_{n-k}([1,n]) \\ E &\mapsto [1,n] \setminus E\end{aligned}$$

est une bijection, et donc

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

cqfd.

Proposition 2.27. *Pour $n \in \mathbb{N}$,*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Démonstration. L'ensemble de parties de $[1,n]$ est l'union disjointe des ensembles de k-parties de $[1,n]$, où k varie de 1 à n. **cqfd.**

Proposition 2.28 (Identité de Pascal)**.**

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

Démonstration. Soient $n \geq k \geq 1$. On peut décomposer $\mathcal{P}_k([1,n])$ en deux groupes disjoints. D'un coté, l'ensemble des parties qui ne contiennent pas n. Il en y a $|\mathcal{P}_k([1,n-1])| = \binom{n-1}{k}$. Les parties E qui contiennent n sont en bijection avec $\mathcal{P}_{k-1}([1,n-1])$. L'application bijective est $E \mapsto E \setminus \{n\}$. Du principe d'addition, on en déduit que

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

cqfd.

Cette identité est très importante, car elle nous permet de calculer les coefficients binomiaux. On le fait avec le **triangle de Pascal** :

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
7	1	7	21	35	35	21	7	1

Proposition 2.29. *Soit $n \in \mathbb{N}^*$ et $k \in [0, n]$. Alors,*

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

Démonstration. Soit E un ensemble de cardinal n. On considère l'ensemble $\mathcal{C} = \{(x, S) \in E \times \mathcal{P}_k(E) : x \in S\}$.

- L'application $\phi : \mathcal{C} \to \mathcal{P}_k(E)$ telle que $(x, S) \mapsto S$ vérifie $|\phi^{-1}(S)| = |S| = k$ pour tout $S \in \mathcal{P}_k(E)$. D'où

$$|\mathcal{C}| = k|\mathcal{P}_k(E)| = k\binom{n}{k}.$$

- L'application $\psi : \mathcal{C} \to E$ telle que $(x, S) \mapsto x$ vérifie $|\phi^{-1}(x)| = |\mathcal{P}_{k-1}(E \setminus \{x\}| = \binom{n-1}{k-1}$ pour tout $S \in \mathcal{P}_k(E)$. D'où

$$|\mathcal{C}| = \binom{n-1}{k-1}|E| = n\binom{n-1}{k-1}.$$

cqfd.

Ici, nous avons utilisé la technique du **double décompte** (aussi appelée le **principe de Fubini**). Elle consiste en calculer le cardinal d'un sous-ensemble d'un produit cartésien de deux façons distinctes (par "lignes" et par "colonnes", si l'on représente le produit cartésien sous la forme d'une matrice). Le résultat, bien sûr, doit être le même calculé des deux façons.

En effet, soient $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_m\}$ et $S \subseteq A \times B$. Et soient

$$s(a_i, *) = \{(a, b) \in S : a = a_i\}$$
$$s(*, b_j) = \{(a, b) \in S : b = b_j\}.$$

Alors, du principe d'addition, on a

$$|S| = \sum_{i=1}^{n} |s(a_i, *)| = \sum_{j=1}^{m} |s(*, b_j)|.$$

On finalise avec une formule pour les coefficients binomiaux :

Théorème 2.30. *Soit E un ensemble fini de cardinal n.*

$$|\mathcal{P}_k(E)| = \binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{si } 0 \leq k \leq n \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. On considère l'application ϕ des k-arrangements (k-uplets avec toutes ses coordonnées distinctes) vers les k-parties qui 'oublie l'ordre' :

$$\phi((a_1, \ldots, a_k)) = \{a_1, \ldots, a_k\}.$$

Pour chaque partie $A \in \mathcal{P}_k(E)$, il y a $|\phi^{-1}(A)| = k!$ k-arrangements avec ce support (car il y a $k!$ façons d'ordonner les k éléments de A, les $k!$ bijections $A \to [1, k]$). Comme il y a $\frac{n!}{(n-k)!}$ k-arrangements, d'après le lemme des bergers, on a

$$k!\,|\mathcal{P}_k(E)| = \frac{n!}{(n-k)!}.$$

cqfd.

2.3.2 Multi-ensembles

Soit E un ensemble, parfois il est utile de représenter une sélection d'éléments de E qui ne sont pas forcement distincts. C'est à dire, un sous-ensemble avec répétition. On définit les multi-ensembles en termes d'applications, en étendant la représentation des parties avec des fonctions caractéristiques $E \to \{0, 1\}$.

Définition 2.31. Soit E un ensemble fini. Un **multi-ensemble** sur E est une application f de E dans $\mathbb{N}$. La **multiplicité** de $e \in E$ est $f(e)$ et la **taille** du multi-ensemble est $\sum_{e \in E} f(e)$.

Les multi-ensembles de taille k sont parfois appelés ***k*-combinaisons avec répétition**, et on les note parfois avec des accolades doubles $\{\!\{\ldots\}\!\}$ encadrant les éléments répétés autant de fois que leur multiplicité.

Exemple 2.32. Soit $E = \{a, b, c, d\}$, la sélection avec répétition $\{\!\{a, a, c, d, d, d\}\!\}$ correspond au multi-ensemble donnée par l'application f définie par

$$f(a) = 2, f(b) = 0, f(c) = 1, f(d) = 3.$$

La taille du multi-ensemble est 6.

Observation 2.33. Si E est un ensemble fini de cardinal n, le nombre de multi-ensembles de E de taille k est le nombre de solutions de l'équation

$$a_1 + \cdots + a_n = k \tag{2.1}$$

avec $(a_1, \ldots, a_n) \in \mathbb{N}^n$.

Démonstration. Pour $E = \{x_1, \dots, x_n\}$, et $f : E \to \mathbb{N}$ un multi-ensemble de taille k, on a $f(x_1) + \cdots + f(x_n) = k$, et donc les n-uplet $(f(x_1), \dots, f(x_n))$ est une solution de (2.1). Réciproquement, chaque solution $(a_1, \dots, a_n)$ donne lieu au multi-ensemble $x_i \mapsto a_i$. **cqfd.**

Le nombre de multi-ensembles de E de taille k est parfois noté $\left(\!\binom{n}{k}\!\right)$ en analogie avec la notation des coefficients binomiaux.

Théorème 2.34. *Si E est un ensemble fini de cardinal n, le nombre de multi-ensembles de E de taille k est*

$$\left(\!\binom{n}{k}\!\right) = \binom{k+n-1}{k}.$$

Preuve formelle. L'application qui chaque multi-ensemble de $[1, n]$ de taille k de la forme $\{1 \leq a_1 \leq a_2 \leq \cdots \leq a_k \leq n\}$ associe la k-partie de $[1, n+k-1]$ $\{1 \leq a_1 < a_2 + 1 < a_3 + 2 < \cdots < a_k + k - 1 \leq n + k - 1\}$ est une bijection (vérifiez-le !). **cqfd.**

Preuve informelle. On répartit k balles indistinguables parmi n boîtes numérotées. Pour représenter une distribution, on dessine les balles sur une ligne et on utilise $n-1$ barres verticales pour représenter les séparations entre deux boîtes consécutives. L'exemple précédent donne le dessin suivant :

$$\circ\circ \,||\, \circ \,|\, \circ\circ$$

Cette représentation contient toute l'information de la répartition, et la détermine uniquement. Par conséquent, choisir une répartition des balles revient à sélectionner la position des barres parmi les balles. On a $k+n-1$ positions (pour les barres et balles) et il faut choisir quelles vont être occupées par les barres. C'est à dire, on a $\binom{k+n-1}{k}$ choix possibles. **cqfd.**

2.3.3 Formule du binôme

Théorème 2.35 (Binôme de Newton)**.** *Dans tout anneau commutatif*[1]

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

1. Un ensemble $\mathcal{A}$ muni de deux lois de composition interne, somme '+' et produit '$\cdot$', telles que : $(\mathcal{A}, +)$ est un groupe abélien (+ associative, commutative, avec neutre et opposé) ; $(\mathcal{A}, \cdot)$ est un monoïde commutatif (associative, commutative, avec neutre) ; et la multiplication est distributive par rapport à la somme.

Preuve combinatoire.

$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ fois}}$$

un terme du développement de ce produit est obtenu en choisissant soit a, soit b dans chaque facteur. Pour le terme $a^k b^{n-k}$, il faut compter les façons de choisir k fois a et $n-k$ fois b, donc exactement $\binom{n}{k}$. **cqfd.**

Preuve calculatoire. Par récurrence sur n.

Initialisation : Pour $n = 0$, $(a+b)^0 = 1 = \binom{0}{0} a^0 b^0$.

Hérédité : Supposons que la propriété est vraie au rang $n \geq 0$, et montrons qu'elle est vraie au rang $n+1$. On a

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

cqfd.

2.4 Les nombres multinomiaux

Définition 2.36. Etant donné un r-uplet $(k_1, k_2, \ldots, k_r)$ d'entiers naturels de somme n, on définit le **coefficient multinomial**

$$\binom{n}{k_1, k_2, \ldots, k_r}$$

comme le nombre de r-uplets $(A_1, A_2, \ldots, A_r)$ de parties disjointes d'un ensemble E de cardinal n (ex. $[1, n]$) telles que $\forall i,\ |A_i| = k_i$. [2]

2. Ceci n'est pas forcement une partition si un des k_i's est 0.

Observation 2.37. $\binom{n}{1,\dots,1} = n!$ et $\binom{n}{k,n-k} = \binom{n}{k} = \binom{n}{n-k}$.

Observation 2.38. Équivalemment, $\binom{n}{k_1,k_2,\dots,k_r}$ est

1. le nombre de "permutations" d'un multi-ensemble sur $[1,r]$ de taille n dont les éléments ont multiplicités respectives $k_1,\dots,k_r$;
2. le nombre d'anagrammes d'un mot de longueur n dont la i-ème lettre distincte apparaît k_i fois ;
3. le nombre d'applications f de $[1,n]$ dans $[1,r]$ telles que $|f^{-1}(i)| = k_i$ pour tout $1 \leq i \leq r$.

Démonstration.

1. À chaque permutation du multi-ensemble de taille n on fait correspondre le r-uplet $(A_1,\dots,A_r)$ où $A_i \subset [1,n]$ sont les positions occupées par l'élément i.
2. Pareil, en définissant $A_i \subset [1,n]$ comme l'ensemble des positions occupées par la i-ème lettre distincte.
3. À chaque telle surjection $f : [1,n] \to [1,r]$ on fait correspondre le r-uplet $(f^{-1}(1),\dots,f^{-1}(r))$.

cqfd.

Théorème 2.39.

$$\binom{n}{k_1,k_2,\dots,k_r} = \frac{n!}{k_1!k_2!\cdots k_r!}$$

Démonstration. Nous montrons le résultat par récurrence sur r. Il est vrai pour $r = 1$ car on récupère un coefficient binomial.

Si $r > 1$, on considère l'application ϕ qui à chaque r-uplet $(A_1,A_2,\dots,A_r)$ de parties de E disjointes vérifiant $|A_i| = k_i$, assigne la k_r-partie A_r. Comme $(A_1,\dots,A_{r-1})$ forment un $(r-1)$-uplet de parties disjointes de $E \setminus A_r$ vérifiant $|A_i| = k_i$, nous avons que chaque A_r distinct est l'image de $\binom{n-k_r}{k_1,\dots,k_{r-1}}$ r-uplets distincts. Du lemme des bergers, on en déduit que

$$\begin{aligned}\binom{n}{k_1,k_2,\dots,k_r} &= \binom{n}{k_r}\binom{n-k_r}{k_1,k_2,\dots,k_{r-1}} \\ &= \frac{n!}{(n-k_r)!k_r!} \cdot \frac{(n-k_r)!}{k_1!k_2!\cdots k_{r-1}!} = \frac{n!}{k_1!k_2!\cdots k_r!}.\end{aligned}$$

cqfd.

Dit autrement, on a $\binom{n}{k_1}$ choix pour le premier ensemble, $\binom{n-k_1}{k_2}$ choix pour le deuxième ensemble, jusqu'à $\binom{n-k_1-\cdots-k_{r-1}}{k_r}$ pour le dernier. Et donc,

$$\binom{n}{k_1}\binom{n-k_1}{k_2}\cdots\binom{n-k_1-\cdots-k_{r-1}}{k_r} = \frac{n!}{k_1!k_2!\cdots k_r!}.$$

Théorème 2.40 (Multinôme de Newton)**.** *Dans tout anneau commutatif*

$$(a_1 + a_2 + \cdots + a_r)^n = \sum_{k_1+k_2+\cdots+k_r=n} \binom{n}{k_1, k_2, \ldots, k_r} a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r}$$

Démonstration. Dans la multiplication $(a_1 + a_2 + \cdots + a_r)^n = (a_1 + a_2 + \cdots + a_r)\cdots(a_1 + a_2 + \cdots + a_r)$, chaque occurrence du terme $a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r}$ correspond à l'élection du terme a_1 dans k_1 des facteurs, le terme a_2 dans k_2 des facteurs, etc. **cqfd.**

2.4.1 Une estimation de $\binom{n}{k}$

Pour finir cette section, essayons de comprendre l'ordre de grandeur des nombres $\binom{n}{k}$. Une borne supérieure évidente est $\binom{n}{k} \leq n^k$.

Lemme 2.41. *Pour tout $x \in \mathbb{R}$, nous avons $1 + x \leq e^x$.*

Théorème 2.42. *Pour tout $n \geq 1$ et pour tout k tel que $1 \leq k \leq n$, nous avons*

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

Démonstration. Pour le minorant, on considère la description du coefficient binomial comme produit de fractions :

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} = \prod_{i=0}^{k-1} \frac{n-i}{k-i}.$$

Pour $n \geq k > i \geq 0$ on a $\frac{n-i}{k-i} \geq \frac{n}{k}$, d'où

$$\binom{n}{k} = \prod_{i=0}^{k-1} \frac{n-i}{k-i} \geq \prod_{i=0}^{k-1} \frac{n}{k} = \left(\frac{n}{k}\right)^k.$$

Pour le majorant, nous allons prouver une inégalité plus forte :

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

De la formule du binôme, on a que pour tout $X \in \mathbb{R}$,

$$\binom{n}{0} + \binom{n}{1}X + \binom{n}{2}X^2 + \cdots + \binom{n}{n}X^n = (1+X)^n.$$

Si $X > 0$, alors on peut supprimer quelques termes de la somme pour obtenir une inégalité

$$\binom{n}{0} + \binom{n}{1}X + \binom{n}{2}X^2 + \cdots + \binom{n}{k}X^k \leq (1+X)^n.$$

En divisant par X^k, on obtient

$$\frac{1}{X^k}\binom{n}{0} + \frac{1}{X^{k-1}}\binom{n}{1} + \frac{1}{X^{k-2}}\binom{n}{2} + \cdots + \binom{n}{k} \leq \frac{(1+X)^n}{X^k}.$$

Si additionnellement nous avons $X < 1$, alors on a que $\frac{1}{X^i} \geq 1$ pour tout $i \in \mathbb{N}^*$, et donc

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{k} \leq \frac{(1+X)^n}{X^k}.$$

Cette inégalité est valide pour tout $X \in]0,1[$. En particulier, pour $X = \frac{k}{n}$:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{k} \leq \left(1 + \frac{k}{n}\right)^n \left(\frac{n}{k}\right)^k.$$

On finit en appliquant le lemme précédent à $\left(1 + \frac{k}{n}\right)$

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{k} \leq \left(1 + \frac{k}{n}\right)^n \left(\frac{n}{k}\right)^k \leq \left(e^{\frac{k}{n}}\right)^n \left(\frac{n}{k}\right)^k = e^k \left(\frac{n}{k}\right)^k.$$

cqfd.

Pour avoir plus de précision dans nos estimations, il faudrait connaître la taille relative de k et n. Notez aussi que nous ne pouvons utiliser Stirling directement dans l'expression $\frac{n!}{k!(n-k)!}$, car k ne tend pas forcement vers ∞.

2.4.2 La "forme" de l'ensemble des coefficients binomiaux

On va essayer de comprendre la "forme" de l'ensemble des coefficients binomiaux $\binom{n}{k}$ pour un n fixé très grand. Nous avons déjà montré la symétrie de cet ensemble respecte $k = \frac{n-1}{2}$, $\binom{n}{k} = \binom{n}{n-k}$. En regardant le triangle de Pascal, on veut aussi que les nombres croissent jusqu'à la moité et qu'après ils décroissent. Montrons-le.

Lemme 2.43. *Pour $n, k \in \mathbb{N}$ avec $0 \leq k \leq n-1$,*

$$\begin{aligned}
\binom{n}{k} &< \binom{n}{k+1} && \text{si et seulement si } k < \frac{n-1}{2}, \\
\binom{n}{k} &= \binom{n}{k+1} && \text{si et seulement si } k = \frac{n-1}{2}, \text{ et} \\
\binom{n}{k} &> \binom{n}{k+1} && \text{si et seulement si } k > \frac{n-1}{2}.
\end{aligned}$$

Démonstration. À partir de l'expression en factorielles, on observe que

$$\frac{\binom{n}{k+1}}{\binom{n}{k}} = \frac{\frac{n!}{(k+1)!(n-k-1)!}}{\frac{n!}{k!(n-k)!}} = \frac{k!(n-k)!}{(k+1)!(n-k-1)!} = \frac{n-k}{k+1},$$

et donc $\frac{\binom{n}{k+1}}{\binom{n}{k}} > 1$ si et seulement si $n-k > k+1$, c'est à dire, $n-1 > 2k$. **cqfd.**

En particulier, les plus grands coefficients binomiaux sont ceux du milieu : $\binom{n}{n/2}$ si n est pair, et $\binom{n}{\lceil n/2 \rceil}$ et $\binom{n}{\lfloor n/2 \rfloor}$ si n es impair. Pour estimer sa taille, on observe d'abord que

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

On a le majorant car la somme de tous les coefficients binomiaux est 2^n. Pour le minorant, comme $\binom{n}{\lfloor n/2 \rfloor}$ est le plus grand des coefficients binomiaux, il doit être plus grand que leur moyenne, qui vaut $\frac{2^n}{n+1}$. Nous voyons donc qu'il s'agit d'un nombre de taille exponentielle en n.

Avec Stirling, on peut faire cette estimation beaucoup plus précise. Rappelons que

$$\binom{n}{n/2} = \frac{n!}{(n/2)!(n/2)!},$$

et que la formule de Stirling dit

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n, \qquad (n/2)! \sim \sqrt{\pi n}\left(\frac{n}{2e}\right)^{n/2};$$

et donc

$$\binom{n}{n/2} \sim \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{\left(\sqrt{\pi n}\left(\frac{n}{2e}\right)^{n/2}\right)^2} = \sqrt{\tfrac{2}{\pi n}}2^n.$$

On peut regarder $\binom{n}{k}$ comme une fonction de k pour un n fixé très grand. À mesure que n croit, le dessin de $\binom{n}{k}$ s'approche à une courbe en forme de cloche

centrée à $\frac{n}{2}$. Cette courbe limite, lorsque on la centre et l'escale convenablement, est la **courbe de Gauss** $x \mapsto e^{\frac{-x^2}{2}}$. Elle est très importante en probabilité et statistique, car c'est la fonction de densité de la distribution normale.

Plus précisément, la fonction $k \mapsto \frac{\binom{n}{k}}{2^n}$ s'approche à $x \mapsto \sqrt{\frac{2}{\pi n}} e^{\frac{-(x-(n/2))^2}{n/2}}$ lorsque $n \to \infty$.

2.5 Formule du crible

Le principe d'addition sert à calculer le cardinal de la réunion de plusieurs ensembles deux-à-deux disjoints. Comment fait-on s'ils ne sont pas disjoints ?

Si A_1 et A_2 sont deux ensembles pas forcement disjoints, alors on a vu que

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

Pour trois ensembles A_1, A_2, A_3, on peut raisonner cas par cas pour montrer que

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

Ceci se généralise à un nombre arbitraire d'ensembles comme suit :

Théorème 2.44. *(Formule du crible/Principe d'inclusion-exclusion)*
Soient $A_1, \ldots, A_n$ des ensembles finis. Alors,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{I \subseteq [1,n], I \neq \varnothing} (-1)^{|I|+1} \left|\bigcap_{i \in I} A_i\right|$$

Démonstration. Nous démontrons le théorème en utilisant les fonctions caractéristiques. On rappelle que la fonction caractéristique d'un partie A d'un ensemble E est l'application

$$\begin{aligned} f_A : E &\to \{0,1\} \\ x &\mapsto \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases} . \end{aligned}$$

Soient $\overline{A}_i$ les complémentaires des A_i pour $1 \leq i \leq n$. Notons $A = \bigcup_{i=1}^{n} A_i$ la réunion des A_i. Alors son complémentaire est

$$\overline{A} = \overline{\bigcup_{i=1}^{n} A_i} = \bigcap_{i=1}^{n} \overline{A}_i.$$

Comme $|A| = |E| - |\overline{A}|$, il suffit de calculer le cardinal de $\overline{A}$.

Nous allons utiliser trois propriétés des fonctions caractéristiques :

1)
$$f_{\overline{A}}(x) = 1 - f_A(x)$$

2)
$$f_{A\cap B}(x) = f_A(x) \cdot f_B(x)$$

3)
$$|A| = \sum_{x\in E} f_A(x)$$

Donc, on a

$$\begin{aligned}\left|\overline{A}\right| &= \sum_{x\in E} f_{\overline{A}}(x) = \sum_{x\in E} f_{\bigcap_{i=1}^n \overline{A}_i}(x) = \sum_{x\in E}\prod_{i=1}^n f_{\overline{A}_i}(x) = \sum_{x\in E}\prod_{i=1}^n (1 - f_{A_i}(x)) \\ &= \sum_{x\in E}\sum_{I\subseteq[1,n]} (-1)^{|I|}\prod_{i\in I} f_{A_i}(x) = \sum_{x\in E}\sum_{I\subseteq[1,n]} (-1)^{|I|} f_{\bigcap_{i\in I} A_i}(x) \\ &= \sum_{I\subseteq[1,n]} (-1)^{|I|}\sum_{x\in E} f_{\bigcap_{i\in I} A_i}(x) = \sum_{I\subseteq[1,n]} (-1)^{|I|}\left|\bigcap_{i\in I} A_i(x)\right|.\end{aligned}$$

Il en découle que

$$|A| = |E| - |\overline{A}| = |E| - \sum_{I\subseteq[1,n]} (-1)^{|I|}\left|\bigcap_{i\in I} A_i(x)\right| = \sum_{I\subseteq[1,n], I\neq\varnothing} (-1)^{|I|+1}\left|\bigcap_{i\in I} A_i(x)\right|,$$

où nous avons utilisé que $E = \bigcap_{i\in\varnothing} A_i(x)$, car c'est le terme qui ce correspond à la fonction caractéristique constante égale à 1. **cqfd.**

2.5.1 Le nombre de surjections, revisité

La formule du crible nous fournit une formule alternative de calculer $|\mathcal{F}_{surj}(E,F)|$, le nombre de surjections de E dans F.

Théorème 2.45. *Soient E et F des ensembles finis non-vides de cardinaux respectifs n et k, tels que $n \geq k$. Alors*

$$|\mathcal{F}_{surj}(E,F)| = \sum_{0\leq\ell\leq k} (-1)^{k-\ell}\binom{k}{\ell}\ell^n$$

Démonstration. Pour simplifier la notation, on pose $E = [1,n]$ et $F = [1,k]$. On considère l'ensemble $\mathcal{F}(E,F) \setminus \mathcal{F}_{surj}(E,F)$ des applications non surjectives de E dans F. Son cardinal est clairement $k^n - |\mathcal{F}_{surj}(E,F)|$.

Pour tout $i \in [1,k]$, notons

$$A_i = \left\{ f : E \to F : \ f^{-1}(i) = \varnothing \right\}.$$

La réunion des A_i est l'ensemble des applications qui ne sont pas surjectives. Pour tout $\varnothing \neq I \subseteq [1,k]$, on pose

$$A_I = \bigcap_{i \in I} A_i = \left\{ f : E \to F : \ f^{-1}(I) = \varnothing \right\},$$

et on remarque que $A_I = \mathcal{F}(E, F \setminus I)$, et donc $|A_I| = (k - |I|)^n$.

La formule du crible donne donc

$$\begin{aligned}
|\mathcal{F}_{surj}(E,F)| =& k^n - \left| \bigcup_{i=1}^{k} A_i \right| = k^n - \sum_{\varnothing \subsetneq I \subseteq [1,k]} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| \\
=& k^n - \sum_{\varnothing \subsetneq I \subseteq [1,k]} (-1)^{|I|-1} |A_I| = k^n - \sum_{\varnothing \subsetneq I \subseteq [1,k]} (-1)^{|I|-1} (k - |I|)^n \\
=& k^n - \sum_{1 \leq i \leq k} \sum_{\substack{I \subseteq [1,k] \\ |I|=i}} (-1)^{|I|-1} (k - |I|)^n = k^n - \sum_{1 \leq i \leq k} \sum_{\substack{I \subseteq [1,k] \\ |I|=i}} (-1)^{i-1} (k-i)^n \\
=& k^n - \sum_{1 \leq i \leq k} \binom{k}{i} (-1)^{i-1} (k-i)^n = k^n + \sum_{1 \leq i \leq k} \binom{k}{i} (-1)^{i} (k-i)^n \\
=& \sum_{0 \leq i \leq k} \binom{k}{i} (-1)^{i} (k-i)^n = \sum_{0 \leq \ell \leq k} \binom{k}{k-\ell} (-1)^{k-\ell} (\ell)^n \\
=& \sum_{0 \leq \ell \leq k} (-1)^{k-\ell} \binom{k}{\ell} (\ell)^n.
\end{aligned}$$

cqfd.

Chapitre 3

Fonctions génératrices

3.1 L'anneau des séries formelles

3.1.1 Rappel : L'anneau des polynômes

Soit $\mathcal{A}$ un anneau commutatif (nous sommes surtout intéressés par les cas $\mathcal{A} = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$). L'anneau des polynômes à coefficients dans $\mathcal{A}$ est l'anneau commutatif $\mathcal{A}[X]$ dont les éléments sont des suites finies $P = (p_i)_{0 \leq i \leq n}$, avec $p_i \in \mathcal{A}$ et $n \in \mathbb{N}$, qu'on écrit sous la forme

$$P(X) = p_0 + p_1 X + p_2 X^2 + \cdots + p_n X^n;$$

muni des lois de somme et produit suivantes :

Pour des polynômes $P(X) = \sum_{k \geq 0} p_k X^k$ et $Q(X) = \sum_{k \geq 0} q_k X^k$, où $p_i = q_j = 0$ pour tout $i > \deg(P)$ et $j > \deg(Q)$,

- la somme de P et Q est le polynôme $(P+Q)(X) = \sum_{k \geq 0} (p_k + q_k) X^k$, et
- le produit de P et Q est le polynôme $(PQ)(X) = \sum_{k \geq 0} \left(\sum_{i=0}^{k} p_i q_{k-i} \right) X^k$

Notez qu'ici, implicitement, on est en train de traiter les coefficients d'un polynôme comme une suite infinie dont tous les termes, sauf un nombre fini, sont 0. On dit qu'une telle suite infinie est à **support fini**.

L'anneau des polynômes est donc une structure algébrique sur l'ensemble de suites à support fini. Nous allons étendre cette structure à l'ensemble de toutes les suites.

3.1.2 Séries formelles

Soit $\mathcal{A}$ un anneau commutatif. Une **suite** à valeurs dans $\mathcal{A}$ est une application $f : \mathbb{N} \to \mathcal{A}$. On utilise souvent la notation $(a_n)_{n \in \mathbb{N}}$ pour désigner une suite f dont

$f(i) = a_i$. Nous allons représenter une suite $(a_n)_{n\in\mathbb{N}}$ comme les coefficients d'une **série formelle** infinie de la forme

$$A(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots = \sum_{n\geq 0} a_nX^n$$

qu'on appelle la **fonction génératrice** de $(a_n)_{n\in\mathbb{N}}$.

Définition 3.1. L'ensemble des **séries formelles** à coefficients dans $\mathcal{A}$, noté $\mathcal{A}[[X]]$ (e.g. $\mathbb{Z}[[X]]$, $\mathbb{Q}[[X]]$, $\mathbb{R}[[X]]$, $\mathbb{C}[[X]]$) est l'ensemble des suites à coefficients dans $\mathcal{A}$ muni des opérations suivantes :

- L'opération somme : Si $A(X) = \sum_{n\geq 0} a_nX^n$ et $B(X) = \sum_{n\geq 0} b_nX^n$ sont respectivement les fonctions génératrices de $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$, alors leur somme est

$$\begin{aligned} A(X) + B(X) &= (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \cdots \\ &= \sum_{n\in\mathbb{N}} (a_k + b_k)X^k \end{aligned}$$

  qui est la série génératrice de la suite $(a_n + b_n)_{n\in\mathbb{N}}$.

- L'opération produit, appelée produit de Cauchy : Si $A(X) = \sum_{n\geq 0} a_nX^n$ et $B(X) = \sum_{n\geq 0} b_nX^n$ sont respectivement les fonctions génératrices de $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$, alors leur produit (de Cauchy) est

$$\begin{aligned} A(X) \cdot B(X) &= (a_0b_0) + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots \\ &= \sum_{n\in\mathbb{N}} \left(\sum_{k=0}^{n} a_kb_{n-k} \right) X^k. \end{aligned}$$

  qui est la série génératrice de la suite $(\sum_{k=0}^{n} a_kb_{n-k})_{n\in\mathbb{N}}$.

Remarque 3.2. On pense aux séries formelles comme une notation alternative pour l'ensemble des suites. En particulier, la variable X ne prend pas de valeur. C'est un "marque-page" qui sert tout simplement à étiqueter les positions des coefficients.

De la même façon que les séries formelles généralisent les polynômes, les **séries entières** généralisent les fonctions polynomiales. Ces deux concepts sont fortement liés, et à cause de ça plusieurs résultats que vous connaissez sur les séries entières sont aussi vrais pour les séries formelles. Ils sont néanmoins deux concepts différents qui ne faut pas confondre. Les séries formelles sont un objet purement algébrique. En particulier, on ne se posera aucun problème de convergence.

Théorème 3.3. *Si $\mathcal{A}$ est un anneau commutatif, l'ensemble $\mathcal{A}[[X]]$ des séries formelles à coefficients dans $\mathcal{A}$ muni de la somme et le produit de Cauchy est un anneau commutatif. Les éléments neutres de l'addition et la multiplication sont les séries $(0,0,0,0,\dots)$ et $(1,0,0,0,\dots)$, et l'opposé de $A(X)$ est donné par $-A(X) = \sum_{n\geq 0}(-a_n)X^n$.*

3.1.3 Une justification pour la notation

À priori, la notation de somme dans la série formelle est purement formelle. Elle a quand même un sens.

Pour rendre la notation plus agile, pour tout $\lambda \in \mathcal{A}$ on écrit simplement λ pour désigner la série génératrice de la suite $(\lambda, 0, 0, \dots)$. Si on note X la série génératrice de la suite $(0, 1, 0, 0, \dots)$, alors on vérifie que la puissance k-ième de X par le produit de Cauchy est la suite qui a un 1 à la k-ième position et 0 ailleurs (on commence les indexes à zéro).

Donc, si $(\lambda_n)_{n\in\mathbb{N}}$ est une suite à support fini, c'est-à-dire, dont les termes sont nuls à partir d'un certain rang : $\exists k \in \mathbb{N}$ tel que $\lambda_n = 0$ pour tout $n > k$. Alors la série génératrice de $(\lambda_n)_{n\in\mathbb{N}}$ est la somme finie

$$\lambda_0 + \lambda_1 \cdot X + \lambda_2 \cdot X^2 + \cdot + \lambda_k \cdot X^k = \sum_{n=0}^{k} \lambda_n X^n,$$

de produits des λ_i avec des puissances de la suite X.

En fait, toute série formelle peut s'écrire comme une *somme infinie* de multiples de puissances de X. Ceci peut se formaliser comme un limite d'une suite de polynômes en introduisant une norme sur l'ensemble des séries formelles, mais c'est malheureusement hors programme (voir [Aigner, 2007, Sect. 2.3]).

On peut identifier les séries à support fini avec les polynômes, alors les opérations qu'on a décrit sont la somme et le produit usuels de l'anneau de polynômes.

Proposition 3.4. *L'anneau commutatif $\mathcal{A}[X]$ des polynômes à coefficients dans $\mathcal{A}$ est un sous-anneau de l'anneau $\mathcal{A}[[X]]$ des séries formelles à coefficients dans $\mathcal{A}$.*

3.1.4 Inverse multiplicatif

Théorème 3.5. *La série formelle $A(X) = a_0 + a_1X + a_2X^2 + \cdots \in \mathcal{A}[[X]]$ admet un inverse multiplicatif si et seulement si a_0 est inversible dans $\mathcal{A}$ (en particulier si et seulement si $a_0 \neq 0$, si $\mathcal{A} = \mathbb{R}$ ou $\mathcal{A} = \mathbb{C}$). Dans ce cas là, l'inverse de $A(X)$ est unique.*

Démonstration.

$\Longrightarrow$ Supposons que $A(X)$ admet un inverse multiplicatif $B(X) = b_0 + b_1X + b_2X^2 + \cdots$. Alors, $A(X)B(X) = 1$. C'est-à-dire,

$$\begin{aligned} 1 &= (a_0 + a_1X + a_2X^2 + \cdots)(b_0 + b_1X + b_2X^2 + \cdots) \\ &= (a_0b_0) + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots . \end{aligned}$$

Donc $a_0b_0 = 1$. C'est à dire, a_0 est inversible d'inverse $a_0^{-1} = b_0$.

$\Longleftarrow$ Supposons que a_0 est inversible. On définit de façon récursive une série formelle $B(X) = b_0 + b_1X + b_2X^2 + \cdots$ qui vérifie les équations imposées par le fait d'être l'inverse de $A(X)$:

$$\begin{cases} a_0b_0 = 1 \\ \sum_{k=0}^{n} a_kb_{n-k} = 0 \qquad \text{pour } n \geq 1 \end{cases}$$

En effet, ce système d'équations a une unique solution donnée par

$$\begin{aligned} b_0 &= \frac{1}{a_0} \\ b_1 &= \frac{1}{a_0}(-a_1b_0) \\ b_2 &= \frac{1}{a_0}(-a_1b_1 - a_2b_0) \\ &\vdots \\ b_k &= \frac{1}{a_0}(-\sum_{i=1}^{k} a_ib_{k-i}) \end{aligned}$$

Et donc, $A(X)$ est inversible. **cqfd.**

On dénote $A(X)^{-1}$, où bien $\frac{1}{A(X)}$, l'inverse multiplicatif de $A(X)$. En particulier, il faut lire la notation $\frac{A(X)}{B(X)}$ comme $A(X)B(X)^{-1}$.

Corollaire 3.6. *Pour tout $\alpha \in \mathcal{A}$, $1 - \alpha X \in \mathcal{A}[[X]]$ est inversible, et son inverse est*

$$\frac{1}{1 - \alpha X} = \sum_{n \in \mathbb{N}} X^n = 1 + \alpha X + \alpha^2X^2 + \alpha^3X^3 + \cdots$$

Démonstration.

(Version 1) Il suffit de vérifier que si $a_0 = 1$, $a_1 = -\alpha$ et $a_n = 0$ pour tout $n \geq 2$, alors la solution des équations du théorème précédent donnent $b_k = \alpha^k \ \forall k \geq 0$.

En effet, on le voit par récurrence sur k.

Initialisation : $b_0 = \frac{1}{a_0} = 1$.

Hérédité :

$$b_k = \frac{1}{a_0}(-\sum_{i=1}^{k} a_i b_{k-i}) = \frac{1}{1}(-(-\alpha)b_{k-1}) \overset{\text{H.R.}}{=} \alpha\alpha^{k-1} = \alpha^k.$$

(Version 2) Il faut vérifier que

$$1 = (1 - \alpha X)(1 + \alpha X + \alpha^2 X^2 + \alpha^3 X^3 + \cdots).$$

En effet,

$$\begin{aligned}(1 - \alpha X)(\sum_{n\geq 0} \alpha^n X^n) &= (\sum_{n\geq 0} \alpha^n X^n) - \alpha X(\sum_{n\geq 0} \alpha^n X^n) \\ &= (\sum_{n\geq 0} \alpha^n X^n) - (\sum_{n\geq 0} \alpha^{n+1} X^{n+1}) = (\sum_{n\geq 0} \alpha^n X^n) - (\sum_{n\geq 1} \alpha^n X^n) \\ &= 1 + (\sum_{n\geq 1} \alpha^n X^n) - (\sum_{n\geq 1} \alpha^n X^n) = 1\end{aligned}$$

cqfd.

En particulier,

Corollaire 3.7. *La série formelle* $(1 - X) \in \mathcal{A}[[X]]$ *est inversible, et son inverse est*

$$\frac{1}{1 - X} = \sum_{n\in\mathbb{N}} X^n = 1 + X + X^2 + X^3 + \cdots$$

3.2 Théorème du binôme pour des exposants négatifs

Définition 3.8. Pour $r \in \mathbb{R}$ et $k \in \mathbb{N}$, on définit le nombre/coefficient binomial généralisé $\binom{r}{k}$ par la formule

$$\binom{r}{k} = \frac{r(r-1)(r-2)\cdots(r-k+1)}{k!}.$$

qui vaut 0 si $k = 0$.

Notez que c'est une généralisation des coefficients binomiaux de la Section 2.3, qu'on récupère quand $r \in \mathbb{N}$.

Voici quelques exemples de coefficients binomiaux généralisés :

- Pour $r = -1$,
$$\binom{-1}{k} = \frac{(-1)(-2)\cdots(-k)}{k(k-1)\cdots 1} = (-1)^k.$$

- Pour $r = -2$
$$\binom{-2}{k} = \frac{(-2)(-3)\cdots(-k)(-k-1)}{k(k-1)\cdots 1} = (-1)^k \frac{(k+1)!}{k!} = (-1)^k(k+1).$$

- Pour $r = -m$ avec $m \in \mathbb{N}$
$$\begin{aligned}\binom{-m}{k} &= \frac{(-m)(-m-1)\cdots(-m-k+1)}{k(k-1)\cdots 1} = (-1)^k \binom{m+k-1}{k} \\ &= (-1)^k \left(\!\!\binom{m}{k}\!\!\right).\end{aligned}$$

- Pour $r = -\frac{1}{2}$
$$\begin{aligned}\binom{-1/2}{k} &= \frac{(-1/2)(-3/2)\cdots(-(2k-1)/2)}{k(k-1)\cdots 1} = \left(\frac{-1}{2}\right)^k \frac{(2k-1)(2k-3)\cdots 1}{k(k-1)\cdots 1} \\ &= \left(\frac{-1}{2}\right)^k \frac{1}{2k(2k-2)\cdots 2} \frac{2k(2k-1)(2k-2)\cdots 1}{k(k-1)\cdots 1} \overset{(*)}{=} \left(\frac{-1}{2}\right)^k \frac{1}{2^k k!} \frac{(2k)!}{k!} \\ &= \left(\frac{-1}{4}\right)^k \binom{2k}{k}.\end{aligned}$$

  où nous avons utilisé à $(*)$ que $2k(2k-2)\cdots 2 = 2^k k!$.

Théorème 3.9. *Pour un nombre entier quelconque $r \in \mathbb{Z}$, la fonction $(1+X)^r$ est la fonction génératrice de la suite $(\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \dots)$. C'est-à-dire*
$$(1+X)^r = \sum_{k \geq 0} \binom{r}{k} X^k.$$

Comme nous connaissons déjà ce résultat quand $r \in \mathbb{N}$, il suffit de considérer le cas des entiers négatifs. On montre un cas légèrement plus général (on obtient le théorème si on pose $\alpha = -1$ dans le résultat suivant).

Proposition 3.10. *Pour tout $\alpha \in \mathbb{C}$ et $m \in \mathbb{N}$*

$$(1-\alpha X)^{-m} = \sum_{k\geq 0}(-1)^k \binom{-m}{k} \alpha^k X^k = \sum_{k\geq 0} \binom{m+k-1}{k} \alpha^k X^k = \sum_{k\geq 0} \left(\!\!\binom{m}{k}\!\!\right) \alpha^k X^k.$$

Démonstration. En effet,

$$(1-\alpha X)^{-1} = 1 + \alpha X + \alpha^2 X^2 + \cdots = \sum_{n\in\mathbb{N}} \alpha^n X^n,$$

et donc

$$\begin{aligned}(1-\alpha X)^{-m} = \left(\frac{1}{1-\alpha X}\right)^m &= \underbrace{(1+\alpha X+\alpha^2X^2+\cdots)\cdots(1+\alpha X+\alpha^2X^2+\cdots)}_{m \text{ fois}} \\ &= \sum_{k\geq 0}\left(\sum_{\substack{x_1,x_2,\ldots,x_m\in\mathbb{N}\\ x_1+x_2+\cdots+x_m=k}} \alpha^{x_1}\alpha^{x_2}\cdots\alpha^{x_m}\right) X^k = \sum_{k\geq 0}\left(\sum_{\substack{x_1,x_2,\ldots,x_m\in\mathbb{N}\\ x_1+x_2+\cdots+x_m=k}} \alpha^{k}\right) X^k \\ &= \sum_{k\geq 0}\left(\sum_{\substack{x_1,x_2,\ldots,x_m\in\mathbb{N}\\ x_1+x_2+\cdots+x_m=k}} 1\right) \alpha^k X^k\end{aligned}$$

Mais le coefficient $\left(\sum_{\substack{x_1,x_2,\ldots,x_m\in\mathbb{N}\\ x_1+x_2+\cdots+x_m=k}} 1\right)$ est le nombre de solutions de l'équation

$$x_1 + x_2 + \cdots + x_m = k$$

dont tous les $x_i \in \mathbb{N}$. Nous avons vu que ceci est le nombre de multi-ensembles de taille k d'un ensemble de cardinal m. C'est à dire $\left(\!\!\binom{m}{k}\!\!\right) = \binom{m+k-1}{k}$. **cqfd.**

En fait, ce résultat se généralise à tout exposant $r \in \mathbb{R}$, mais nous n'avons pas (encore) défini des puissances des séries formelles par des exposants qui ne sont pas des entiers naturels !

3.3 Équations de récurrence linéaires

3.3.1 La suite de Fibonacci

La **suite de Fibonacci** [1] est la suite $(f_n)_{n\in\mathbb{N}}$ définie par les conditions initiales et l'équation de récurrence suivante

$$\begin{cases} f_0 = 0 \\ f_1 = 1 \\ f_n = f_{n-1} + f_{n-2} \quad \text{pour } n \geq 2. \end{cases}$$

Nous allons calculer une formule explicite pour f_n à partir de sa série génératrice

$$F(X) = f_0 + f_1 X + f_2 X^2 + \cdots = \sum_{n\in\mathbb{N}} f_n X^n.$$

On part de l'équation de récurrence, qui est valable pour chaque $n \geq 2$. On peut donc la multiplier par X^n et en faire la somme pour tout $n \geq 2$. On exprime l'équation résultante en termes de $F(X)$. On la résout, ce qui nous permet d'exprimer $F(X)$ comme un quotient de polynômes. Comme suit :

$$\begin{aligned}
f_n &= f_{n-1} + f_{n-2} && \forall n \geq 2, \\
f_n X^n &= f_{n-1} X^n + f_{n-2} X^n && \forall n \geq 2, \\
\sum_{n\geq 2} f_n X^n &= \sum_{n\geq 2} f_{n-1} X^n + \sum_{n\geq 2} f_{n-2} X^n, \\
\sum_{n\geq 2} f_n X^n &= X \sum_{n\geq 2} f_{n-1} X^{n-1} + X^2 \sum_{n\geq 2} f_{n-2} X^{n-2}, \\
\sum_{n\geq 2} f_n X^n &= X \sum_{n\geq 1} f_n X^n + X^2 \sum_{n\geq 0} f_n X^n, \\
F(X) - f_0 - f_1 X &= X(F(X) - f_0) + X^2 F(X) \\
F(X) - X &= X F(X) + X^2 F(X), \\
(1 - X - X^2) F(X) &= X, \\
F(X) &= \frac{X}{1 - X - X^2}.
\end{aligned}$$

1. Cette suite doit son nom à Leonardo Fibonacci (v. 1175 - v. 1250) qui dans son ouvrage *Liber abaci* (1202) proposa un problème dont la solution est la suite de Fibonacci. Il s'agit d'étudier la taille d'une population de lapins (pas trop réaliste) qui se comporte comme suit : (i) Au début du premier mois, on introduit une couple de lapereaux. (ii) Les lapereaux ont besoin d'un mois pour grandir avant de procréer ; ils ne procréent qu'à partir de la fin de son deuxième mois. (iii) Chaque début de mois, toute couple susceptible de procréer engendre effectivement une nouvelle couple de lapereaux. (iv) Les lapins ne meurent jamais. Quel est le nombre f_n de couples de lapins au début du n-ième mois ?

Les racines de $1 - X - X^2$ sont $\lambda = -\frac{1+\sqrt{5}}{2}$ et $\mu = -\frac{1-\sqrt{5}}{2}$. (On remarque que $\lambda = -\varphi = \frac{1}{1-\varphi}$ et $\mu = \varphi - 1 = \frac{1}{\varphi}$, où $\varphi = \frac{1+\sqrt{5}}{2}$ est le *nombre d'or.*)

Du *Théorème de décomposition en éléments simples*, on sait qu'il existent $a, b \in \mathbb{C}$ tels que

$$\frac{X}{1 - X - X^2} = \frac{a}{X - \lambda} + \frac{b}{X - \mu}.$$

C'est plus convenable de diviser les dénominateurs par λ et μ, respectivement, et travailler avec les constantes $A = \frac{-a}{\lambda}$ et $B = \frac{-b}{\mu}$ et avec les coefficients $\varphi' = 1 - \varphi = \frac{1}{\lambda}$ et $\varphi = \frac{1}{\mu}$:

$$\frac{X}{1 - X - X^2} = \frac{\frac{-a}{\lambda}}{1 - \frac{X}{\lambda}} + \frac{\frac{-b}{\mu}}{1 - \frac{X}{\mu}} = \frac{A}{1 - \frac{X}{\lambda}} + \frac{B}{1 - \frac{X}{\mu}} = \frac{A}{1 - \varphi' X} + \frac{B}{1 - \varphi X}.$$

Pour trouver les valeurs de A et B, on multiplie

$$\begin{aligned}\frac{X}{1 - X - X^2} &= \frac{A}{1 - \varphi' X} + \frac{B}{1 - \varphi X} = \frac{A(1 - \varphi X) + B(1 - \varphi' X)}{(1 - \varphi' X)(1 - \varphi X)} \\ &= \frac{(A + B) + (-A\varphi - B\varphi')X}{1 - X - X^2}\end{aligned}$$

et on obtient le système suivant

$$\begin{cases} A + B & = 0 \\ -A\varphi - B\varphi' & = 1 \end{cases}$$

dont la solution est $A = \frac{-1}{\sqrt{5}}$ et $B = \frac{1}{\sqrt{5}}$.

D'où,

$$\begin{aligned}F(X) = \frac{X}{1 - X - X^2} &= \frac{\frac{1}{\sqrt{5}}}{1 - \varphi X} - \frac{\frac{1}{\sqrt{5}}}{1 - \varphi' X} \\ &= \frac{1}{\sqrt{5}} \sum_{n \in \mathbb{N}} \varphi^n X^n - \frac{1}{\sqrt{5}} \sum_{n \in \mathbb{N}} \varphi'^n X^n = \sum_{n \in \mathbb{N}} \frac{1}{\sqrt{5}} (\varphi^n - \varphi'^n) X^n\end{aligned}$$

et donc

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

3.3.2 Récurrences linéaires homogènes à coefficients constants

Cette méthode sert à trouver la forme générale de toute suite $(y_0, y_1, y_2, \dots)$ qui vérifie une récurrence linéaire homogènes à coefficients constants. C'est à dire, une récurrence de la forme

$$y_{n+k} = a_{k-1}y_{n+k-1} + a_{k-2}y_{n+k-2} + \cdots + a_1 y_{n+1} + a_0 y_n$$

où $a_i \in \mathbb{C}$.

Les étapes à suivre sont :

0.- *Étude combinatoire et obtention de la relation de récurrence.*

1.- *Calcul de la série génératrice associée à notre suite.*

(a) Multiplier l'équation de récurrence par X^{n+k} et faire la somme pour $n \in \mathbb{N}$.

(b) En déduire une équation en fonction de la série génératrice $Y(X) = \sum_{n\in\mathbb{N}} y_n X^n$ et les termes initiaux de $y_0, \dots, y_k$.

(c) Résoudre et obtenir une expression comme fraction rationnelle $\frac{P(X)}{Q(X)}$.

(d) Décomposer en fractions simples de la forme $\frac{\beta}{(1-\alpha X)^m} = \beta \sum_{n\in\mathbb{N}} \binom{n+m-1}{m} \alpha^n X^n$.
Rappel : Si $Q(X) = \beta(X-\alpha_1)^{m_1} \cdots (X-\alpha_k)^{m_k} \in \mathbb{C}[X]$ avec $\beta, \alpha_i \neq 0$, alors $\exists P'(X) \in \mathbb{C}[X]$ et $\gamma_{ij} \in \mathbb{C}$ où $1 \leq i \leq k$ et $1 \leq j \leq m_k$, tels que

$$\frac{P(X)}{Q(X)} = P'(X) + \sum_{\substack{1\leq i\leq k \\ 1\leq j\leq m_k}} \frac{\gamma_{ij}}{(1-\frac{X}{\alpha_i})^j}$$

2.- *Obtention du terme général avec le théorème du binôme généralisé.*

Deuxième partie

Graphes

Chapitre 4

Introduction à la théorie de graphes

4.1 Graphes et isomorphismes

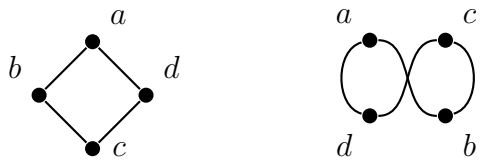
Définition 4.1. Un **graphe** (simple non-orienté) est un couple $G = (S, A)$, où S est un ensemble fini quelconque et A est un sous-ensemble de $\mathcal{P}_2(S)$. Les éléments de S sont appelés **sommets** (ou nœuds) et les éléments de A sont appelés **arêtes**.

Soit $G = (S, A)$ un graphe. On écrit respectivement $S(G)$ et $A(G)$ pour désigner son ensemble de sommets et d'arêtes. L'**ordre** de G est le cardinal de son ensemble de sommets, $|S(G)|$. On dit que $s, s' \in S$ sont **adjacents** ou **voisins** lorsque $\{s, s'\} \in A$.

On représente souvent les graphes par des dessins dans le plan, où les sommets sont représentés par des points du plan, et les arêtes par des lignes joignant les paires de points correspondantes.

Il ne faut pas confondre un graphe, qui est un objet purement combinatoire, avec son dessin. Un même graphe peut être représenté de plusieurs façons. Par exemple, voici deux représentations du graphe

$$G = (\{a, b, c, d\}, \{\{a, b\}, \{b, c\}, \{c, d\}, \{d, a\}\})$$



Observation 4.2. Ce qu'on appelle 'graphe' ici est d'habitude appelé 'graphe simple non-orienté' pour le distinguer d'autres notions voisines. En effet, il existent autres notions de graphe qui admettent des boucles et des arêtes multiples (parfois appelés des **multigraphes**), où les arêtes sont orientés, où valuées ... Sauf si cela

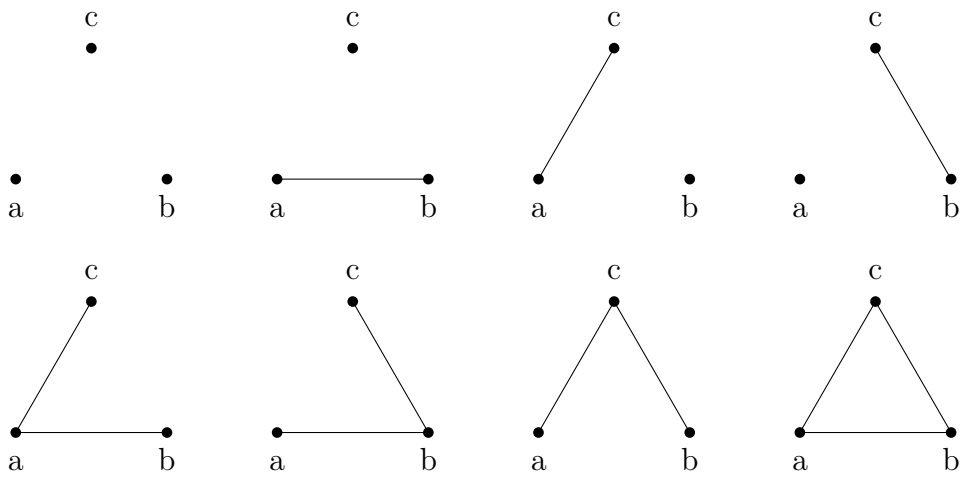
est explicitement mentionné, tout graphe sera considéré simple et non-orienté, et nous n'allons pas insister à le préciser.

Question 4.3. Quel est le nombre de graphes distincts sur un ensemble fixé de n sommets S ?

Solution. Un graphe sur l'ensemble de sommets S est déterminé par son ensemble d'arêtes, qui est une partie de $\mathcal{P}_2(S)$. Le nombre de graphes est donc le nombre de parties de $\mathcal{P}_2(S)$:

$$|\mathcal{P}(\mathcal{P}_2(S))| = 2^{|\mathcal{P}_2(S)|} = 2^{\binom{n}{2}}.$$

Par exemple, il y a 8 graphes distincts dont l'ensemble des sommets est $S = \{a, b, c\}$:



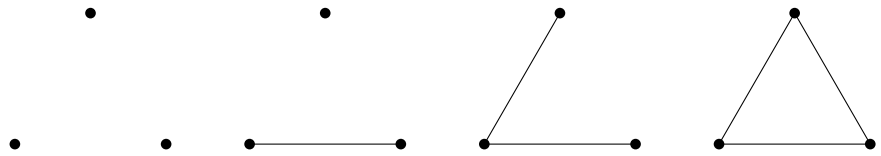
4.1.1 Isomorphisme

Définition 4.4. Deux graphes $G = (S, A)$ et $G' = (S', A')$ sont dits **isomorphes** s'il existe une bijection $\varphi : S \to S'$, dite **isomorphisme**, telle que pour toute paire de sommets $\{x, y\} \in \mathcal{P}_2(S)$ on a

$$\{x, y\} \in A \qquad \Longleftrightarrow \qquad \{\varphi(x), \varphi(y)\} \in A'.$$

L'isomorphisme envoie des sommets adjacents sur des sommets adjacents, et des sommets non adjacents sur des sommets non adjacents. Il peut être vu simplement comme une façon de "renommer les sommets" d'un graphe sans changer les adjacences. La relation $\cong$, où $G \cong G'$ s'ils sont isomorphes, est une relation d'équivalence sur les graphes.

Par exemple, les graphes d'ordre 3 se répartissent en quatre classes d'isomorphisme. On dit qu'il y a, *à isomorphisme près*, 4 graphes simples d'ordre 3 distincts :



Question 4.5. Quel est le nombre de graphes d'ordre n à isomorphisme près ?

Solution. Ceci est une question beaucoup plus difficile [1]. On peut quand même trouver des estimations raisonnables assez facilement.

Soit $\mathcal{G}_n$ l'ensemble des graphes dont les sommets sont $[1, n]$, et soit

$$\pi : \mathcal{G}_n \to \mathcal{G}/\cong$$

l'application qui assigne chacun de ces graphes à sa classe d'isomorphisme. Quelle est la taille de la classe d'isomorphisme de G ? Chaque isomorphisme est déterminé par une bijection $S \to S$. Comme le nombre de bijections d'un ensemble de cardinal n est $n!$, chaque classe d'équivalence contient au plus $n!$ graphes (et au moins 1).

Donc, le nombre de classes d'équivalence est au moins

$$\frac{|\mathcal{G}_n|}{n!} = \frac{2^{\binom{n}{2}}}{n!}.$$

Cette fonction de n ne croît pas beaucoup plus lentement que $2^{\binom{n}{2}}$. En effet, considérons les logarithmes de ces deux fonctions (et en utilisant que $n! \leq n^n$) :

$$\log_2\left(2^{\binom{n}{2}}\right) = \binom{n}{2} = \frac{n^2}{2}\left(1 - \frac{1}{n}\right)$$

$$\log_2\left(\frac{2^{\binom{n}{2}}}{n!}\right) = \binom{n}{2} - \log_2(n!) \geq \binom{n}{2} - n\log_2(n) = \frac{n^2}{2}\left(1 - \frac{1}{n} - \frac{2\log_2(n)}{n}\right).$$

Donc, pour les grandes valeurs de n, les logarithmes des deux fonctions se comportent "à peu près comme" la fonction $\frac{1}{2}n^2$.

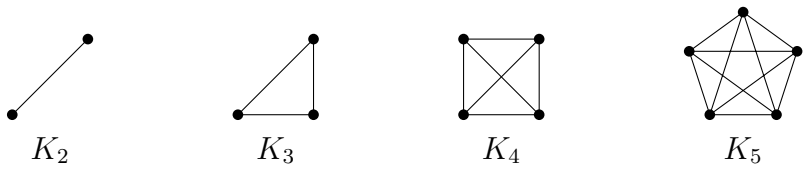
1. En fait, le problème de décider si deux graphes sont isomorphes est très important et très difficile. C'est un sujet de recherche actuel : en 2015, le mathématicien hongrois László Babai a annoncé un nouveau algorithme pour résoudre ce problème qui fait largement descendre la borne de complexité de ce problème qui joue un rôle fondamental en théorie de la complexité. C'est un des résultats récents les plus importants en algorithmique.

4.2 Bestiaire

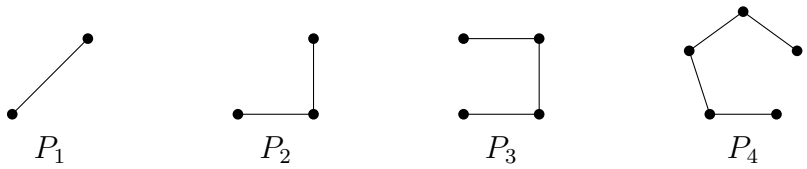
Nous allons donner des exemples de (classes d'isomorphismes de) graphes naturels, que l'on rencontre souvent.

- Le n-**stable**, ou stable d'ordre n, S_n : $S(S_n) = [1, n]$, $A(S_n) = \varnothing$.

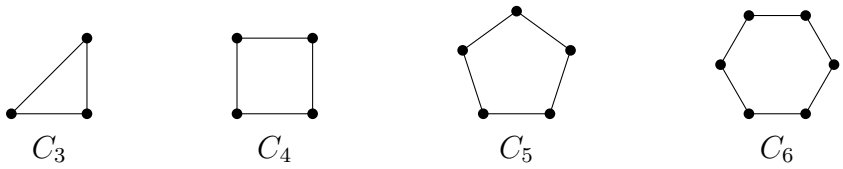
- La n-**clique**, ou **graphe complet**, K_n : $S(K_n) = [1, n]$, $A(K_n) = \mathcal{P}_2(S)$.



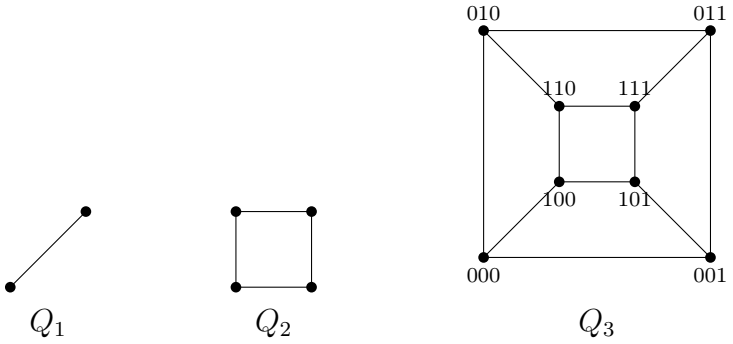
- La n-**chaîne** ou chaîne de longueur n, P_n : $S(P_n) = [0, n]$ (c'est donc un graphe d'ordre $n + 1$), $A(P_n) = \{\{i, i + 1\} : 0 \leq i < n\}$.



- Pour $n \geq 3$, le n-**cycle** ou cycle de longueur n, C_n : $S(C_n) = [1, n]$ (c'est donc un graphe d'ordre n), $A(C_n) = \{\{i, j\} : |i - j| = 1 \text{ ou } |i - j| = n - 1\}$.

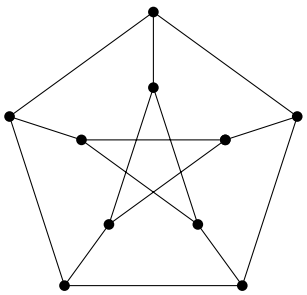


- Pour $d \geq 0$, le d-**cube** Q_d, ou cube de dimension d : $S(Q_d) = \{0, 1\}^d$, $A(Q_d) = \{\{x, y\} : \ x \text{ et } y \text{ diffèrent en une seule position}\}$.

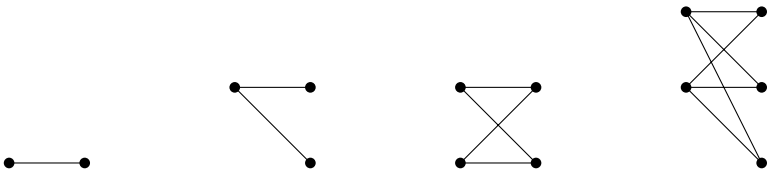


Q_1 Q_2 Q_3

- Le *graphe de Petersen* est le graphe suivant, étudié en exercice :



- Pour $n, m \in \mathbb{N}^*$, le graphe (n,m)-**biparti complet**, $K_{n,m}$: $S(K_{n,m}) = \{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_m\}$ (c'est donc un graphe d'ordre $n+m$), $A(K_{n,m}) = \{\{a_i, b_j\} : 1 \leq i \leq n, 1 \leq j \leq m\}$.



K_{11} K_{12} K_{22} K_{23}

4.3 Degrés

Soit G un graphe. Le **voisinage** d'un sommet $x \in S(G)$ est l'ensemble des sommets qui lui sont adjacents. Le **degré** d'un sommet $x \in S(G)$, noté $\boldsymbol{d(x)}$, est le cardinal de son voisinage :

$$d(x) = |\{y \in S \setminus \{x\} : \{x, y\} \in A\}| .$$

Le **degré minimum**, respectivement **maximum**, du graphe G est défini comme

$$\delta(G) = \min_{s \in S} d(s)$$

respectivement

$$\Delta(G) = \max_{s \in S} d(s).$$

Si ces deux nombres sont égaux, c'est-à-dire si tous les sommets ont le même degré k, on dit que le graphe est k-**régulier**.

4.3.1 Le lemme des poignées de main

Théorème 4.6 (Lemme des poignées de mains)**.** *Soit $G = (S, A)$ un graphe, alors :*

$$\sum_{s \in S} d(s) = 2|A|.$$

C'est-à-dire, le nombre d'arêtes d'un graphe est égal à la demi-somme des degrés de ses sommets.

Démonstration. On utilise la technique du double décompte. Notons B l'ensemble des couples $(s, a) \in S \times A$ tels que $s \in a$. Comme chaque arête a deux bouts, on a

$$|B| = \sum_{a \in A} |\{s \in S : \ s \in a\}| = \sum_{a \in A} 2 = 2|A|.$$

D'autre part, chaque sommet s appartient à $d(s)$ arêtes. On a donc

$$|B| = \sum_{s \in S} |\{a \in A : \ s \in a\}| = \sum_{s \in S} d(s),$$

d'où le résultat. **cqfd.**

En conséquence,

Corollaire 4.7. *Tout graphe possède un nombre pair de sommets de degré impair.*

Démonstration. Il suffit de remarquer que l'ensemble S des sommets est la réunion disjointe de l'ensemble I des sommets qui sont de degré impair et de l'ensemble P des sommets qui sont de degré pair. D'après le lemme des poignées de mains, on a

$$\sum_{s \in S} d(s) = \sum_{s \in P} d(s) + \sum_{s \in I} d(s) = 2|A|$$

On en déduit donc que $\sum_{s \in I} d(s)$, qui est une somme de nombres impairs, doit être pair. Ceci entraîne que $|I|$ est pair. **cqfd.**

4.3.2 Matrices associées à un graphe

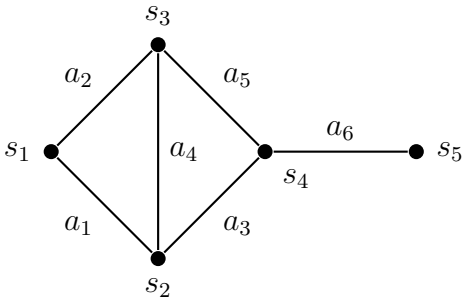
Soit $G = (S, A)$ un graphe, où les sommets et les arêtes sont numérotés : $S = \{s_1, s_2, \ldots, s_n\}$ et $A = \{a_1, a_2, \ldots, a_m\}$.

Matrice d'incidence

La **matrice d'incidence** de G est la matrice M de taille $n \times m$ définie par

$$m_{i,j} = \begin{cases} 1 \text{ si } s_i \text{ est une des deux extrémités distinctes de } a_j, \\ 0 \text{ si } s_i \text{ n'est pas une extrémité de } a_j. \end{cases}$$

Exemple :



$$M = \begin{array}{c} \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \end{array} \begin{array}{c} \begin{array}{cccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Notez que la somme des éléments de la colonne d'indice j vaut 2. La somme des éléments de la ligne i est, par définition, le degré de s_i. Ceci nous fournit un preuve alternative du lemme des poignées de mains :

Démonstration alternative du Théorème 4.6. Le nombre suivant est égal à la somme de tous les éléments de la matrice d'incidence M :

$$\sum_{s \in S} d(s) = \sum_{i=1}^{n} d(s_i) = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} m_{ij} \right) = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} m_{ij} \right) = \sum_{j=1}^{m} 2 = 2|A|.$$

cqfd.

Matrice d'adjacence

La **matrice d'adjacence** A_G du graphe G est une matrice $n \times n$ définie par

$$a_{ij} = \begin{cases} 1 & \text{si } \{s_i, s_j\} \in A, \\ 0 & \text{sinon.} \end{cases}$$

On voit que cette matrice est symétrique. La somme des éléments d'une ligne (ou colonne) est le degré du sommet correspondant.

Pour le graphe précédent, la matrice d'adjacence est :

$$M = \begin{array}{c} \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \end{array} \begin{array}{c} \begin{array}{ccccc} s_1 & s_2 & s_3 & s_4 & s_5 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

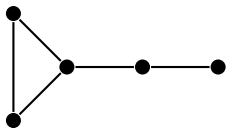
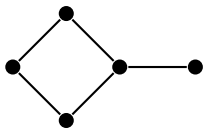
4.3.3 Le théorème d'Havel et Hakimi

Soit G un graphe sur l'ensemble de sommets $\{s_1, \dots s_n\}$. La suite

$$(\deg(s_1), \deg(s_2), \dots, \deg(s_n))$$

est appelée la **suite des degrés** de G (en général on ne tiendra pas compte de l'ordre et, par convention, on écrira les termes en ordre croissant).

Deux graphes isomorphes ont toujours la même suite de degrés, mais la réciproque n'est pas vraie. Par exemple,


n'est pas isomorphe à

.

Une suite d'entiers naturels $(d_1, \dots, d_n) \in [0, n-1]^n$ est dite **graphique** si elle est la suite de degrés d'un graphe G.

Théorème 4.8 (Havel-Hakimi)**.** *Soit $n \in \mathbb{N}^*$ et soient $d_1 \leq d_2 \leq d_3 \leq \cdots \leq d_n$ des entiers naturels. Alors la suite $(d_1, \dots, d_n)$ est graphique si et seulement si la suite $(d'_1, \dots, d'_{n-1})$ est graphique, où*

$$d'_i = \begin{cases} d_i & \text{pour } i < n - d_n, \\ d_i - 1 & \text{pour } i \geq n - d_n. \end{cases}$$

Démonstration.

$\Longleftarrow$ Supposons que $(d'_1, \dots, d'_{n-1})$ est une suite graphique, et soit $G' = (S', A')$, avec $V = \{s'_1, \dots, s'_{n-1}\}$, un graphe tel que $\deg(s'_i) = d'_i$. Alors le graphe $G = (S, A)$, obtenu en ajoutant un nouveau sommet s_n à G comme suit

$$\begin{aligned} S &= S' \cup \{s_n\}, \\ A &= A' \cup \{\{s_i, s_n\} : \ n - d_n \leq i \leq n-1\}, \end{aligned}$$

a $(d_1, \dots, d_n)$ comme suite de degrés.

$\Longrightarrow$ Supposons que $(d_1, \dots, d_n)$ est une suite graphique. Nous voulons montrer que $(d'_1, \dots, d'_{n-1})$ est aussi une suite graphique. Si on trouve un graphe G à n sommets dont la suite de degrés est $(d_1, \dots, d_n)$ et tel que le sommet s_n est adjacent à tous les sommets s_i avec $n - d_n \leq i \leq n-1$, alors nous pouvons renverser la construction de la preuve précédente : si l'on supprime s_n à G, on obtient un graphe G' dont la suite de degrés est $(d'_1, \dots, d'_{n-1})$.

Nous allons montrer qu'il existe un graphe G qui vérifie ces propriétés. Supposons par l'absurde qu'un tel graphe n'existe pas. Considérons alors un graphe G

avec sommets $\{s_1, \ldots, s_n\}$ et degrés $d(s_i) = d_i$ pour $1 \leq i \leq n$ et tel que s_n soit adjacent à un maximum de sommets dans $\{s_{n-d_n}, \ldots, s_{n-1}\}$ (il existe puis que la suite est graphique).

Par hypothèse, il existe un k, $n - d_n \leq k \leq n - 1$, tel que $\{s_k, s_n\} \notin A$. De plus, comme $d(s_n) = d_n$, il existe un ℓ, $1 \leq \ell \leq n - d_n - 1$, tel que $\{s_\ell, s_n\} \in A$.

Comme $\ell < k$, on a $d(s_k) \geq d(s_\ell)$. Deux cas sont alors possibles.

Si $d(s_k) = d(s_\ell)$, alors si l'on renumérote les sommets de G en échangeant s_k et s_ℓ, on obtient un graphe G' dont la suite de degrés reste inchangée. Par contre, dans ce nouveau graphe, s_n a un voisin supplémentaire dans $\{s_{n-d_n}, \ldots, s_{n-1}\}$, ce qui contredit la maximalité de G.

Si $d(s_k) > d(s_\ell)$, alors il existe un $m \neq k, \ell$ tel que s_m soit adjacent à s_k mais pas à s_ℓ. On a forcement que $m \neq n$. On considère le graphe G' obtenu de G en remplaçant les arêtes $\{s_n, s_\ell\}$ et $\{s_k, s_m\}$ par les arêtes $\{s_n, s_k\}$ et $\{s_\ell, s_m\}$. La suite de degrés reste inchangé, mais dans G' le sommet s_n est adjacent à strictement plus de sommets dans $\{s_{n-d_n}, \ldots, s_{n-1}\}$, ce qui est une contradiction.

cqfd.

Question 4.9. Existe-t'il un graphe dont la suite des degrés soit $(1, 1, 1, 2, 2)$? Si oui, donner un exemple.

Solution. No, car le nombre de sommets impairs doit être pair.

Question 4.10. Existe-t'il un graphe dont la suite des degrés soit $(1, 1, 1, 3, 4)$? Si oui, donner un exemple.

Solution. D'après le théorème d'Havel et Hakimi, on a les équivalences suivante :

$$\begin{aligned}(1,1,1,3,4) \text{ graphique} &\iff (0,0,0,2) \text{ graphique} \\ &\iff (0,-1,-1) \text{ graphique}\end{aligned}$$

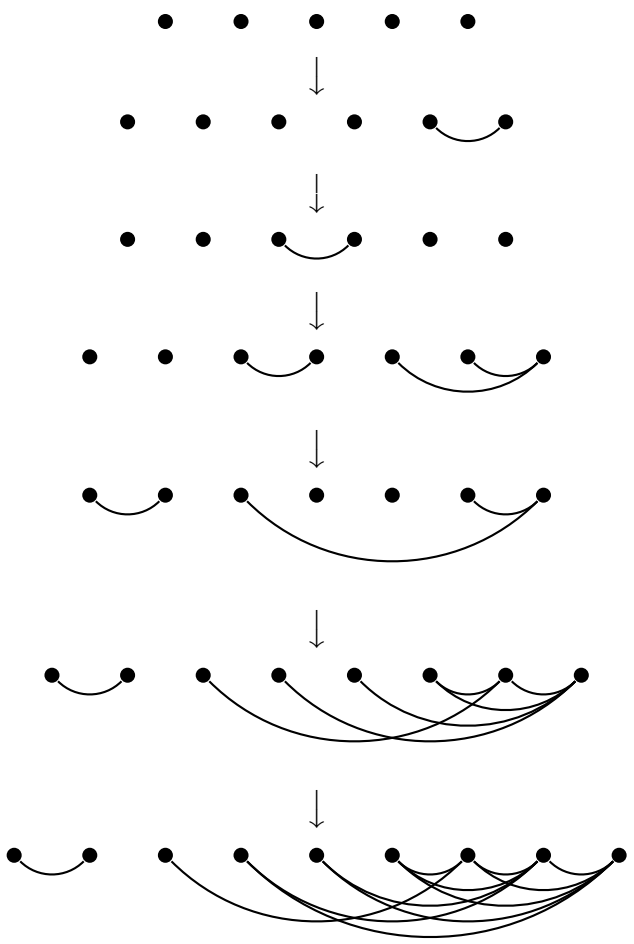
Mais $(-1, -1, 0)$ n'est clairement pas une suite graphique, et donc on en déduit qu'il n'existe pas de graphe dont la suite des degrés soit $(1, 1, 1, 3, 4)$.

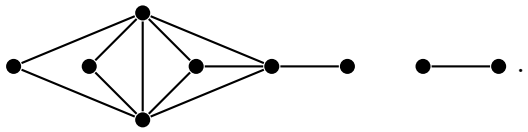
Question 4.11. Existe-t'il un graphe dont la suite des degrés soit $(1, 1, 1, 2, 2, 3, 4, 5, 5)$? Si oui, donner un exemple.

Solution. D'après le théorème d'Havel et Hakimi, on a les équivalences suivantes :

$$\begin{aligned}(1,1,1,2,2,3,4,5,5) \text{ graphique} &\iff (1,1,1,1,1,2,3,4) \text{ graphique} \\ &\iff (1,1,1,0,0,1,2) \text{ graphique} \\ &\iff (0,0,1,1,1,1,2) \text{ graphique} \\ &\iff (0,0,1,1,0,0) \text{ graphique} \\ &\iff (0,0,0,0,1,1) \text{ graphique} \\ &\iff (0,0,0,0,0) \text{ graphique}\end{aligned}$$

On en déduit qu'il existe un graphe dont la suite de degrés est $(1, 1, 1, 2, 2, 3, 4, 5, 5)$. De plus, l'idée utilisée pour démontrer l'implication ($\Longleftarrow$) dans la preuve du théorème nous fournit une stratégie pour construire un tel graphe :



Un graphe qui peut être dessiné comme :  .

4.4 Théorie extrémale des graphes

4.4.1 Sous-graphes

Définition 4.12. Un **sous-graphe** d'un graphe $G = (S, A)$ est un graphe $G' = (S', A')$ tel que $S' \subset S$ et $A' \subset A$.

Si $A' = A \cap \mathcal{P}_2(S')$, alors on dit que G' est le **sous-graphe de G induit par S'**, ce qu'on note $G' = G[S']$

On dit qu'un sous-graphe est un sous-graphe **couvrant** si $S' = S$.

Question 4.13. Quel est le nombre de sous-graphes de K_n ? Quel est le nombre de sous-graphes induits de K_n ? Quel est le nombre de sous-graphes couvrants de K_n ?

Solution. Respectivement $\sum_{k=0}^{n} \left(\binom{n}{k} \cdot 2^{\binom{k}{2}} \right)$, 2^n et $2^{\binom{n}{2}}$.

4.4.2 Théorème de Turán

On dit que G **contient** le graphe G' s'il existe un sous-graphe de G isomorphe à G'.

Théorème 4.14 (Théorème de Turán (1941))**.** *Soit $G = (S, A)$ un graphe à n sommets et m arêtes, et soit $r \geq 2$ un entier. Si G ne contient pas K_r, alors*

$$m \leq \left(1 - \frac{1}{r-1}\right) \frac{n^2}{2}.$$

Démonstration. Par récurrence sur n et r. Pour $n = 1$ ou $r = 2$, il n'y a rien à démontrer. Soient donc $n > 1$ et $r > 2$ deux entiers, et supposons le résultat vrai pour $n' < n$ ou $r' < r$. On considère un graphe simple $G = (S, A)$ d'ordre n qui ne contient pas de r-clique (K_r).

Si G ne contient pas de $(r-1)$-clique, on peut appliquer l'hypothèse de récurrence avec $r' = r - 1$ et on obtient

$$m \leq \left(1 - \frac{1}{r-2}\right) \frac{n^2}{2} \leq \left(1 - \frac{1}{r-1}\right) \frac{n^2}{2}.$$

Nous pouvons donc supposer que G contient une $(r-1)$-clique, c'est-à-dire qu'il existe une partie V de S de cardinal $r-1$ telle que tous les éléments de V sont voisins entre eux. Notons $W = S \setminus V$. On sépare les arêtes de G en trois parties A_{VV}, A_{WW} et A_{VW}.

- A_{VV} est l'ensemble des arêtes qui ont les deux extrémités dans V. Comme $G[V]$ est un $(r-1)$-clique,

$$|A_{VV}| = \binom{r-1}{2} = \frac{(r-1)(r-2)}{2}.$$

- A_{WW} est l'ensemble des arêtes qui ont les deux extrémités dans W. Comme G ne contient pas de r-clique, il en est de même pour $G[W]$, qui est un graphe d'ordre $n-(r-1) < n$. L'hypothèse de récurrence s'applique alors, et donc

$$|A_{WW}| \leq \left(1 - \frac{1}{r-1}\right) \frac{(n-r+1)^2}{2} = \left(\frac{r-2}{r-1}\right) \frac{(n-r+1)^2}{2}.$$

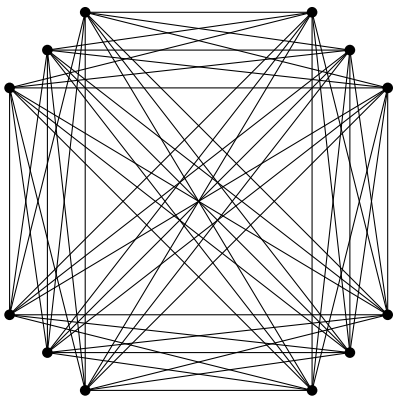
- A_{VV} est l'ensemble des arêtes qui ont une extrémité dans V et l'autre dans W. Comme G ne contient pas de K_r, et $G[V] \cong K_{r-1}$, chaque sommet dans W a au plus $(r-2)$ voisins dans V, car sinon ce sommet avec V formerait un r-clique. On a donc

$$|A_{VW}| \leq (r-2)(n-r+1).$$

Pour finir

$$\begin{aligned}
|A| &= |A_{VV}| + |A_{WW}| + |A_{VW}| \\
&\leq \frac{(r-1)(r-2)}{2} + \left(\frac{r-2}{r-1}\right) \frac{(n-r+1)^2}{2} + (r-2)(n-r+1) \\
&= \frac{1}{2}\left(\frac{r-2}{r-1}\right)\left((r-1)^2 + (n-r+1)^2 + 2(r-1)(n-r+1)\right) \\
&= \frac{1}{2}\left(\frac{r-2}{r-1}\right)\left((r-1)^2 + n^2 - 2n(r-1) + (r-1)^2 + 2(r-1)n - 2(r-1)^2\right) \\
&= \frac{1}{2}\left(\frac{r-2}{r-1}\right) n^2 = \left(1 - \frac{1}{r-1}\right)\frac{n^2}{2}. \qquad \textbf{cqfd.}
\end{aligned}$$

On remarque que si $n = k(r-1)$ est un multiple de $r-1$, on peut construire un graphe d'ordre n sans r-clique de la façon suivante : on répartit les sommets en $r-1$ groupes de k éléments et deux sommets quelconques sont voisins si et seulement s'ils n'appartiennent pas au même groupe. Voici l'exemple pour $r = 5$ et $k = 3$:



Il est clair que ce graphe ne contient pas de r-clique puisque d'après le principe des tiroirs toute partie de S de cardinal r contient deux sommets de même groupe, donc non voisins. Comptons les arêtes du graphe. Il y a $\binom{r-1}{2} = \frac{(r-1)(r-2)}{2}$ paires de groupes et k^2 arêtes entre éléments de chaque paire de groupes. On a donc

$$|A| = \frac{(r-1)(r-2)}{2}k^2 = \left(1 - \frac{1}{r-1}\right)\frac{n^2}{2}$$

et la borne donnée par le théorème de Turan est atteinte.

Voici une application géométrique de ce théorème :

Théorème 4.15 (Erdös)**.** *Soit S un ensemble de points du plan de diamètre au plus 1. Alors le nombre de paires de points à distance au moins $\frac{1}{\sqrt{2}}$ est au plus $\frac{n^2}{3}$.*

Démonstration. On considère le graphe $G = (S, A)$ où $\{x, y\} \in A$ si et seulement si $d(x, y) > \frac{1}{\sqrt{2}}$. Nous voulons montrer que G ne contient pas de K_4.

En effet, parmi chaque quadruplet de points, on peut trouver trois points x, y, z qui forment un angle d'au moins 90° : si les points forment un quadrilatère,les angles intérieurs somment 360°, et si un point est dans le triangle formé par les autres, alors il définit trois angles dont la somme est 360°.

Supposons qu'il y a un 4-clique dans G avec sommets x, y, z, t. On peut supposer que l'angle formé par x, y, z est $\geq 90°$. Mais si $d(x, y) > \frac{1}{\sqrt{2}}$ et $d(y, z) > \frac{1}{\sqrt{2}}$, alors $d(x, z) > 1$, ce qui amène à une contradiction.

Donc G n'a pas de 4-clique, et donc du Théorème de Turàn, G a au plus $\frac{n^2}{3}$ arêtes. **cqfd.**

4.4.3 Graphe complémentaire et stables

Le **graphe complémentaire** d'un graphe $G = (S, A)$ est le graphe $\overline{G} = (S, \mathcal{P}_2(S) \setminus A)$ où deux sommets distincts sont voisins si et seulement s'ils ne le sont pas dans G.

Un **stable** ou **ensemble indépendant** d'un graphe G est un ensemble de sommets de G deux à deux non adjacents.

Corollaire 4.16. *Soit $G = (S, A)$ un graphe d'ordre n et m arêtes. Et soit $\alpha(G)$ le cardinal du plus grand stable de G. Alors*

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

Démonstration. Un stable de G se correspond à une clique de $\overline{G}$. Donc $\overline{G}$ est un

graphe qui ne contient pas $K_{\alpha(G)+1}$. Donc, du théorème de Turàn

$$\frac{n(n-1)}{2} - m = |E(\overline{G})| \leq \left(1 - \frac{1}{\alpha(G)}\right)\frac{n^2}{2} = \left(\frac{\alpha(G)-1}{\alpha(G)}\right)\frac{n^2}{2}$$
$$\alpha(G)n^2 - \alpha(G)n - 2\alpha(G)m \leq \alpha(G)n^2 - n^2$$
$$\alpha(G)(2m+n) \geq n^2$$

cqfd.

4.5 Théorie de Ramsey

Définition 4.17. Pour $s, t \in \mathbb{N}^*$, le **nombre de Ramsey** $R(s,t)$ est le plus petit entier $n \in \mathbb{N}^*$ tel que tout graphe G à n-sommets contienne soit un K_s soit un S_t induit. Équivalemment, soit G contient K_s soit $\overline{G}$ contient K_t.

À priori, $R(s,t)$ pourrait être ∞, mais nous verrons dans le Théorème 4.19 qu'il s'agit bien d'un nombre fini.

Observation 4.18. Pour tout $s, t \in \mathbb{N}^*$:

- $R(s,t) = R(t,s)$.
- $R(1,t) = 1$.
- $R(2,t) = t$.

Démonstration.

- Montrons d'abord que $R(s,t) \geq R(t,s)$. En effet, si $n \geq R(t,s)$ alors $\overline{G}$ contient soit K_t soit S_s, d'où G contient soit S_t soit K_s. Le même raisonnement preuve que $R(t,s) \geq R(s,t)$.
- Tout graphe à $n \geq 1$ sommets contient K_1.
- Soit G un graphe d'ordre $n \geq t$. Si G à au moins une arête, alors G contient K_2. Sinon, G est isomorphe à S_n qui contient S_t. Ceci preuve que $R(2,t) \leq t$. Il faut montrer que t est le plus petit entier avec cette propriété. En effet, S_{t-1} est un graphe d'ordre $t-1$ qui ne contient ni K_2 ni S_t.

cqfd.

Théorème 4.19. *Pour $s, t \geq 2$, on a*

$$R(s,t) \leq R(s-1,t) + R(s,t-1).$$

Démonstration. Soit $G = (S, A)$ un graphe à $n = R(s-1,t)+R(s,t-1)$ sommets, et soit $u \in S$. Soient $V = \{v \in S : \{u,v\} \in A\}$ et $W = \{v \in S : \{u,v\} \notin A\}$. Alors

$$|V| + |W| = n - 1$$

Du principe des tiroirs, soit $|V| \geq R(s-1,t)$ soit $|W| \geq R(s,t-1)$.

- Si $|V| \geq R(s-1,t)$ alors soit $G[V]$ contient S_t (et alors G aussi), soit $G[V]$ contient K_{s-1} ; et alors $G[V \cup u]$ contient K_s.
- Si $|W| \geq R(s,t-1)$ alors soit $G[W]$ contient K_s (et alors G aussi), soit $G[W]$ contient S_{t-1} ; et alors $G[V \cup u]$ contient S_t. **cqfd.**

Corollaire 4.20. *Pour $s, t \in \mathbb{N}^*$,*

$$R(s,t) \leq \binom{s+t-2}{s-1} = \binom{s+t-2}{t-1}.$$

Démonstration. Par récurrence sur $s+t \geq 2$. Lorsque $s+t = 2$, $R(1,1) = 1 \leq \binom{0}{0}$. Supposons la propriété vraie au rang $s+t \geq 2$, et montrons qu'elle est vraie au rang $s+t+1$. En effet,

$$R(s,t) \leq R(s-1,t) + R(s,t-1) \overset{\text{H.R.}}{\leq} \binom{s+t-3}{s-2} + \binom{s+t-3}{s-1} = \binom{s+t-2}{s-1}.$$

cqfd.

On connaît très peu de valeurs exactes de $R(s,t)$. Par exemple, on sait que $R(3,3) = 6$ et $R(4,4) = 18$, mais $R(5,5)$ n'est pas encore connu (on sait qu'il est entre 43 et 48).

Chapitre 5

Chaînes, parcours, cycles et tours

5.1 Chaînes, parcours

Définition 5.1. Soit $G = (S, A)$ un graphe et $k \in \mathbb{N}$ un entier naturel.

- Une ***k*-chaîne**, ou chaîne de longueur k, est un sous-graphe de G qui est isomorphe à une k-chaîne.

  Une k-chaîne peut être vue comme une suite

  $$(s_0, s_1, \ldots, s_k)$$

  de sommets distincts de G tels que $\{s_i, s_{i+1}\}$ est une arête de G pour tout $0 \leq i \leq k-1$.

- Un **parcours** de longueur k est une suite de sommets de G

  $$(s_0, s_1, \ldots, s_k)$$

  où $\{s_i, s_{i+1}\}$ est une arête de G pour tout $0 \leq i \leq k-1$.

  On dit que le parcours $\gamma = (s_0, s_1, \ldots, s_k)$ **visite** chacun des sommets s_i et chacune des arêtes $\{s_i, s_{i+1}\}$. Le sommet s_0 est l'**origine** de γ et s_k est son **extrémité**, et on dit que γ **relie** s_0 et s_k. Si $s_0 = s_k$ on dit que le parcours est **fermée**.

  Notez qu'une chaîne est un parcours dont tous les sommets sont distincts.

- Un ***k*-cycle**, ou cycle de longueur k, est un sous-graphe de G qui est isomorphe à un k-cycle.

  Un k-cycle peut être vu comme une suite

  $$(s_0, s_1, \ldots, s_{k-1}, s_k)$$

où $s_k = s_0$ et $s_0, \ldots, s_{k-1}$ sont des sommets distincts de G tels que $\{s_i, s_{i+1}\}$ est une arête de G pour $0 \leq i \leq k-1$.

- Un **tour** de longueur k est un parcours

$$(s_0, s_1, \ldots, s_k)$$

où $s_0 = s_k$ et toutes les arêtes $\{s_i, s_{i+1}\}$, $0 \leq i \leq k-1$, sont distinctes.

Remarque 5.2. La notation dans le polycopié de Bernardi (et d'autres ouvrages) est : 'chaîne' pour ce qu'on appelle ici 'parcours' et 'chaîne élémentaire' pour ce qu'on appelle ici 'chaîne' ; 'cycle' pour ce qu'on appelle ici 'tour' et 'cycle élémentaire' pour ce qu'on appelle ici 'cycle'.

Lemme 5.3. *S'il existe dans G un parcours γ reliant deux sommets x et y, alors il existe dans G une chaîne reliant x et y (dont les sommets et arêtes sont dans γ).*

Démonstration. Soit $\gamma' = (x = s_0, s_1, \ldots, s_k = y)$ un parcours de longueur minimale qui utilise des sommets et des arêtes de γ. Si les sommets s_i sont tous différents, alors γ est la chaîne cherché.

Sinon, si $s_i = s_j$ pour $i < j$, alors $\gamma' = (s_0, \ldots, s_i, s_{j+1}, \ldots, s_k)$ est un parcours qui relie x et y avec des sommets et des arêtes de γ qui est de longueur strictement plus courte que γ. Ce qui contredit son choix. **cqfd.**

5.1.1 Connexité

Un graphe est dit **connexe** si pour toute paire de sommets x et y de G, il existe un parcours reliant x à y. (On obtient une définition si on remplace *parcours* par *chaîne*, grâce au Lemme 5.3.)

Soit $G = (S, A)$ un graphe, on considère la relation binaire 'être relié à' définie sur S en posant x est relié à y si et seulement s'il existe un parcours reliant x et y. (Encore grâce au Lemme 5.3, on peut remplacer *parcours* par *chaîne* dans cette définition.)

Théorème 5.4. *La relation 'être relié à' est une relation d'équivalence sur S.*

Démonstration.

- Réflexive : (x) est un parcours de longueur 0 dont l'origine et l'extrémité sont x ;
- Symétrique : Si $(x, s_1, \ldots, s_k, y)$ est un parcours reliant x et y, alors $(y, s_k, \ldots, s_1, x)$ est un parcours reliant y et x ;

- Transitive : Si $(x, s_1, \ldots, s_k, y)$ est un parcours reliant x et y et $(y, w_1, \ldots, w_\ell, z)$ est un parcours reliant y et z, alors $(x, s_1, \ldots, s_k, w_1, \ldots, w_\ell, z)$ est un parcours reliant x et z.

cqfd.

Les classes d'équivalence de cette relation d'équivalence sont dites les **composantes connexes** de G. Un graphe est donc **connexe** s'il possède une seule composante connexe.

Théorème 5.5. *Un graphe $G = (S, A)$ est connexe si et seulement si pour toute partition de S en deux parties non vides U et V, il existe une arête $a \in A$ dont une extrémité est dans U et l'autre dans V.*

Démonstration.
$\Longrightarrow$: Soit G connexe et soient U et V une partition de S en deux parties non-vides. Soient $x \in U$ et $y \in V$. Comme G est connexe, il existe une chaîne $(x = s_0, \ldots, s_k = y)$ d'origine x et extrémité y. L'ensemble $I = \{i \in [0, k];\ s_i \in V\}$ n'est pas vide puisque $s_k = t \in V$, et ne contient pas 0 puisque $s_0 = s \in U$. Il admet donc un plus petit élément $r > 0$. On a que $s_{r-1} \notin V$, et donc $s_{r-1} \in U$ et $s_r \in V$. L'arête $\{s_{r-1}, s_r\}$ a une extrémité dans U et une autre dans V.
$\Longleftarrow$: Supposons que pour toute partition de S en deux parties non vides U et V, il existe une arête $a \in A$ dont une extrémité est dans U et l'autre dans V. Considérons deux sommets s et t de S. Notons U la composante connexe de s, et V son complémentaire. Si $t \in U$ alors s et t sont reliés. Supposons que $t \in V$ pour chercher une contradiction. Ni U ni V ne sont alors pas vides. On applique l'hypothèse sur G : il existe une arête $e = u, v$, avec u dans U et $v \in V$. Mais alors u et v sont dans la même composante connexe, et $v \in U$, ce qui est une contradiction. **cqfd.**

5.2 Distance

Définition 5.6. Soit $G = (S, A)$ un graphe connexe. On définit la **distance** entre deux sommets $s, t \in S$, notée $d_G(s, t)$, comme étant la longueur de la chaîne la plus courte existant de s à t.

Si G n'est pas connexe, on étend la définition en posant $d_G(s, t) = \infty$. Mais dans ce cas là, la fonction n'est pas une distance (une fonction $f : E \times E \to \mathbb{R}^+$ avec séparation ($d_G(s, t) = 0 \iff s = t$), symétrie ($d_G(s, t) = d_G(t, s)$) et inégalité triangulaire ($d_G(s, t) \leq d_G(s, x) + d_G(x, t) \forall s, x, t \in S$)).

Théorème 5.7. *Soit $G = (S, A)$ un graphe, et A_G sa matrice d'adjacence. Pour tout $k \in \mathbb{N}$ le nombre de parcours de longueur k reliant s_i à s_j est égal au coefficient $(A_G^k)_{ij}$ de la puissance k-ième de A_G.*

Démonstration. Par récurrence sur k. Pour $k = 0$, la matrice A_G^0 est la matrice identité I_n, et il est clair que le nombre de parcours de longueur 0 d'origine s_i et extrémité s_j vaut 1 si $i = j$ et 0 sinon.

Supposons la propriété vraie pour $k \in \mathbb{N}$ et montrons qu'elle est vraie au rang $k+1$. Un parcours de longueur $k+1$ d'origine s_i et extrémité s_j s'écrit $(s_0, \ldots, s_k, s_{k+1})$, avec $s_0 = s_i$ et $s_{k+1} = s_j$. Si $s_k = s_\ell$, alors $(s_0, \ldots, s_k)$ est un parcours de longueur k d'origine s_i et extrémité s_ℓ et $\{s_\ell, s_j\}$ est une arête de G.

Pour chaque voisin s_ℓ de s_j, soit P_ℓ le nombre de $(k+1)$-parcours reliant s_i à s_j telles que le k-ième sommet du parcours soit s_ℓ. Alors $|P_\ell|$ est égal au nombre de parcours de longueur k reliant s_i à s_ℓ. D'après l'hypothèse de récurrence, ce nombre est $(A_G^k)_{i\ell}$. Du principe d'addition, le nombre de parcours de longueur $k+1$ reliant s_i à s_j est la somme pour tous les voisins s_ℓ de s_j du nombre de parcours de longueur k reliant s_i à s_ℓ :

$$\sum_{s_\ell \text{ voisin de } s_j} |P_\ell| = \sum_{s_\ell \text{ voisin de } s_j} (A_G^k)_{i\ell} = \sum_{s_\ell \in S} (A_G^k)_{i\ell}(A_G)_{\ell j} = (A_G^{k+1})_{ij}.$$

cqfd.

Corollaire 5.8. *La distance entre deux sommets distincts s_i, s_j de G vérifie*

$$d_G(s_i, s_j) = \min\left\{k \geq 0 :\ (A_G^k)_{ij} \neq 0\right\}.$$

5.2.1 Graphes valués et Algorithme de Dijkstra

Définition 5.9. Un **graphe valué** (S, A, μ) est un graphe $G = (S, A)$ muni d'une fonction $\mu : A \to \mathbb{R}_+^*$ appelée **valuation** (ou **coût**, ou **poids** ou **longueur**...).

La valuation d'un parcours $\gamma = (s_0, s_1, \ldots, s_k)$ est alors définie par

$$\mu(\gamma) = \sum_{i \in [1,k]} \mu(\{s_{i-1}, s_i\}).$$

On définit la distance $d_\mu(s,t)$ entre deux sommets d'un graphe valué comme le minimum des valuations des chaînes d'origine s et extrémité t, si une telle chaîne existe, et ∞ s'il n'en existe pas.

Observation 5.10. Si on pose $\mu(a) = 1$ pour toute $a \in A$, alors $d_\mu(s,t) = d_G(s,t)$.

Pour déterminer $d_\mu(s,t)$ pour un sommet fixé s et tout sommet $t \in S$, on peut

utiliser l'**algorithme de Dijkstra** :

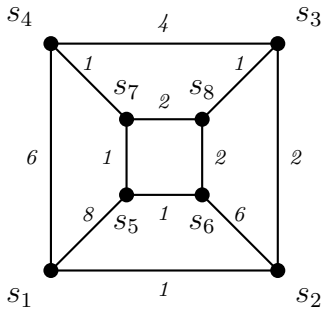
Algorithme 1 : Algorithme de Dijkstra

Données : Un sommet s d'un graphe valué $G = (S, A, \mu)$
Résultat : Pour tout t dans S, $C[t]$ contient $d_\mu(s,t)$. Si $0 < C[t] < \infty$, alors $T[t]$ contient la première étape dans une chaîne de coût minimal menant de t à s.

pour chaque t *dans* S **faire** $C[t] \leftarrow \infty$;
$C[s] \leftarrow 0$;
$V \leftarrow \varnothing$; `// ensemble des sommets dont on connaît la distance`
$W \leftarrow S$; `// complément de` V
tant que *il y a dans* W *un sommet* t *tel que* $C[t]$ *est fini* **faire**
  $u \leftarrow$ un sommet de W tel que $C[u]$ soit minimal ;
  $V \leftarrow V \cup \{u\}$;
  $W \leftarrow W \setminus \{u\}$; `// On transfère` u `de` W `vers` V
  pour chaque *voisin* x *de* u **faire**
    si $C[u] + d_\mu(\{u,x\}) < C[x]$ **alors**
      $C[x] \leftarrow C[u] + d_\mu(u,x)$;
      $T[x] \leftarrow u$;
    fin
  fin
fin

Pour montrer que cet algorithme est correct, il suffit de vérifier que l'*invariant de boucle* suivant est maintenu : si $t \neq s$ est dans V, alors il existe un chemin de moindre coût de t à s commence par $T[t]$ et reste dans V. On peut montrer que la complexité de cet algorithme est en $\mathcal{O}((n+m)\log(n))$, où n est le nombre de sommets et m le nombre d'arêtes.

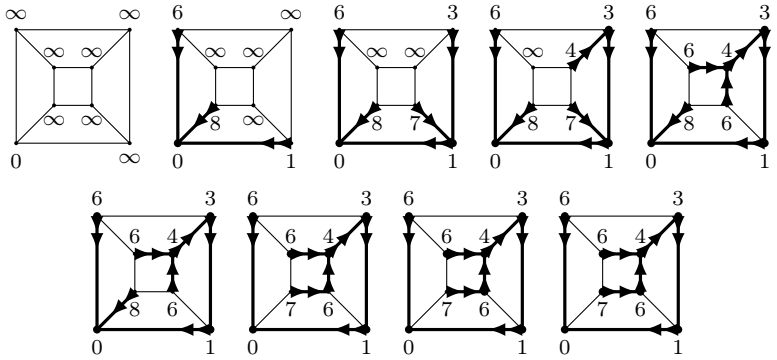
Voici par exemple les étapes de l'algorithme sur la valuation suivante du cube Q_3.



Nous les représentons dans le tableau suivant, où chaque ligne est une nouvelle itération de l'algorithme, et nous montrons les valeurs de V et des entrées de C. A coté de chaque entrée de C, entre parenthèses, nous montrons les entrés de T.

V	$C[s_1]$	$C[s_2]$	$C[s_3]$	$C[s_4]$	$C[s_5]$	$C[s_6]$	$C[s_7]$	$C[s_8]$
$\varnothing$	$\mathbf{0}$	∞	∞	∞	∞	∞	∞	∞
$\{s_1\}$		$\mathbf{1(s_1)}$	∞	$6(s_1)$	$8(s_1)$	∞	∞	∞
$\{s_1, s_2\}$			$\mathbf{3(s_2)}$	$6(s_1)$	$8(s_1)$	$7(s_2)$	∞	∞
$\{s_1, s_2, s_3\}$				$6(s_1)$	$8(s_1)$	$7(s_2)$	∞	$\mathbf{4(s_3)}$
$\{s_1, s_2, s_3, s_8\}$				$\mathbf{6(s_1)}$	$8(s_1)$	$6(s_8)$	$6(s_8)$	
$\{s_1, s_2, s_3, s_8, s_4\}$					$8(s_1)$	$\mathbf{6(s_8)}$	$6(s_8)$	
$\{s_1, s_2, s_3, s_8, s_4, s_6\}$					$7(s_6)$		$\mathbf{6(s_8)}$	
$\{s_1, s_2, s_3, s_8, s_4, s_6, s_7\}$					$\mathbf{7(s_6)}$			
$\{s_1, s_2, s_3, s_8, s_4, s_6, s_7, s_5\}$								

Une représentation alternative du déroulement de l'algorithme est donnée dans le dessin suivant. Ici, les étiquettes des sommets représentent le tableau C et le tableau T est représenté par des flèches qui pointent de t vers $T[t]$. Si un sommet est dans V, le point correspondant est plus gros.



Avec ce dessin, il suffit de suivre les flèches pour trouver le chemin à moindre coût qui amène au coin en bas à gauche.

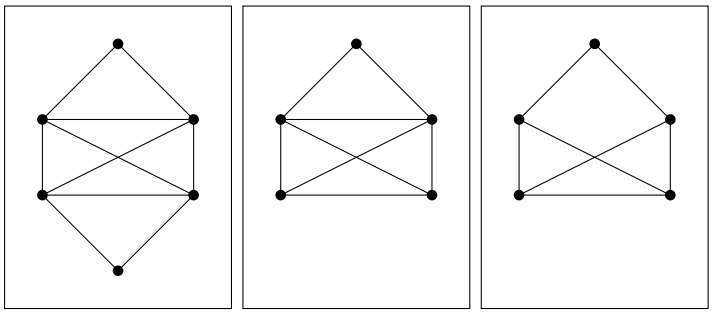
5.3 Tours et parcours eulériens (et hamiltoniens)

5.3.1 Graphes eulériens

Un **tour eulérien** d'un graphe G est un tour qui visite (au moins une fois) chaque sommet de G et une fois (et une seule) chaque arête de G. Un **graphe eulérien** est un graphe qui admet un tour eulérien.

Un **parcours eulérien** est un parcours qui visite une fois et une seule chaque arête de G, et au moins une fois chaque sommet de G. Un graphe **semi-eulérien** est un graphe qui admet un parcours eulérien.

Des trois graphes suivants, le premier est eulérien, le second est semi-eulérien sans être eulérien, et le troisième n'est pas semi-eulérien.



Théorème 5.11. *Soit G un graphe d'ordre au moins 2. Alors G est eulérien si et seulement s'il est connexe et tous ses sommets sont de degré pair.*

Démonstration.

$\Longrightarrow$ Soit $G = (S, A)$ un graphe eulérien et $\gamma = (s_0, s_1, \ldots, s_k = s_0)$ un tour eulérien. Alors G est connexe. En effet, tout sommet de G est dans γ et pour toute paire $s_i, s_j \in S$ avec $i < j$, $(s_i, s_{i+1}, \ldots, s_{j-1}, s_j)$ est un parcours qui les relie.

Pour $s \in S$, soit A_s l'ensemble des arêtes incidentes à s. On dit que $a \in A_s$ est **entrante** si $s = s_i$ et $a = \{s_{i-1}, s_i\}$, et **sortante** si $s = s_i$ et $a = \{s_i, s_{i+1}\}$. L'application $\{s_{i-1}, s_i\} \mapsto \{s_i, s_{i+1}\}$ (et $\{s_{k-1}, s_k\} \mapsto \{s_0, s_1\}$ si $s_k = s$) est une bijection entre les arêtes sortantes et les arêtes entrantes de A_s. On en déduit que $|A_s| = d(s)$ est pair.

$\Longleftarrow$ Soit G connexe avec tous les sommets de degré pair. On considère un parcours sans arêtes répétées $\gamma = (s_0, \ldots, s_k)$ de longueur maximale (qui existe car le nombre d'arêtes est fini). On va montrer que γ est un tour eulérien.

D'abord, on voit que forcement $s_0 = s_k$. Sinon, le nombre d'arêtes de γ incidentes à s_k serait impair, mais comme le degré de s_k dans G est pair, il y aurait forcement une arête de G incidente à s_k qui ne serait pas dans γ. En l'ajoutant à γ on obtiendrait un parcours plus long sans arêtes répétées, contredisant le choix de γ.

De plus, toutes les arêtes de E sont visitées par γ. Supposons que $\{u, v\}$ soit une arête qui n'est pas visitée par γ. Par connexité, il existe alors une chaîne

$$s_0 = u_0, u_1, \ldots, u_r = u$$

qui relie s_0 et u. Posons $u_{r+1} = v$ et soit a la première arête de cette chaîne qui n'appartient pas à γ (un telle arête existe car $\{u_r, u_{r+1}\}$ n'est pas dans γ). Cette arête est forcement incidente à un sommet de γ de la forme $\{s_i, t\}$ avec $s_i \in \gamma$. Alors

$$(t, s_i, s_{i+1}, \ldots, s_k = s_0, s_1, \ldots, s_{i-1})$$

est un parcours sans arêtes répétées plus long que γ. Ce qui contredit le choix de γ.

Supposons enfin qu'il existe un sommet s non visité par γ. Comme G est connexe, il existe une arête e incidente à s, et cette arête n'est pas visitée par γ, ce qui est impossible comme on vient de le voir. **cqfd.**

Corollaire 5.12. *Un graphe G est semi-eulérien si et seulement si il est connexe et le nombre de ses sommets de degré impair est* 0 *ou* 2.

Démonstration.

$\Longrightarrow$ Supposons γ est un parcours semi-eulérien de G. Alors G est connexe, car tous les sommets sont relies à travers de γ. De plus, comme on a vu dans la preuve précédente, tous les sommets qui ne sont pas une extrémité ont forcement degré pair. Comme le nombre de sommets de degré impair est pair, ce nombre doit valoir 0 ou 2.

$\Longleftarrow$ Si G n'a pas de sommets de degré impair, alors G est eulérien et donc semi-eulérien. Si G a deux sommets de degré impair u et v, on ajoute un nouveau sommet s au graphe et les arêtes $\{u, s\}$ et $\{u, t\}$. Le graphe G' qu'on obtient est bien connexe et à tous le sommets de degré pair. Il est donc eulérien et a un tour eulérien γ. Les arêtes $\{u, s\}$ et $\{u, t\}$ sont forcement consécutives dans le tour. En les retirant de γ, on obtient un parcours semi-eulérien de G. **cqfd.**

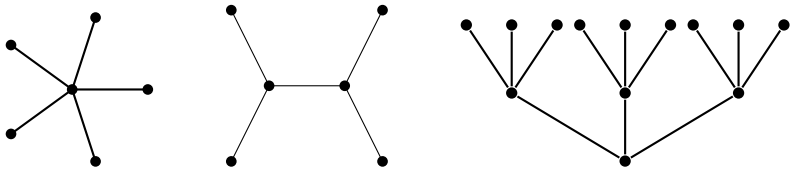
5.3.2 Graphes hamiltoniens

Un **cycle hamiltonien** est un cycle qui visite tous les sommets d'un graphe. Sa longueur est donc l'ordre n du graphe. Un **graphe hamiltonien** est un graphe qui admet un cycle hamiltonien. Une **chaîne hamiltonienne** est une chaîne qui visite tous les sommets d'un graphe. Un graphe **semi-hamiltonien** est un graphe qui admet une chaîne semi-hamiltonienne.

5.4 Arbres

Définition 5.13. Une **forêt** est un graphe **acyclique**, qui ne contient pas de cycle. Un **arbre** est un graphe connexe acyclique.

Voici quelques arbres.



Un **sommet pendant** ou **feuille** d'un graphe est un sommet de degré 1.

Lemme 5.14. *Si $G = (S, A)$ est une forêt, et si A n'est pas vide, alors il y a au moins deux feuilles dans G.*

Démonstration. Soit

$$\gamma = (v_0, v_1, \ldots, v_k)$$

une chaîne de longueur maximale. Comme A n'est pas vide, alors $k > 0$. On va montrer que v_0 et v_k sont des feuilles.

En effet, si $u \neq v_1$ était un autre voisin de v_0 :

- Si $u = v_i$ pour un $i > 1$, alors $(v_0, v_1, \ldots, v_i, u)$ serait un cycle, ce qui contredirait l'acyclicité de G ;
- et si $u \neq v_i$ pour tout i, alors $(u, v_0, \ldots, v_k)$ serait une chaîne de longueur $k + 1$, encore une contradiction.

On en déduit $d(v_0) = 1$, et de même $d(v_k) = 1$. **cqfd.**

Corollaire 5.15. *Si $G = (S, A)$ est un arbre d'ordre $|S| = n$, alors il y a dans A exactement $n - 1$ arêtes.*

Démonstration. Par récurrence sur n. Pour $n = 1$, $A = \varnothing$ et $|A| = 0$.

Si $n > 1$, il y a au moins deux sommets. Comme G est connexe, il y a au moins une chaîne qui les joint, donc A n'est pas vide. Il y a donc au moins un sommet pendant s, qui est adjacent à une unique arête e. Le graphe $G' = G \setminus \{s\} = (S \setminus \{s\}, A \setminus \{e\})$ est un arbre d'ordre $n - 1$. On peut lui appliquer l'hypothèse de récurrence. On a

$$|A| - 1 = |A \setminus \{e\}| = |S \setminus \{s\}| - 1 = (|S| - 1) - 1,$$

et donc $|A| = |S| - 1$. **cqfd.**

Lemme 5.16. *Si un graphe $G = (S, A)$ admet deux chaînes distinctes $\gamma = (v_0 = u, v_1, \ldots, v_\ell = v)$ et $\delta = (w_0 = u, w_1, \ldots, w_m = v)$ qui relient u et v, alors G contient un cycle.*

Démonstration. Soit $1 \leq i \leq \ell - 1$ le plus petit index tel que $v_i \neq w_i$ (qui existe car les chaînes sont distinctes), et soit j, $i < j \leq \ell$, le plus petit index plus grand que i tel qu'il existe un k, $i < k \leq m$, tel que $v_j = w_k$ (qui existe car $v_\ell = w_m$). Alors

$$(v_{i-1}, \ldots, v_j, w_{k-1}, w_{k-2}, \ldots, w_{i-1})$$

est un cycle. **cqfd.**

Théorème 5.17. *Soit $G = (S, A)$ un graphe d'ordre n. Les propriétés suivantes sont équivalentes :*

(i) *G est un arbre (acyclique et connexe).*

(ii) *Pour tout couple (u, v) de sommets, il existe une chaîne simple d'origine u et extrémité v et une seule.*

(iii) *G est connexe et a $n - 1$ arêtes.*

(iv) *G est une forêt (acyclique), et $m = n - 1$.*

(v) *G est connexe, et pour toute arête $e \in A$, $G \setminus e = (S, A \setminus e)$ n'est pas connexe (G est connexe minimal).*

(vi) *G est une forêt, et pour toute arête $e \notin A$, $G \cup e = (S, A \cup \{e\})$ admet un cycle (G est une forêt maximale).*

Démonstration.

(i) $\Longrightarrow$ (ii) L'existence d'un chemin est impliquée par la connexité, et l'unicité est impliquée par l'acyclicité, grâce au Lemme 5.16.

(i) $\Longleftarrow$ (ii) L'existence d'un chemin implique la connexité, et l'unicité implique l'acyclicité, car dans il y a deux chaînes distinctes reliant toute paire de sommets d'un cycle.

(i) $\Longrightarrow$ (iii) Voir Lemme 5.15.

(i) $\Longleftarrow$ (iii) Il faut montrer l'acyclicité. Si G avait un cycle, alors on pourrait supprimer une arête e du cycle sans changer la connexité du graphe (car on peut remplacer toute apparition de cette arête dans un parcours par l'autre partie du cycle). Après avoir effectué cette opération avec tous les cycles, nous arrivons à un graphe acyclique et connexe, et donc un arbre, à moins de $n - 1$ arêtes, ce qui contredit le Lemme 5.15.

(i) $\Longrightarrow$ (iv) Voir Lemme 5.15.

(i) $\Longleftarrow$ (iv) Si G n'était pas connexe, alors l'ajout d'une arête entre deux composantes connexes distinctes ne crée pas de cycle (s'il y avait un cycle, ces deux sommets seraient déjà dans la même composante connexe avant l'ajout de l'arête). On pourrait ajouter des arêtes jusqu'à on ait un graphe connexe et acyclique avec plus de $n - 1$ arêtes, ce qui contredit le Lemme 5.15.

(i) $\Longrightarrow$ (v) G est connexe par définition. S'il y avait une arête e telle que $G \setminus e$ est toujours connexe, alors il y aurait une chaîne γ joignant les deux extrémités de e. La concaténation de cette chaîne avec e est un cycle. Contradiction.

(i) $\Longleftarrow$ (v) G est connexe par définition. G n'a pas de cycle, car sinon on pourrait supprimer une arête du cycle et le graphe resterait connexe (car on peut remplacer toute apparition de cette arête dans un parcours par l'autre partie du cycle).

(i) $\Longrightarrow$ (vi) G est acyclique par définition. Soient u, v deux sommets qui ne sont pas adjacents. Comme G est connexe, il existe une chaîne γ qui les relie. L'ajout de l'arête (u, v) crée un cycle.

(i) $\Longleftarrow$ (v) G est acyclique par définition. Montrons qu'il est connexe. Soient, $u, v \in S$. S'ils sont adjacents ils sont reliés par une chaîne. S'ils ne le sont pas, soit $G' = G \cup \{u, v\}$. G' contient un cycle γ, qui doit utiliser l'arête $\{u, v\}$ car G est acyclique. Alors $\gamma \setminus \{u, v\}$ est un parcours qui relie u et v.

cqfd.

Remarque 5.18. Ce théorème est complètement analogue au résultat suivant d'algèbre linéaire (et ceci n'est pas une coïncidence) :

Théorème 5.19. *Soit E un K-espace vectoriel de dimension n, et $B = (b_i)_{1 \leq i \leq m}$ une famille finie d'éléments de E. Les propriétés suivantes sont équivalentes :*

(i) B est une base de E.

(ii) Pour tout vecteur $x \in E$, il existe une famille $(\lambda_i)_{1 \leq i \leq m}$ de scalaires telle que $\sum_{i=1}^{m} \lambda_i b_i = x$ et une seule.

(iii) B est une famille génératrice de E et $m = n$.

(iv) B est une famille libre et $m = n$.

(v) B est une famille génératrice de E et pour tout $i \leq m$ la famille obtenue en enlevant b_i à B ne l'est pas (B est génératrice minimale).

(vi) B est libre et quelle que soit la valeur de b_{m+1}, la famille $(b_i)_{1 \leq i \leq m+1}$ ne l'est pas (B est libre maximale).

Chapitre 6

Coloration, graphes bipartis et couplages

6.1 Colorations

Définition 6.1. Une application $f : S \to C$ de l'ensemble des sommets d'un graphe $G = (S, A)$ est une **coloration** du graphe si $f(u) \neq f(v)$ pour toute arête $\{u, v\} \in A$. On appelle **couleur** du sommet s l'élément $f(s)$ de C et la condition s'exprime sous la forme "Si deux sommets sont voisins, ils sont de couleurs différentes".

On dit que G est ***k*-coloriable** s'il existe une coloration de G utilisant au plus k couleurs. Le **nombre chromatique** $\chi(G)$ du graphe G est le plus petit entier k pour lequel il est k-coloriable.

Observation 6.2. Si f est surjective, les ensembles de sommets des différentes couleurs forment une partition de S en k stables.

Proposition 6.3.

- $\chi(G) = 1$ *si et seulement si* G *est un* n*-stable,*
- $\chi(G) = n$ *si et seulement si* G *est une* n*-clique,*
- $\chi(P_n) = 2$ *pour* $n \geq 1$*,*
- $\chi(C_n) = \begin{cases} 2 \text{ si } n \geq 4 \text{ est pair} \\ 3 \text{ si } n \geq 3 \text{ est impair.} \end{cases}$,
- $\chi(Q_d) = 2$ *pour* $d \geq 1$*,*
- $\chi(Petersen) = 3$*,*

- $\chi(K_{n_1,\ldots,n_k}) = k$.

La preuve de cette proposition sera faite en exercice.

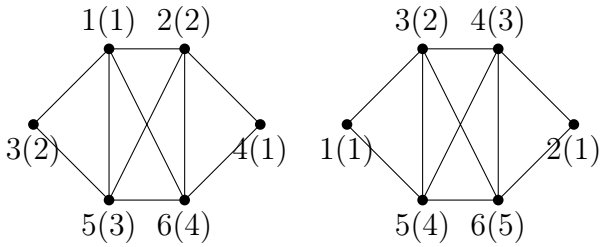
À chaque numérotation $[1, n] \to S$ des sommets, on fait naturellement correspondre une coloration par des entiers naturels non nuls grâce à l'**algorithme glouton** :

Algorithme 2 : Algorithme glouton

Données : Un graphe $G = (S, A)$
Résultat : Une coloration de $f : S \to \mathbb{N}$ de G.
pour $i \leftarrow 0$ **à** n **faire**
  colorier le sommet i avec la première couleur parmi $\{1, 2, 3 \ldots\}$ qui n'est pas déjà utilisée par un voisin du sommet i
fin

Ainsi, le sommet s_1 est colorié avec la couleur 1, le sommet s_2 est colorié avec la couleur 2 s'il est voisin de s_1 et avec la couleur 1 sinon, etc.

Dans la figure suivante, nous avons appliqué cet algorithme deux fois au même graphe, mais avec des numérotations différentes des sommets. Entre parenthèses les numéros des couleurs sont indiqués. On voit que la première numérotation utilise 4 couleurs en tout alors que la deuxième en utilise 5. On peut montrer qu'il existe toujours une numérotation des sommets telle que l'algorithme glouton utilise $\chi(G)$ couleurs, mais cela n'a rien d'évident (nous le ferons en exercice).



Proposition 6.4. *Le nombre chromatique d'un graphe vérifie*

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

où $\Delta(G)$ est le maximum des degrés des sommets de G

Démonstration. En fait, quel que soit l'ordre choisi sur les sommets, l'algorithme glouton utilise au maximum $\Delta(G)+1$ couleurs distinctes. Soit en effet k le numéro de la plus haute couleur utilisée, et s un sommet qui a cette couleur. L'algorithme glouton attribue la couleur k à s parce que les voisins de s déjà coloriés occupent toutes les couleurs de 1 à $k-1$. Donc s a au moins $k-1$ voisins distincts, et $k - 1 \leq \Delta(G)$, d'où $\chi(G) \leq k \leq \Delta(G) + 1$. **cqfd.**

6.1.1 Graphes bipartis

Un graphe est dit **biparti** s'il est 2-coloriable. Équivalemment, si on peut diviser l'ensemble de sommets en deux parties X, Y disjointes de façon que chaque arête du graphe ait une extrémité dans X et l'autre dans Y [1]. Les parties X et Y sont appelées les **classes** de la bipartition (cette bipartition n'est pas unique en général).

Par exemple, les graphe bipartis complets $K_{n,m}$ et les cycle C_n pour n pair sont des graphes bipartis.

Théorème 6.5. *Un graphe $G = (S, A)$ est biparti si et seulement s'il n'existe pas dans G de cycle de longueur impaire.*

Démonstration. Si G est biparti, il existe une partition $S = X \sqcup Y$ telle que toute arête ait une extrémité dans X et une autre dans Y. Si $\gamma = (v_0, v_1, \ldots, v_k = v_0)$ est un k-cycle et si $v_0 \in X$, on voit, par récurrence sur i, que $v_i \in X$ pour i pair et $v_i \in Y$ pour i impair. On sait que $v_k \in X$. Donc k est pair.

Réciproquement, supposons que G n'admette pas de cycle impair. Sans perte de généralité, nous pouvons supposer que G est connexe (car un graphe est biparti si et seulement si chacune de ses composantes connexes l'est). Choisissons un sommet $s \in S$. Notons

$$\begin{aligned} X &= \{\text{extrémités des } k\text{-chaînes d'origine } s, \text{ avec } k \text{ pair}\} \\ Y &= \{\text{extrémités des } k\text{-chaînes d'origine } s, \text{ avec } k \text{ impair}\} \end{aligned}$$

Comme G est connexe, il est clair que $S = X \cup Y$. D'autre part, tout voisin d'un élément de X est dans Y et tout voisin d'un élément de Y est dans X. Il reste à prouver que $X \cap Y = \varnothing$. Si $t \in X \cap Y$ il existe une chaîne paire γ et une chaîne impaire δ d'origine s et extrémité t. La concaténation de ces deux chaînes est un parcours fermé de longueur impaire. On peut donc en extraire un cycle impair (voir exercices), une contradiction. **cqfd.**

6.2 Couplages

Définition 6.6. Un **couplage** d'un graphe $G = (S, A)$ est un ensemble $M \subseteq A$ d'arêtes tel que deux d'entre elles n'ont pas d'extrémité en commun. Un sommet est dit **saturé** s'il est extrémité d'une arête de M, et $X \subseteq S$ est **saturé** si tous ses sommets le sont. Un couplage est dit **parfait** si S est saturé.

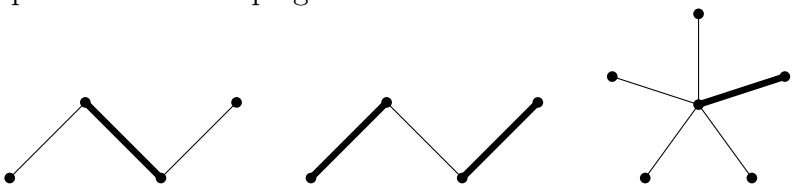
Exemples 6.7. Considérons le graphe biparti complet $K_{n,n}$ avec classes de bipartition $X = \{x_1, \ldots, x_n\}$ et $Y = \{y_1, \ldots, y_n\}$. Un couplage parfait de $K_{n,n}$ définit une bijection entre X et Y. Il y a donc $n!$ couplages parfaits de $K_{n,n}$.

1. Nous acceptons que les parties X et Y soient vides, et donc un graphe sans arêtes est biparti selon cette définition.

Pour les graphes complets, l'existence d'un couplage parfait dépend de la parité de son ordre. K_{2n+1} n'admet pas de couplage parfait, car le nombre de sommets est impair. K_{2n} admet $(2n-1)(2n-3)\cdots 3\cdot 1$ couplages parfaits.

Définition 6.8. Un couplage est dit **maximal** si on ne peut pas lui ajouter d'arête, et **maximum** s'il a le plus grand nombre possible d'arêtes.

Exemple 6.9.
Voici trois graphes avec des couplages :



Maximal	Oui	Oui	Oui
Maximum	Non	Oui	Oui
Parfait	Non	Oui	Non

Soit $G = (S, A)$ un graphe et M un couplage de G. Un chaîne **alternée** est une chaîne dont les arêtes sont alternativement dans M et dans $A \setminus M$. Elle est dite **augmentante** si ses extrémités ne sont pas saturées.

Théorème 6.10 (Berge 1957)**.** *Un couplage M est maximum si et seulement s'il n'existe pas de chaîne augmentante dans G.*

Démonstration. On montre la contraposée des deux implications.

$\Longrightarrow$ Supposons qu'il existe une chaîne augmentante $\gamma = (v_0, \ldots, v_k)$. Et soit M' le couplage obtenu par l'échange des arêtes de M le long de la chaîne γ. C'est facile de vérifier que M' est aussi un couplage, qui a une arête de plus que M, ce qui montre que M n'était pas maximum.

$\Longleftarrow$ Supposons que M est un couplage non-maximum, et soit M' un couplage tel que $|M'| \geq |M|$. Considérons le sous-graphe H engendré par les arêtes de G qui sont dans M ou dans M', mais pas dans les deux. Tout sommet de H est de degré ≤ 2. C'est facile à voire que les composantes connexes de H doivent être des cycles ou bien des chaînes. Les cycles doivent être de longueur pair, car ses arêtes sont alternées, et ont donc le même nombre d'arêtes de M et M'. Les chaînes doivent être aussi alternées. Comme le nombre d'arêtes de M' est supérieur à celui de M, au moins une de ces chaînes doit avoir une arête de plus de M' que de M. C'est une chaîne augmentante pour M. **cqfd.**

Soit $G = (S, A)$ un graphe et $X \subset S$, le **voisinage** $N(X)$ est l'ensemble des voisins des sommets de S, $\{s \in S : \exists x \in X, \{s, x\} \in A\}$.

Théorème 6.11 (Hall 1935)**.** *Un graphe biparti G de bipartition X, Y admet un couplage saturant X si, et seulement si*

$$|N(U)| \geq |U|$$

pour tout $U \subset X$.

Démonstration.

$\Longrightarrow$ Pour tout $U \subset X$, les voisins dans M des sommets de U sont des sommets différents de $N(U)$. D'où $|S| \leq |N(S)|$.

$\Longleftarrow$ Par contraposée. Supposons que M est un couplage maximum qui ne sature pas X, alors nous allons construire un ensemble U tel que $|N(U)| < |U|$.

Soit $s \in X$ un sommet qui n'est pas saturé, et soient

- V l'ensemble de sommets de Y qui sont reliés à s par une chaîne alternée, et
- U l'ensemble de sommets de X qui sont reliés à s par une chaîne alternée (en particulier $s \in U$).

Soit $M' \subset M$ l'ensemble des arêtes de M qui sont incidentes à un sommet de $U \cup V$. Nous allons montrer d'abord que M' est un couplage parfait entre $U \setminus \{s\}$ et V. Toute chaîne alternante qui relie s à $x \in U \setminus \{s\}$ doit avoir la dernière arête dans M', par parité. Donc tout $x \in U \setminus \{s\}$ est incident à (exactement) une arête de M'.

S'il y avait un sommet $y \in V$ qui n'était incident à aucune arête de M', alors la chaîne qui le relie à s serait augmentante, et M ne serait pas maximum. Donc tout $y \in V$ est incident à (exactement) une arête de M'. D'où M' est un couplage parfait entre $U \setminus \{s\}$ et V, et $|U \setminus \{s\}| = |M'| = |V|$.

Montrons que $N(U) \subseteq V$. Soit $x \in U$ et soit γ une chaîne alternante entre s et x. Soit $y \in N(x)$. Si $y \in \gamma$, alors $y \in V$. Si $y \notin \gamma$, alors on ajoute l'arête $\{x, y\}$ à γ et on obtient une chaîne alternante de u à y, d'où $y \in V$.

Donc $|N(U)| \leq |V| = |U| - 1$, ce qui complète la preuve. **cqfd.**

Corollaire 6.12. *Pour $k > 0$, tout graphe biparti k-régulier contient un couplage parfait.*

Démonstration. Soit $G = (S, A)$ un graphe biparti k-régulier de bipartition (X, Y). En comptant les arêtes par leur extrémité dans X ou par leur extrémité dans Y on retrouve $|A| = k|X| = k|Y|$. D'où $|X| = |Y|$.

Soit maintenant $U \subset X$ et soit T l'ensemble des arêtes incidentes a un sommet de U. Alors $|T| = k|U|$. Ces arêtes font partie des $k|N(U)|$ arêtes incidentes à $N(U)$. D'où

$$k|U| \leq k|N(U)| \implies |U| \leq |N(U)|.$$

Le graphe contient donc un couplage qui sature X. Comme $|X| = |Y|$, le couplage sature aussi $|Y|$ et est un couplage parfait. **cqfd.**

Chapitre 7

Planarité

7.1 Dessiner des graphes dans le plan

Nous allons étudier les graphes qui peuvent être dessinés dans le plan sans des croisements d'arêtes, les **graphes planaires**. Cette partie est plus informelle que celles précédentes car pour certaines preuves une démonstration rigoureuse a besoin de connaissances de topologie que nous n'avons encore pas.

Définition 7.1 (informelle)**.** Un dessin d'un graphe G dans le plan tel que le dessin de deux arêtes distinctes sont d'intersection vide sauf aux extrémités est appelé un **dessin plan**. Un graphe est **planaire** s'il admet un dessin plan.

Pour formaliser cette définition il faut parler de arcs et courbes de Jordan. Un **arc** est un sous-ensemble $\alpha \subset \mathbb{R}^2$ qui est l'image $\alpha = \gamma([0,1]) = \{\gamma(x) : x \in [0,1]\}$ d'une fonction $\gamma : [0,1] \to \mathbb{R}^2$ qui est injective et continue de l'intervalle fermé $[0,1]$ au plan. Les points $\gamma(0)$ et $\gamma(1)$ sont les extrémités de l'arc. Une **courbe de Jordan** est un arc dont les extrémités coïncident (donc injective seulement sur $[0,1)$). Le théorème crucial pour tout preuve rigoureuse sur les graphes planaires est le Théorème de la courbe de Jordan. Intuitivement, il est évidant, mais une preuve formelle n'est pas du tout simple.

Théorème 7.2. *Toute courbe de Jordan α divise son complémentaire en deux parties connexes : l'intérieur d'α et l'extérieur d'α. Et α constitue le bord de ces deux parties : tout arc joignant un point interne et un point externe doit intersecter α.*

Nous allons faire une présentation informelle sans preuves rigoureuses. Commençons avec une preuve informelle du fait que K_5 et $K_{3,3}$ ne sont pas planaires.

Théorème 7.3. *K_5 et $K_{3,3}$ ne sont pas planaires.*

Idée de la preuve. Soit C un cycle couvrant de K_5 ou $K_{3,3}$. Il doit être dessiné comme une courbe fermée. Les cordes doivent être dessinées soit à l'intérieur soit à l'extérieur. Deux cordes sont en conflit si ses extrémités s'alternent. Si deux cordes sont en conflit, une doit être dessinée à l'intérieur et l'autre à l'extérieur.

$K_{3,3}$ contient 3 cordes qui sont en conflit deux-à-deux. Nous en pouvons placer au plus une à l'intérieur et au plus une à l'extérieur.

K_5 contient 5 cordes. Chaque corde est compatible avec deux cordes, qui ne sont pas compatibles entre elles. On peut donc au plus placer deux cordes à l'intérieur et deux cordes à l'extérieur. **cqfd.**

La raison pour laquelle on présente ces deux exemples c'est que, dans un certain sens, ils sont la seule obstruction pour être planaire. Le graphe obtenu par **subdivision** de l'arête $\{u, v\}$ du graphe $G = (S, A)$ est le graphe $G' = (S', A')$ avec $S' = S \cup \{x\}$ et $A' = A \cup \{u, x\} \cup \{x, v\} \setminus \{u, v\}$. G' est une **subdivision** de G s'il est obtenu par des subdivisions d'arêtes successives.

Théorème 7.4 (Kuratowski)**.** *Un graphe G est planaire si et seulement s'il ne contient pas de sous-graphe isomorphe à une subdivision de $K_{3,3}$ ou K_5.*

7.2 Formule d'Euler

Les **faces** d'un dessin plan d'un graphe $G = (S, A)$ sont les composantes connexes du complément du dessin. Il y a une face externe (pas bornée) et plusieurs faces internes (bornées). Une arête est **incidente** à une face si elle appartient à sa frontière.

Observation 7.5. Une arête d'un graphe plan est incidente à :

- deux faces distinctes si elle appartient à un cycle,
- une seule face si elle n'appartient pas à un cycle.

L'ensemble des arêtes incidentes à une face fixée forme un parcours fermé de G.

Lemme 7.6. *Tout arbre est planaire et se dessine avec une seule face externe.*

Théorème 7.7. *Soit $G = (S, A)$ un graphe planaire connexe avec $s = |S|$ sommets et $a = |A|$ arêtes. Et soit f le nombre de faces d'un dessin plan de G. Alors,*

$$s - a + f = 2.$$

Démonstration. Par récurrence sur le nombre d'arêtes du graphe. Si $a = 0$, le graphe contient un seul sommet et le dessin une seule face (la face externe). On a donc $s - a + f = 1 - 0 + 1 = 2$.

Supposons donc $a \geq 1$. Nous distinguons deux cas :

1. Le graphe n'a pas de cycle. Alors G est un arbre et $a = s - 1$; et il y a une seule face (la face externe). On a donc,

$$s - a + f = s - (s - 1) + 1 = 2.$$

2. Sinon, G contient une arête e dans un cycle. Alors $G \setminus e$ est connexe et vérifie l'hypothèse de récurrence car on peut enlever l'arc qui correspond à e au dessin plan de G pour obtenir un dessin plan de $G \setminus e$. Dans le dessin initial, e était incidente à deux faces F_1 et F_2, qui deviennent une seule après avoir enlevé l'arête e. Donc, f' est le nombre de faces du dessin de $G \setminus e$, on a $f' = f - 1$. Et le nombre de sommets et arêtes de $G \setminus e$ sont $s' = s$ et $a' = a - 1$.

   On obtient donc de l'hypothèse de récurrence

$$2 = s' - a' + f' = s - (a - 1) + (f - 1) = s - a + f.$$

cqfd.

Corollaire 7.8. *Soit $G = (S, A)$ un graphe planaire avec au moins 3 sommets. Alors $|A| \leq 3|S| - 6$.*

Démonstration. Soit F l'ensemble de faces du dessin de G. Soit

$$I = \{(e, f) \in E \times F : \ e \text{ arête au bord de la face } f\}$$

l'ensemble de paires arête-face incidentes.

Observons d'abord que toute face est bordée par un parcours fermée de G qui est de longueur ≥ 3. (Comme il n'y a pas de boucle, un parcours de longueur 2 s'obtient seulement quand il y a une seule arête, mais on a ≥ 2 sommets.) Donc $|I| \geq 3|F|$.

De plus, chaque arête est incidente à au plus 2 faces. Donc $2|A| \geq |I|$. On a donc, $3|F| \leq 2|A|$.

De plus, de la formule d'Euler, $|F| = 2 - |S| + |A|$. Donc,

$$\begin{aligned} 3(2 - |S| + |A|) = 3|F| &\leq 2|A| \\ 6 - 3|S| + 3|A| &\leq 2|A| \\ |A| &\leq 3|S| - 6. \end{aligned}$$

cqfd.

Corollaire 7.9. *Tout graphe planaire $G = (S, A)$ admet un sommet de degré ≤ 5.*

Démonstration. Soit $n = |S|$ et $m = |A|$. Pour $n = 1, 2$ la propriété est triviale. Supposons donc $n \geq 3$, et soit δ le degré minimum de G.

Alors, du Lemme des poignées de mains avec le résultat précédent.

$$n\delta \leq \sum_{s \in S} d(s) = 2m \leq 2(3n - 6) = 6n - 12.$$

Donc,

$$\delta \leq 6 - \frac{12}{n} < 6.$$

cqfd.

Corollaire 7.10 (Théorème des 6-couleurs)**.** *Tout graphe planaire est* 6*-coloriable.*

Démonstration. Par récurrence sur le nombre de sommets. Si $n = 1$ le résultat est trivial. Sinon, soit v un sommet de degré ≤ 5. On colorié par récurrence $G \setminus v$ avec 6 couleurs. Il en y a au plus 5 qui sont utilisés par des voisins de v. On peint v avec le sixième. **cqfd.**

Le Théorème des 5-couleurs, est un peu plus compliqué mais faisable. Par contre, le Théorème des 4-couleurs est un résultat très important, qui est resté ouvert pendant long temps. Quand en 1976 Appel et Haken l'ont démontré, une forte controverse c'est crée, car la preuve relie en un ordinateur qui vérifie plus de 1500 cas particuliers.

Théorème 7.11 (Théorème des 4-couleurs)**.** *Tout graphe planaire est* 4*-coloriable.*

Bibliographie

[Aigner, 2007] Aigner, M. (2007). *A course in enumeration*, volume 238 of *Graduate Texts in Mathematics*. Springer, Berlin.