Mathématique discrètes

Robin P.

2015-16, premier quadrimèstre

Contents

1 Théorie des graphes

1.1 Définitions

Intro Le problème des sept ponts de Königsberg est une des origines de la théorie des graphes : Au XVIIIe siècle, Leonhard Euler fut réquisitionné pour résoudre le problème suivant. *La ville de Königsberg est composée de sept ponts reliant quatre zones habitables d'une manière précise. Est-il possible de passer par tous les ponts et de revenir au point de départ en n'empruntant qu'une et une seule fois chaque pont ?* Euler a donc simplifié le problème en schématisant les zones habitables de manière ponctuelle et les ponts par des segments. C'est ainsi qu'il a trouvé que c'était impossible.

Def
- Une graphe Γ est un triplet (V, E, γ) où V est un ensemble fini dont les éléments sont appelés *sommets* du graphe, E est un ensemble fini dont les éléments sont appelés *arêtes* du graphe ; et γ est une fonction $\gamma : E \to \mathcal{P}aire(V)$ où $\mathcal{P}aire(V)$ est un ensemble non-ordonné. On note souvent $\Gamma = (V, E)$ en omettant volontairement l'expression de γ.
- Soient $\gamma(e) = \{x, y\}, e \in E, x, y \in V$. On dit que x et y sont *adjacents* et que e est *incident* à x et y.

Def
- Soit $\Gamma = (V, E)$, un graphe. $\gamma(e) = \{x, x\}, e \in E, x \in V$ est appelé un lacet.
- Si au moins deux arête sont incidentes à $x, y \in V$, on les appelle *arêtes multiples*.
- Un graphe est simple s'il n'a ni lacet ni arête multiple. Dans ce cas, on omet γ et on note $\Gamma = (V, E)$ avec $E \subseteq \mathcal{P}aire(V)$.

Def Soit $\Gamma = (V, E)$, un graphe. Le degré d'un sommet $v \in V$ est le nombre d'arêtes incidentes à v tel que les lacets comptent pour deux arêtes. Ce degré se note $\deg(v) \in \mathbb{N}\ \forall v \in V$.

Exemple Dans le cas du graphe d'une molécule de chimie organique comme un alcane par exemple, on a :

$$\deg(C) = 4, \deg(H) = 1.$$

Théorème Soit $\Gamma = (V, E)$, un graphe. Alors $\sum_{v \in V} \deg(v) = 2\#E$.

Corollaire La somme des degrés d'un graphe est pair.

Def Le graphe complet $\mathcal{K}_n$ est le graphe simple à n sommets pour lequel chaque sommet est adjacent à tous les autres. Autrement dit, $\forall x, y \in V, x \neq y, \exists e \in E$ tq $\gamma(e) = \{x, y\}$.

Def Un graphe $\Gamma' = (U, F)$ est un sous-graphe de $\Gamma = (V, E)$ si $U \subseteq V$ **et** $F \subseteq E$. On note alors $\Gamma' \leq \Gamma$. (Et pas $\Gamma' \subseteq \Gamma$!!)

1.2 Chemins dans les graphes

Def
- Soit $\Gamma = (V, E), v, w \in V$. Un chemin de v à w de longueur n est une séquence alternée de $(n + 1)$ sommets $(v_0, \ldots, v_n)$ et n arêtes $(e_1, \ldots, e_n)$ de la forme $(v = v_0, e_1, v_1, \ldots, e_{n-1}, v_{n-1}, e_n, v_n = w)$ tel que e_i est incident à v_{i-1} et $v_i\ \forall i \in \{1, \ldots, n\}$ et $e_i \neq e_j\ \forall i \neq j$.
- Un chemin ne possédant aucune répétition de sommet sauf peut-être $v_0 = v_n$ est dit *simple*.

Remarque Dans les graphes simples, on ne note que les sommets et pas les arêtes.

Def
- Un graphe $\Gamma = (V, E)$ est connexe si $\forall x, y \in V$, il existe un chemin de x à y.
- Soit $\Gamma = (V, E)$, un graphe et $x \in V$, la *composante connexe* de Γ contenant x est $\Gamma' \leq \Gamma$ dont les sommets et les arêtes sont ceux contenus dans un chemin de Γ démarrant en x.

Def Soit $\Gamma = (V, E)$ et $v \in V$. Un cycle est un chemin de v à v. Un cycle simple est un cycle de v à v dans lequel seul v est répété.

1.3 Arbres

Def Un arbre est un graphe simple, connexe qui ne contient aucun cycle. Les sommets de degré 1 sont appelés *feuilles*.

Prop Si T est un arbre avec $p \geq 2$ sommets, alors T contient au moins 2 feuilles.

Dém Soit T un arbre à p sommets, alors considérons un chemin $(v_0, \dots, v_k)$ de longueur maximale avec $v_i \in V \ \forall i 1 \leq i \leq r$. Alors v_0 et v_k sont de degré 1. Effectivement, si $\deg(v_0) \geq 2$, alors $\exists e \in E$ tq $\gamma(e) = \{x, v_0\}, x \neq v_1$. Par définition de T, il ne contient aucun cycle, donc $x \neq v_i \ \forall i \in \{2, \dots, k\}$ et $(x, v_0, \dots, v_k)$ est de longueur supérieure à $(v_0, \dots, v_k)$. Or $(v_0, \dots, v_k)$ est de longueur maximale. Pareil pour v_k.

Théorème Soit T, un graphe simple à p sommets. Les assertions suivantes sont équivalentes :

(i) T est un arbre ;

(ii) T a $p-1$ arêtes et aucun cycle ;

(iii) T a $p-1$ arêtes et est connexe.

Dém En montrant que $(i) \Rightarrow (ii)$, que $(ii) \Rightarrow (iii)$, et que $(iii) \Rightarrow (i)$, le théorème est démontré.

- Montrons que $(i) \Rightarrow (ii)$ en montrant qu'un arbre à p sommets a $p-1$ arêtes par récurrence.

  Pour $p = 1$, T a 0 arête.
  Pour $p \geq 2$, T a au moins 2 feuilles. Enlevons-en une et l'arête incidente à cette feuille. On obtient $T' \leq T$, un sous-arbre à $p-1$ sommets et $p-2$ arêtes en assumant que T en avait $p-1$.

- Montrons que $(ii) \Rightarrow (iii)$ en montrant qu'aucun cycle $\Rightarrow$ connexe.

  Supposons par l'absurdre que T n'est pas connexe. Soient T_i, les t composantes connexes de T tel que $t \geq 2$. Chaque T_i est un arbre (pas de cycle), donc chaque T_i a $p_i - 1$ arêtes pour p_i, le nombre de sommets de T_i. Par définition, $\sum_{i=1}^{t} p_i = p$, le nombre de sommets de T. Et $\sum_{i=1}^{t}(p_i - 1) = (p-1)$, le nombre d'arêtes de T. Or $\sum_{i=1}^{t}(p_i - 1) = \sum_{i=1}^{t} p_i - t = p - t$. Cela implique $t = 1$, or par construction, nous avions $t \geq 2$. Il y a contradiction. T est donc connexe.

- Montrons que $(iii) \Rightarrow (i)$ en montrant que si T a $p-1$ arêtes et est connexe, alors T est un arbre.

  Supposons par l'absurde que T n'est pas un arbre. Il existe donc un cycle car T est simple par hypothèse et connexe par construction. On considère le sous-graphe T' de T obtenu en retirant une arête du cycle. Si T' contient encore un cycle, réitérer le procédé. Si T' ne contient plus de cycle, T' est un arbre. Or T' a toujours p sommets (car aucun sommet de T n'a été retiré) et un nombre strictement inférieur à $p-1$ arêtes. Or dans $(i) \Rightarrow (ii)$, il a été montré qu'un arbre à p sommets $\Rightarrow (p-1)$ arêtes. Il y a donc contradiction et alors T est un arbre.

Exemple Les alcanes ($C_n H_{2(n+1)}$) sont des molécules représentables avec un graphe à $3n+2$ sommets dont n de degré 4 et $2n+2$ de degré 1. Donc, comme $\sum_{v \in V} \deg(v) = 2\#E$, $4n + 1(2n+2) = 6n + 2 = 2(3n+1)$, alors $\#E = 3n+1$, on a bien $\#V - \#E = 1$.

Def
- Deux graphes $\Gamma_1 = (V_1, E_1, \gamma_1)$ et $\Gamma_2 = (V_2, E_2, \gamma_2)$ sont *isomorphes* s'il existe une bijection $f : V_1 \to V_2$ et une bijection $g : E_1 \to E_2$ telles que $\forall e \in E, e$ est incident à $v, w \in V_1 \Leftrightarrow g(e) \in E_2$ est incident à $f(v), f(w) \in V_2$.
- Le couple (f, g) est appelé un *isomorphisme de graphe*, et on note $\Gamma_1 \sim \Gamma_2$.

Remarques
- lorsque Γ_1 et Γ_2 sont simples, $E_i \subseteq \mathcal{P}aire(V_i)$ avec $i \in \{1, 2\}$, alors la bijection g est induite par f, c'est à dire $e = \{v, w\} \in E_1 \Rightarrow g(e) := \{f(v), f(w)\} \in E_2$.
- Deux graphes isomorphes ont les mêmes propriétés.
- Le problème d'énumérer les alcanes non isomorphes fut résolu par Cayley.

1.4 Graphes hamiltoniens

Exemple En prenant l'exemple du dessin du dodécaèdre en perspective, on peut se demander s'il existe un moyen de parcourir l'entièreté des sommets en un seul cycle. C'est la question que s'est posée Hamilton.

Def
- Un cycle hamiltonien dans un graphe Γ est un cycle simple contenant tous les sommets de Γ.
- Les graphes ayant un cycle hamiltonien sont dits *graphes hamiltoniens*.

Def Un graphe $\Gamma = (V, E)$ est biparti si on peut écrire $V = B \cup W$ avec $B \cap W = \{\}$ (B et W sont des partitions) et si toute arête de Γ est incidente à $v \in B$ et à $w \in W$.

Remarque Un graphe complet avec $p \geq 2$ sommets n'est pas biparti.

Lemme Si Γ est biparti, tous ses cycles simples sont de longueur paire.

Dém Soit Γ, un graphe biparti. Par l'absurde, supposons qu'il existe un cycle simple $(v_0, e_1, \dots, v_{2n}, e_{2n}, v_{2n+1})$ de longueur impaire. Par définition, $v_i \in B$ $\forall i$ pair et $v_i \in W$ $\forall i$ impair (ou inversement). Or, par définition du cycle, on a $v_0 = v_{2n+1}$. Il y a donc contradiction, le cycle est alors de longueur paire.

Théorème Un graphe biparti avec un nombre impair de sommets n'est pas hamiltonien.

Dém Soit Γ, un graphe hamiltonien avec un nombre impair de sommets. Par définition, il contient un cycle simple passant par tous ses sommets, à savoir contenir un cycle de longueur impaire, ce qui est impossible par le lemme précédent.

Théorème (de Dirac) Soit $\Gamma = (V, E)$, un graphe simple avec $p \geq 3$ sommets et $\forall v \in V, \deg(v) \geq \frac{p}{2}$, alors Γ est hamiltonien.

Dém Montrons d'abord que Γ est connexe puis qu'il est cyclique. De là, il restera à prouver que ce cycle est hamiltonien.

- Montrons que Γ est connexe. Supposons donc par l'absurde qu'il ne le soit pas. Alors la plus petite de ses composantes connexes $\Gamma' \leq \Gamma$ a moins de $\frac{p}{2}$ sommets. Or, $\forall v \in V, \deg(v) \geq \frac{p}{2}$. Il y a contradiction donc Γ est connexe.
- Montrons maintenant que Γ est cyclique.

  Soit $C = (v_0, \dots, v_k)$, un plus long chemin simple dans Γ avec $v_0 \neq v_k$ et $k < p$. Par hypothèse, $\deg(v_0) \geq \frac{p}{2}$ et $\deg(v_k) \geq \frac{p}{2}$. Tous les sommets adjacents à v_0 sont dans $\{v_i \text{ tq } 1 \leq i \leq k\}$ et tous les sommets adjacents à v_k sont dans $\{v_i \text{ tq } 0 \leq i \leq k-1\}$. Comme $k < p$ (donc $\frac{k}{2} < \frac{p}{2}$), il doit exister $i \in \{0, \dots, k-1\}$ tq $\{v_i, v_k\}, \{v_{i+1}, v_0\} \in E$. Il existe donc un cycle $\overline{C} = (v_0, v_1, \dots v_i, v_k, v_{k-1}, \dots, v_{i+1}, v_0)$.
- Reste à prouver que $\overline{C}$ est hamiltonien.

  Supposons par l'absurde qu'il ne l'est pas. Il existe donc $y \notin \overline{C}$. Comme Γ est connexe, on peut supposer qu'$\exists \{v_j, y\} \in E$ avec $\in \{0, \dots, k\}$. On peut donc construire un chemin $\widetilde{C} = (y, v_j, \dots v_0, v_{i+1}, v_k, v_i, \dots, v_{j+1})$, or C était un plus long chemin. Donc $\nexists y$.

Illustration Un code de Gray d'ordre n est un arrangement cyclique de 2^n mots binaires de longueur n tel que deux mots adjacents ne diffèrent que d'un seul élément.

Un tel code peut être construit sur base d'un graphe hamiltonien. Pour construire un code de Gray d'ordre $(n+1)$ sur base d'un code de Gray d'ordre n, il faut écrire le code de Gray d'ordre n en le suffixant de 0 à chaque élément, puis le faire suivre du même code de Gray d'ordre n, à l'envers, suffixé de 1 à chaque élément.

1.5 Graphes eulériens

Def
- Un cycle eulérien dans un graphe Γ est un cycle simple contenant toutes les arêtes de Γ.
- Un graphe Γ est eulérien s'il contient un cycle eulérien.

Proposition Si un graphe est eulérien, alors tous ses sommets sont de degré pair.

Lemme Soit Γ un graphe $|\, \forall v \in V, \deg(v)$ est pair. Alors l'ensemble des arêtes se partitionne en une union (arête-)disjointe de cycles.

Dém Prouvons-le par récurrence sur q, le nombre d'arêtes.

- Le lemme est vrai pour $q = 2$.
- Supposons qu'il soit vrai pour $q \leq k$ et prouvons qu'il l'est pour $q = k + 1$.

  Soient $\Gamma = (V, E)$, un graphe de $k + 1$ arêtes et $v_0 \in V$. On démarre un chemin en v_0 et on ajoute des sommets jusqu'à répétition d'un des sommets. On le note v_j. Soit $\Gamma' = (V', E') \leq \Gamma = (V, E)$ dont $V' = V$ et $E' = E \setminus C$ avec C le chemin de v_j à v_k. Donc $\#E' \leq k$. Par hypothèse de récurrence, les arêtes de E' se partitionnent en une union arête-disjointe de cycles $C_1, \dots, C_n$. Comme $E' = E \setminus C$ ne contient aucune arête de C par définition, l'union $C, C_1, \dots, C_n$ est une partition arête-disjointe de E.

Théorème (d'Euler-Hierholzer) Soit Γ un graphe connexe. Γ est eulérien $\iff \forall v \in V, \deg(v)$ est pair.

Dém
- Par la proposition, Γ eulérien $\Rightarrow$ degrés pairs.
- Par le lemme, degrés pairs $\Rightarrow E$ se partitionne en une union arête-disjointe de cycles.

1.6 Application : le problème du voyageur de commerce (TSP) et arbres couvrants minimums (ACM)

Énoncé Un vendeur doit visiter un certain nombre de villes avant de rentrer chez lui (d'où il est parti). Comment doit-il choisir sa route afin de minimiser les distances ?

Objectif Déterminer un cycle hamiltonien de poids minimum dans $\Gamma = (V, E, \gamma, w)$ un graphe valué tel que V est l'ensemble des villes, E l'ensemble des routes, $w : E \to \mathbb{R}$ une fonction associant à chaque arête un poids réel.

Remarque Un graphe complet $\mathcal{K}_n$ a $\frac{1}{2}(n-1)!$ cycles hamiltoniens différents. On ne connait pas d'algorithme efficace pour résoudre ce problème.

Def Un arbre couvrant dans un graphe $\Gamma = (V, E)$ est un arbre $T = (V', E') \leq \Gamma$ tel que $V = V'$.

Algorithme de Kurska Il existe un algorithme (celui de Kurska) qui permet de trouver des arbres couvrants de poids minimum dans un graphe valué. La procédure est la suivante :

(i) Choisir une arête de plus petit poids pas encore dans V' de manière à ne pas créer de cycle ;

(ii) Réitérer tant que $\#V' \neq \#V$.

Comme dans un arbre, $\#E = \#V - 1$, cet algorithme s'exécute en $\#V - 1$ étapes. Il est donc en complexité $O(n)$ avec n le nombre de sommets.

Remarque Si C est un cycle hamiltonien dans Γ, alors $C \setminus \{e\}$ est un arbre couvrant. Une solution du TSP est toujours plus grande ou égale au poids d'un arbre couvrant minimum.

De plus, soient $\Gamma = (V, E)$ et $v \in V$. Tout cycle hamiltonien $C_H \leq \Gamma$ contient deux arêtes incidentes à v. Le reste du chemin est un autre arbre couvrant de $\Gamma \setminus \{v\}$. Une solution du TSP est donc toujours plus grande ou égale à la somme des poids des 2 arêtes incidentes à v + le poids d'un arbre couvrant de $\Gamma \setminus \{v\}$.

1.7 Relations et ordres partiels

Def Soit P un ensemble. Une ordre partiel sur P est une relation sur P (un ensemble de couples $(p_1, p_2) \in P^2$) notée $p_1 \leq p_2$ suivant les propriétés suivantes $\forall p, q, r \in P$:

- $p \leq p$ (réflexivité) ;
- $(p \leq q) \wedge (q \leq r) \Rightarrow (p \leq r)$ (transitivité) ;
- $(p \leq q) \wedge (q \leq p) \Rightarrow (p = q)$ (antisymétrie).

Remarque On note $(P, \leq)$ un ensemble partiellement ordonné.

Def $\mathcal{P}(E)$ est l'ensemble des parties de E, c'est-à-dire l'ensemble de tous les sous-ensembles de E.

Remarque Un ordre partiel $(P, \leq)$ peut se représenter à l'aide d'un graphe dirigé que l'on simplifie en enlevant les lacets (axiome de réflexivité) et en enlevant les arêtes que l'on peut obtenir par transitivité. De plus, par antisymétrie, il n'y a pas de cycle. Par convention, on enlève les flèches et le dessine de bas en haut.

Def Soit $(P, \leq)$, un ordre partiel. Son diagramme de Hasse est le graphe simple $\Gamma = (V, E)$ tel que :

- $e = \{x, y\} \in E \iff (x \leq y) \wedge (\nexists z \in V \text{ tq } x \leq z \leq y)$.
- $x \leq y \Rightarrow x$ plus bas que y dans sa représentation.

Def Soit $(P, \leq)$ un ordre partiel.

- Une chaine dans P est un sous-ensemble $C \subseteq P$ tel que $\forall c_1, c_2 \in C, (c_1 \leq c_2) \vee (c_2 \leq c_1)$.
- Une antichaine dans P est un sous-ensemble $A \subseteq P$ tel que $\forall a_1, a_2 \in A, \neg((a_1 \leq a_2) \vee (a_2 \leq a_1))$.

Théorème (de Dilworth) Soit $(P, \leq)$ un ensemble fini partiellement ordonné. Il existe une antichaine A et une partition de P par des chaines tel que $\#Q = \#A$ avec Q l'ensemble des partitions de P.

Dém Ce théorème se prouve par récurrence sur $\#P$:

- si $\#P = 0$, alors $\#Q = \#A = \#P = 0$ car $Q = A = P = \emptyset$.
- si $\#P > 0$, notons $a = \max P$. Pour un certain k naturel, $\exists C_1, \ldots, C_k$, une partition de $P \setminus \{a\}$ et A_0 une antichaine de $P \setminus \{a\}$ telle que $\#A_0 = k$ par hypothèse de récurrence.

  Prouvons qu'il y a toujours une antichaine dans P. $\forall 1 \leq i \leq k, \exists x_i$ le plus grand élément dans $A_0 \cap C_i$. L'ensemble $A = \{x_i \text{ tq } 1 \leq i \leq k\}$ est une antichaine car $\forall i \neq j, \exists y \in (A \cap C_j)$ tel que $y \leq x_j$ (par définition de x_j) et comme $y \not\leq x_j$, $x_j \leq x_i$ (transitivité).

  Prouvons maintenant qu'il y a une antichaine de même cardinal que Q :

  - Si a majore l'un des x_i, soit $K = \{a\} \cup \{z \in C_i \text{ tq } z \leq x_i\}$, alors $P \setminus K$ n'a pas d'antichaine de cardinal k, donc $P \setminus K$ peut être, par hypothèse de récurrence, partitionné en $k-1$ chaines et $A \setminus \{x_i\}$ est une antichaine de cardinal $\#A - 1 = k - 1$. P est donc partitionnable en k chaines (les $k-1$ de de $P \setminus K$ et K) et $\exists$ une antichaine A de cardinal k.
  - Sinon, $A \cup \{a\}$ est une antichaine de cardinal $k+1$ et P est partitionnable en $k+1$ chaines : $C_0 = \{a\}, C_1, \ldots, C_k$.

Remarque
- Soit $(P, \leq)$ un ordre partiel fini avec une partition Q de P et une antichaine $A \subseteq P$. Alors $\#A < \#Q$ car si $\#A > \#Q$, alors $\exists i, j, k$ tq $\exists C_i \ni \{a_j, a_k\}$. Ce qui veut dire que a_j et a_k sont comparables car dans une chaine, ce qui est impossible par définition de l'antichaine.
- Soit $(P, <)$, une ordre total. Pour toute antichaine $A \subseteq P, \#A \in \{0, 1\}$.

Def Soit $\Gamma = (V, E)$ une graphe simple.

- Un couplage M de Γ est un sous-ensemble d'arêtes de E deux à deux non adjacentes. Un sommet $v \in V$ incident à une arête $e \in M$ est dit couplé.
- Un transversal T de Γ est un sous-ensemble de sommets de T tel que $\forall e \in E, \exists v \in T$ tq e est incidente à v.

Def Soit $\Gamma = (V = B \sqcup W, E)$, un graphe biparti et M un couplage. Un chemin alterné dans Γ est un chemin qui démarre en un sommet de B non couplé et alterne une arête de $E \setminus M$ et une arête de M et ainsi de suite.

Théorème (de König) Soit $\Gamma = (V = B \sqcup W, E)$, un graphe biparti. La cardinalité maximale d'un couplage de Γ est égale à la cardinalité minimale d'un transversal de Γ.

Dém Soient $\Gamma = (V = B \sqcup W, E)$, un graphe biparti et M un couplage de cardinalité maximale dans Γ. $\forall m \in M$, choisissons un de ses sommets incidents comme suit :

- Le sommet $\in W$ s'il existe un chemin alterné arrivant à ce sommet,
- le sommet $\in B$ sinon.

Notons U l'ensemble des sommets obtenus. Montrons que U est un transversal de Γ (avec $\#U = \#M$). Si $\#U < \#M$, alors $\exists e \in M$ tq $\nexists v \in U | v \in \gamma(e)$.

Soit $e = \{b, w\} \in E$. Il faut montrer que soit $b \in U$, soit $w \in U$. On peut supposer $e \notin M$ car si $e \in M$, alors $(b \in U) \vee (w \in U)$ par définition. Comme M est maximal, $\exists e' = \{b', w'\} \in M$ tq $(b = b') \vee (w = w')$. On peut supposer $b = b'$ car sinon $w = w'$, donc $\{b, w\} = \{b, w'\}$ ou encore $\{b, w\}$ est un chemin alterné, ce qui implique que $w \in U$ par définition de U. Toujours par définition de U, si $b = b' \in U$, alors $w' \in U$. $\exists$ donc P, un chemin alterné dans Γ terminant en w'.

- Soit $P' := P \setminus \{\{w, b\}, \{w', b\}\}$. P' est un chemin alterné arrivant en w, donc $w \in U$ par définition de U.
- Soit $P' := P \cup \{w, b\} \cup \{w', b\}$. Alors il existe un couplage de cardinalité $\#M$, il y a donc contradiction.

Lemme Soient $(P, \leq)$, un ordre partiel, $\Gamma = (V = (B = P \times \{1\}) \sqcup (W = P \times \{2\}), E)$ un graphe biparti et T un transversal dans Γ. Le sous-ensemble $A \subseteq P$ défini comme suit : $A := \{p \in P \text{ tq } (p, 1), (p, 2) \notin T\}$ est une antichaine.

Dém Supposons, par l'absurde, que A n'est pas une antichaine (est une chaine). Alors $\exists a \neq b \in A$ tels que $a \leq b$ (par définition de la chaine dans Γ). $\exists$ donc $\{(a, 1), (b, 2)\} \in E$, donc $a \in T$ ou $b \in T$. De là, il faut déduire que soit a soit $b \notin A$, il y a contradiction, A est bien une antichaine.

Proposition Les théorèmes de Dilwoth et de König sont équivalents.

Dém Pour montrer que König $\iff$ Dilworth, montrons séparément les implications. Premièrement, montrons que König $\Rightarrow$ Dilworth, nous montrerons Dilworth $\Rightarrow$ König par la suite.

Soit $(P, \leq)$, un ordre partiel. Construisons un graphe biparti $\Gamma = (V = B \sqcup W, E)$ avec $B = P \times \{1\}$ et avec $W = P \times \{2\}$ tel que pour $p, q \in P, \{(p,1),(q,2)\} \in E \iff (p \leq q) \wedge (p \neq q)$.

Soient M et T, respectivement un couplage et un transversal de cardinalité maximale et minimale dans Γ. Le théorème de König dit que $\#M = \#T$. Définissons $A \subseteq P := \{p \in P \text{ tq } (p,1),(p,2) \notin T\}$, par le lemme précédent, nous savons que A est une antichaine. De là découle $\#A = \#\{p \in P \text{ tq } (p,1),(p,2) \notin T\} \leq \#P - \#T$.

Soit Q, un ensemble de n partitions de P : $Q = \{C_1, \ldots, C_n\}$.

- Soit $C_i = \{p_0, \ldots, p_l\}$ avec $l \geq 1$ si $\{(p_N, 1), (p_{N+1}, 2)\} \in E$ et $(p_l, 1), (p_l, 2)$ pas incidents à M.
- Soit $C_i = \{p\}$ si $(p,1),(p,2)$ ne sont pas incidents à M.

De là, Q est une partition de P. Nous pouvons exprimer $\#P = \sum_i \#C_i = \#M + \#Q$. Autrement dit, $\#Q = \#P - \#M = \#P - \#T \leq \#A$. Or, comme $\#A \leq \#Q$ par la remarque ci-dessus, alors $\#Q = \#A$.

Reste à prouver que Dilworth $\Rightarrow$ König.

Soit $\Gamma = (V = B \sqcup W, E)$, un graphe biparti. On définit un ordre partiel $(P, \leq)$ tel que $P = V$ et $\forall (b,w) \in B \times W, b \leq w \iff \exists e \in E \text{ tq } \{b,w\} = \gamma(e)$. Par le théorème de Dilworth, il existe A une antichaine et Q un ensemble de partition en antichaines de P tels que $\#A = \#Q$. Seules les arêtes $\{b,w\}$, les singletons $\{v\}$ peuvent être des chaines (en omettant les chaines triviales $\{\}$). Comme $\forall q \in Q, q$ est une partition de P, l'ensemble $M = E \cap Q$ est un couplage car $\forall v \in V, \exists! q \in Q \text{ tq } v \in q$. De plus, comme Γ est biparti, l'ensemble $T := \{b \in P \setminus A \text{ tq } a \in A, \{a,b\} \in E\} = P \setminus A$ est un transversal de Γ. Pour montrer König, il reste à prouver que $\#M = \#T$.

$(\forall v \in T, \exists e \in M \text{ tq } v \in \gamma(e)) \Rightarrow (\#M \geq \#T)$. De plus, $(\forall e = \{b,w\} \in M, \exists v \in T \text{ tq } (v = b) \vee (v = w)) \Rightarrow (\#T \geq \#M)$. Donc $\#T = \#M$.

2 Arithmétique modulaire

2.1 Les entiers et la division euclidienne

Rappel L'ensemble des entiers se note $\mathbb{Z}$ tel que $\mathbb{N} \subset \mathbb{Z}$. Plus précisément, $\mathbb{Z} = \mathbb{N}_0 \cup -\mathbb{N}_0 \cup \{0\}$. Cet ensemble est défini par deux opérations :

- l'addition interne $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : a, b \mapsto a + b$.

  Cette opération respecte les propriétés suivantes :

  (i) associativité ;

  (ii) existence du neutre ;

  (iii) existence de l'opposé ;

  (iv) commutativité.

  $(\mathbb{Z}, +)$ est donc un groupe commutatif.

- la multiplication interne $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : a, b \mapsto ab$.

  Cette opération respecte les propriétés suivantes :

  (i) associativité ;

  (ii) double distributivité (gauche et droite) sur l'addition ;

  (iii) commutativité ;

  (iv) inexistence de diviseur de zéro ;

  (v) existence du neutre.

$(\mathbb{Z}, +, \cdot)$ est donc un anneau ($(\mathbb{Z}, +)$ est un groupe et $\cdot$ respecte (i) et (ii)) unital (v) commutatif (iii) intègre (iv).

Axiome Il existe sur $\mathbb{Z}$ une relation d'ordre $\leq$ telle que :

(i) $\leq$ est un ordre total ;

(ii) $\forall a, b, c \in \mathbb{Z}, a \leq b \iff a + c \leq b + c$;

(iii) $\forall a, b, c \in \mathbb{Z}, (c \geq 0) \wedge (a \leq b) \Rightarrow ac \leq bc$.

Def On définit la valeur absolue d'un entier $a \in \mathbb{Z}$ telle que :

$$|a| = \begin{cases} a \text{ si } a \geq 0 \\ -a \text{ sinon} \end{cases}.$$

La valeur absolue est conçue telle que $\forall a, b \in \mathbb{Z}, (|a| = 0) \iff (a = 0), |ab| = |a||b|$.

Def Soient $a, b \in \mathbb{Z}$. a divise b $(a|b) \iff \exists c \in \mathbb{Z}$ tq $ac = b$.

Remarque La divisibilité est une relation car elle suit les propriétés de réflexivité, transitivité et d'antisymétrie.

Théorème (division euclidienne) Soient $a, b \in \mathbb{Z}$ tq $b \neq 0$. $\exists! q, r \in \mathbb{Z}$ tq $a = bq + r$ avec $0 \leq r < b$.

Def Un nombre $p \in \mathbb{N}$ est premier $\iff (p \notin \{0, 1\}) \wedge (\nexists q \in \mathbb{N} \setminus \{1, p\}$ tq $q|p)$.

Def Un entier d est un GCD de a et $b \iff (d|a) \wedge (d|b) \wedge (c \in \mathbb{Z}, (c|a) \wedge (c|b) \Rightarrow c|d)$. On le note $d = GCD(a, b)$. De plus, $\forall a \in \mathbb{Z}, GCD(a, 0) := |a|$.

2.1.1 L'algorithme d'Euclide

Proposition Soient $a, b \in \mathbb{Z}, b \neq 0, q, r \in \mathbb{Z}$ tq $a = bq + r$. Alors $GCD(a, b) = GCD(b, r)$.

Dém Soient $a, b, q, r \in \mathbb{Z}$ tq $a = bq + r$ et $c \in \mathbb{Z}$. Comme $a = bq + r$, si $(c|b) \wedge (c|r)$, alors $c|a$. Et comme $r = a - bq$, si $(c|a) \wedge (c|b)$, alors $c|r$.

Algorithme Soient $a, b \in \mathbb{Z}, b \neq 0$. Pour déterminer $GCD(a, b)$, on suppose $a, b \geq 0$ car $GCD(a, b) = GCD(-a, b) = GCD(a, -b) = GCD(-a, -b)$. Par le théorème de la division euclidienne, $\exists! q_1, r_1 \in \mathbb{Z}$ tq $a = bq_1 + r_1$ avec $0 \leq r_1 < |b|$. Si $r_1 = 0$, alors $GCD(a, b) = GCD(b, 0) = |b|$. Sinon, on itère en prenant b et r_1. Par la DE[1], $\exists! q_2, r_2$ tq $b = r_1 q_2 + r_2$ avec $0 \leq r_2 < r_1$. Si $r_2 = 0$, alors $GCD(b, r_1) = GCD(r_1, 0) = r_1$. Sinon, on réitère sur la formule $r_i = r_{i+1} q_{i+2} + r_{i+2}$ avec $a, b = r_{-1}, r_0$. $\exists$ donc N tq $r_N = 0$. On a donc $GCD(a, b) = GCD(b, r_1) = GCD(r_i, r_{i+1}) = GCD(r_{N-1}, r_N) = r_{N-1}$.

Proposition Soient $a, b \in \mathbb{Z}, b \neq 0$. $\exists! s, t \in \mathbb{Z}$ tq $GCD(a, b) = sa + tb$.

Dém Soient $a, b \in \mathbb{Z}$. Supposons $a, b \geq 0$. Soient $r_i, 1 \leq i \leq n$, les restes successifs de la DE de l'algorithme d'Euclide avec $r_i = r_{i+1} q_{i+2} + r_{i+2}$, $0 \leq r_i < r_{i+1}$.

On construit s et t comme suit :

$$\begin{aligned} GCD(a, b) = r_n &= r_{n-2} - q_n r_{n-1} \\ &= s_1 t_{n-2} + t_1 r_{n-1} \quad \text{où } s_1 = 1, t_1 = -q_n \\ &= s_1 r_{n-2} + t_1 (r_{n-3} - q_{n-1} r_{n-2}) \\ &= s_2 r_{n-3} + t_2 r_{n-2} \quad \text{où } s_2 = t_1, t_2 = (s_1 - t_1 q_{n-1}) \\ &= \ldots \end{aligned}$$

On construit, inductivement, $s_k = t_{k-1}, t_k = (s_{k-1} - t_{k-1} q_{n-(k-1)})$ tq $GCD(a, b) = s_k r_{n-(k+1)} + t_k r_{n-k}$.

De là, $s_n r_{n-1} + t_n r_0 = s_n a + t_n b$.

[1] Division euclidienne.

2.1.2 Décomposition en nombres premiers

Def Deux entiers $a, b \in \mathbb{Z}_0$ sont premiers entre eux $\iff GCD(a,b) = 1$.

Proposition (lemme de Bézout) Soient $a, b \in \mathbb{Z}$. a et b sont premiers entre eux $\iff \exists s, t \in \mathbb{Z}$ tq $sa + tb = 1$.

Lemme (de Gauss) Soient $a, b \in \mathbb{Z}$ tq a et b sont premiers entre eux, $c \in \mathbb{Z}$ tq $b|ac$. Alors $b|c$.

Dém Soient a, b deux entiers premiers entre eux. Donc $GCD(a,b) = 1$, ou encore $\exists! s, t \in \mathbb{Z}$ tq $1 = sa + tb$. De là, $c = sac + tbc$. Or, on sait que $b|ac$ et $b|b$, donc $b|sac + tbc = c$.

Corollaire Soient $a, b, p \in \mathbb{Z}$ tq p est premier. Si $p|ab$, alors $(p|a) \vee (p|b)$.

Dém Soient $a, b, p \in \mathbb{Z}$ tq p est premier. Si $p|a$, le corollaire est bon. Sinon, si $p \not| a$, comme p est premier, a et p sont premiers entre eux. Donc par le lemme de Gauss, $p|b$.

Théorème (décomposition en facteurs premiers) $\forall z \in \mathbb{Z}, \exists n \in \mathbb{N}, p_1 \dots p_n$, n nombres premiers différents deux à deux et $e_1 \dots e_n \in \mathbb{N}_0$ tq $z = (\pm 1) \prod_{i=1}^{n} p_i^{e_i}$. Cette expression est unique (à l'ordre d'expression des i^e termes).

2.2 Groupes, anneaux et entiers $\mod n$

2.2.1 Définitions

Def Un groupe $(G, *)$ est un ensemble non vide G muni d'une loi de composition $* : G \times G \to G : g, h \mapsto g * h$ tq

(i) $*$ est associative ;

(ii) $\exists$ un neutre $e \in G$ tq $\forall g \in G, g * e = e * g = g$;

(iii) $\forall g \in G, \exists$ un inverse $g^{-1} \in G$ tq $g^{-1} * g = g * g^{-1} = e$.

Def Soient $(G, *)$ un groupe et un sous-ensemble $H \subseteq G$. Si $(H, *)$ est un groupe, on note $H \leq G$ ou $(H, *) \leq (G, *)$ le sous-groupe H.

Proposition Soient $(G, *)$ un groupe et $H \subseteq G$. $H \leq G \iff$:

(1) $e \in H$;

(2) $\forall g, h \in G, g * h^{-1} \in H$.

Dém Pour montrer la double implication il faut montrer les implications séparément. Montrons d'abord que $H \leq G \Rightarrow (1) \wedge (2)$. Ensuite, montrons que $(1) \wedge (2) \Rightarrow H \leq G$.

Montrons d'abord la première implication. Comme $H \leq G$, H est un groupe, donc (1) et (2) sont vérifiés naturellement. Montrons ensuite la seconde implication. La propriété des groupes (i) se montre par (2) car $\forall g, h \in H, g * (h^{-1})^{-1} \in H$ (il faut que h^{-1} soit dans H, ce qui est prouvé dans (iii)). La propriété (ii) se montre par la proposition (1). La propriété (iii) se montre comme suit : soit $g = e \in H$. $\forall h \in H, e * h^{-1} = h^{-1} \in H$ par la proposition (2).

Def Soit $(G, *)$ un groupe. Si la loi de composition $*$ est commutative, G est un groupe abélien (commutatif) et est noté $(G, +)$[2].

Proposition Soit $S \subseteq \mathbb{Z}$ tq $\#S > 0, (S, +) \leq (Z, +)$. $\exists k \in \mathbb{Z}$ tq $S = k\,\mathbb{Z}$.

Dém
- Si $S = \{0\}$, alors $S = 0\,\mathbb{Z}$.
- Si $\#S > 1$, on prend $k = \min\{s \in S \text{ tq } s > 0\}$ (le plus petit entier positif $\in S$). Reste à prouver que $S = k\,\mathbb{Z}$. Supposons par l'absurde qu'$\exists s \in S$ tq $s \notin k\,\mathbb{Z}$. Par la division euclidienne, $\exists! q, r \in Z$ tq $s = kq + r$ avec $0 \leq r < k$. Si $r \neq 0$, sinon $s \in k\,\mathbb{Z}$. $r = kq - s \in S$ car $(s \in S) \wedge (k \in S \Rightarrow kq \in S)$. Or $0 < r < k$ alors que k est le plus petit entier positif de S. Donc il y a contradiction.

Proposition Soient $k, l \in \mathbb{Z}$. On définit $k\,\mathbb{Z} + l\,\mathbb{Z} := \{kz_1 + lz_2 \text{ tq } z_1, z_2 \in \mathbb{Z}\}$. $k\,\mathbb{Z} + l\,\mathbb{Z} = GCD(k,l)\,\mathbb{Z}$.

[2] Le symbole $+$ précise que la composition est commutative.

Dém
- Montrons que $GCD(k,l)\,\mathbb{Z} \subseteq k\,\mathbb{Z} + l\,\mathbb{Z}$.
  Par la proposition d'Euclide $\exists s,t \in \mathbb{Z}$ tq $sk+tl = GCD(k,l)$. Donc $\forall z \in \mathbb{Z}, GCD(k,l)z \in GCD(k,l)\,\mathbb{Z} = (sk+tl)z = k(sz) + l(tz) \in k\,\mathbb{Z} + l\,\mathbb{Z}$.
- Montrons ensuite que $k\,\mathbb{Z} + l\,\mathbb{Z} \subseteq GCD(k,l)\,\mathbb{Z}$.
  Par définition, $\forall z_1, z_2 \in \mathbb{Z}, \exists y_1, y_2$ tq $GCD(k,l)y_1 = z_1$ et $GCD(k,l)y_2 = z_2$. $\forall z_1, z_2 \in \mathbb{Z}, kz_1 + lz_2 \in k\,\mathbb{Z} + l\,\mathbb{Z} = GCD(k,l)(y_1 k + l y_2) \in GCD(k,l)\,\mathbb{Z}$.

2.2.2 Groupes quotients

Remarque Ici, $(G,+)$ représente un groupe abélien, l'inverse de $g \in G$ n'est donc plus noté g^{-1} mais $-g$ par convention.

Def Une classe latérale d'un sous-groupe $H \leq G$ est un ensemble $g + H := \{g + h \text{ tq } h \in H\}$ pour $g \in G$ fixé.

Proposition Soient $(G,+)$ un groupe abélien, H un sous-groupe tq $H \leq G$ et $g, g' \in G$. $g + H = g' + H \iff \forall h \in H, \exists! h' \in H$ tq $g + h = g' + h'$.

Dém Pour montrer ceci, il faut montrer les implications séparément. Commençons par montrer l'implication $\Rightarrow$. $\forall h \in H, g + h \in g + H = g' + H \Rightarrow g' + h' = g + h$ avec $h' \in H$. Reste à prouver que h' est unique. Supposons donc $h', \widetilde{h} \in H$ tq $g' + h' = g' + \widetilde{h}$. En réorganisant, on obtient $e + h' = e + \widetilde{h}$ ou encore $h' = \widetilde{h}$.

Montrons maintenant l'implication $\Leftarrow$. Comme $\forall f = g + h \in g + H, \exists! f' = g' + h' \in g' + H$ tq $f = f'$, alors $g + H \subseteq g' + H$. De plus, comme $\forall h, h'$ est unique et que h et h' viennent du même ensemble, $\#(g + H) = \#(g' + H)$. Donc $g + H = g' + H$.

Def On note G/H l'ensemble des classes latérales de H avec $H \leq G$. $G/H := \{g + H \text{ tq } g \in G\}$. S'il n'y a pas d'ambigüité sur le sous-groupe, on note $\overline{g} := g + H$.

Exemple Soient $(\mathbb{Z},+)$, un graphe abélien et $7 \in \mathbb{Z}$. $\mathbb{Z}/7\,\mathbb{Z} := \{7\,\mathbb{Z}, 1 + 7\,\mathbb{Z}, \ldots, 6 + 7\,\mathbb{Z}\} := \{\overline{0}, \overline{1}, \ldots, \overline{6}\}$.

Proposition Soient $(\mathbb{Z},+)$ et $k \in \mathbb{Z}$. $\mathbb{Z}/k\,\mathbb{Z}$ est une partition de $\mathbb{Z}$.

Dém Par définition, $\mathbb{Z}/k\,\mathbb{Z}$ est une partition de $\mathbb{Z} \iff (\forall i,j \in \{0,\ldots,k-1\}, c_i \cap c_j \neq \emptyset \iff i = j) \wedge (\bigcup_{c \in \mathbb{Z}/k\,\mathbb{Z}} c = \mathbb{Z})$. Pour montrer l'union totale, montrons que $\forall r_1, r_2 \in \mathbb{Z}, (r_1 + k\,\mathbb{Z}) \cap (r_2 + k\,\mathbb{Z}) \neq 0 \iff r_1 = r_2 + kz'$ avec $z' \in \mathbb{Z}$. Soit $z \in (r_1 + k\,\mathbb{Z}) \cap (r_2 + k\,\mathbb{Z})$. Alors $\exists q_1, q_2 \in \mathbb{Z}$, par la DE, tq $r_1 + kq_1 = z = r_2 + kq_2$. Donc $r_1 = r_2 + k(q_2 - q_1)$. Pour démontrer l'intersection vide, également par la DE, $\forall z \in \mathbb{Z}\, \exists q, r \in \mathbb{Z}$ tq $z = kq + r \in r \in k\,\mathbb{Z}$.

Théorème Soient $(G,+)$ un groupe abélien et $H \leq G$. Alors G/H est muni d'une loi $\overline{+}$ tq $(G/H, \overline{+})$ est un groupe abélien. Précisément, on définit $\forall g, g' \in G, \overline{g} \overline{+} \overline{g'} := \overline{g + g'}$.

Remarque Une opération d'addition a été définie sur base d'une autre opération. Il faut cependant vérifier si elle est *bien définie*[3], à savoir que si $\overline{\widetilde{g}} = \overline{g}$ et $\overline{\widetilde{g}'} = \overline{g'}$, alors il faut que $\overline{\widetilde{g}} \overline{+} \overline{\widetilde{g}'} = \overline{g} \overline{+} \overline{g'}$.

Dém Soient $\widetilde{g}, g, \widetilde{g}', g' \in G$ tels que $\overline{g} = \overline{\widetilde{g}}, \overline{g'} = \overline{\widetilde{g}'}$. Comme $\overline{g} = \overline{\widetilde{g}}$, on a $g - \widetilde{g} = h \in H$ et comme $\overline{\widetilde{g}'} = \overline{g'}$, on a $\widetilde{g}' - g = h' \in H$. De plus, $\overline{\widetilde{g}} \overline{+} \overline{\widetilde{g}'} := \overline{\widetilde{g} + \widetilde{g}'} = \overline{(g - h) + (g' - h')} = \overline{(g + g') - (h + h')} = \overline{g + g'} = \overline{g} \overline{+} \overline{g'}$.

Maintenant que nous savons que l'addition est bien définie, il faut prouver qu'elle confère à G/H une structure de sous-groupe commutatif :

(1) $e \in G$, alors $\overline{e}$ est le neutre pour G/H.

(2) Soit $g \in G$. $-g = -(g + H) := (-g) + H = \overline{-g}$.

(3) $\overline{+}$ est commutatif car cet opérateur est défini selon l'opérateur $+$ de G qui, lui, est commutatif.

Def Pour $n \in \mathbb{N}_0$, $n\,\mathbb{Z} \leq \mathbb{Z}$, on définit le groupe des entiers modulo n comme le groupe quotient $(\mathbb{Z}/n\,\mathbb{Z}, \overline{+})$ où $\overline{a} \overline{+} \overline{b} = \overline{a + b}$.

2.2.3 Isomorphismes de groupes

Def Soient $(G,*), (G',*')$, deux groupes. Un morphisme de groupes est une application $f : G \to G'$ telle que $\forall g, h \in G, f(g * h) = f(g) *' f(h)$.

[3] Le terme *bien défini* veut dire *défini sans ambiguïté* sur une autre opération, à savoir, si on définit $*'$ sur un ensemble E' sur base de $*$ défini sur un ensemble E, alors il faut que $a * b = a' * b' \Rightarrow f(a) *' f(b) = f(a') * f(b')$ où f est une application définie par $f : E \to E'$.

Def Un morphisme de groupes $f : G \to G'$ est dit :

- injectif si $\forall g, h \in G, f(g) = f(h) \Rightarrow g = h$;
- surjectif si $\forall g' \in G', \exists g \in G$ tq $f(g) = g'$;
- bijectif s'il est injectif et surjectif.

Def Soient $(G, *), (G, *')$ deux groupes et $f : G \to G'$ un morphisme de groupes.

$$\mathrm{Im}(f) := \{f(g) \text{ tq } g \in G\} = f(G) \subseteq G',$$
$$\mathrm{Ker}(f) := \{g \in G \text{ tq } f(g) = e' \in G'\} = f^{-1}(e') \subseteq G.$$

Proposition $\mathrm{Ker}(f)$ est un sous-groupe de G et $\mathrm{Im}(f)$ est un sous-groupe de G'.

Lemme Soit $(G, *)$ un groupe. Si $x \in G = x * x$, alors $x = e$ où e est le neutre de G.

Dém Soient $(G, *), x \in G$ tq $x = x * x$. Par définition de G, $\exists x^{-1} \in G$ tq $x * x^{-1} = e$. En ajoutant x^{-1} de part et d'autre de l'équation, on obtient $x * x^{-1} = x * x * x^{-1} \iff e = x * e = x$.

Lemme Soient $(G, *), (G', *')$ et $f : G \to G'$ un morphisme de groupes. $\forall x \in G, f(x)^{-1} = f(x^{-1})$.

Dém Soient $f : G \to G'$ un morphisme de groupes. $e' \in G' = f(e) = f(x^{-1} * x) = f(x^{-1}) *' f(x) \iff f(x)^{-1} = f(x^{-1})$.

Proposition Soient $(G, *), (G', *')$, deux groupes et $f : G \to G'$, un morphisme de groupes. Alors :

- f est injective $\iff \mathrm{Ker}(f) = \{e\}$
- f est surjective $\iff \mathrm{Im}(f) = G'$

Dém Montrons d'abord la première équivalence (l'injectivité).

- Prouvons d'abord f injective $\Rightarrow \mathrm{Ker}(f) = \{e\}$. Pour ce faire, montrons que $e \in \mathrm{Ker}(f)$ puis montrons qu' $\nexists x \neq e \in \mathrm{Ker}(f)$.
  - $f(e) = f(e * e) = f(e) *' f(e)$. Or, par le lemme ci-dessus, $f(e) = e' \in G'$, donc $e \in \mathrm{Ker}(f)$.
  - Par définition d'une fonction injective, $\forall g, h \in G, f(g) = f(h) \Rightarrow g = h$. Donc $\forall g \in G$ tq $f(g) = f(e) \Rightarrow g = e$. e est donc le seul élément de $\mathrm{Ker}(f)$.
- Prouvons ensuite $\mathrm{Ker}(f) = \{e\} \Rightarrow f$ injective. Soient $g_1, g_2 \in G$. $f(g_1) = f(g_2) \Leftrightarrow f(g_1) *' (f(g_2))^{-1} = f(g_2) *' (f(g_2))^{-1} = e'$. Comme par le lemme précédent, $f(x)^{-1} = f(x^{-1})$, alors $f(g_1 * g_2^{-1}) = e'$. Donc $g_1 * g_2^{-1} \in \mathrm{Ker}(f)$. Cependant, par hypothèse, on peut dire que si $x \in \mathrm{Ker}(f)$, alors $x = e$. Donc $g_1 * g_2^{-1} = e$, ou encore $g_1 = g_2$.

Il faut encore maintenant montrer la seconde équivalence (la surjectivité).

Cette preuve est cependant immédiate : $\mathrm{Im}(f) = G' \iff \{f(g) \text{ tq } g \in G\} = G' \iff \forall g' \in G', \exists g \in G \text{ tq } f(g) = g' \iff f$ est surjective.

Def Soient $(G, *), (G', *')$ deux groupes.

- Un isomorphisme de groupe est un morphisme bijectif $f : G \to G'$.
- $(G, *)$ et $(G', *')$ sont dits isomorphes s'$\exists f : G \to G'$ un isomorphisme. On note $G \sim G'$.

Exemple $\exp : \mathbb{R} \to \mathbb{R}_0^+$ est un isomorphisme entre $(\mathbb{R}, +)$ et $(\mathbb{R}_0^+, \cdot)$

2.2.4 Les anneaux

Def Un anneau $(A, +, \cdot)$ est un ensemble A non vide muni d'une opération de deux opérations ($+ : A \times A \to A$ et $\cdot : A \times A \to A$) respectant les propriétés suivantes :

- $(A, +)$ est un groupe commutatif ;
- $\cdot$ est une opération associative ;
- $\cdot$ est une opération distributive sur $+$.

Def
- $(A, +, \cdot)$ est un anneau commutatif si l'opération multiplicative $\cdot$ est associative ;
- $(A, +, \cdot)$ est un anneau unital s'$\exists 1 \in A$ tq $\forall a \in A, 1 \cdot a = a = a \cdot 1$.

Exemples
- Mq $0 \cdot a = 0$.Par définition, $0 = 0 + 0$. Donc $\forall a \in A, 0 \cdot a = (0 + 0) \cdot a \iff 0a = 0a + 0a$. Par le lemme précédent, $x = x + x \Rightarrow x = e$ où e est le neutre. Ici, le neutre est 0. Donc $\forall a \in A, 0a = 0$.
- Mq dans un anneau unital $(A, +, \cdot)$, $\forall a \in A, (-1) \cdot a = -a$. Comme vu plus haut, $\forall a \in A, 0a = 0$. Donc $\forall a \in A, (1 + (-1)) \cdot a = 0 \iff 1 \cdot a + (-1) \cdot a = 0 \iff (-1) \cdot a = -a$.

Proposition Soit $k \in \mathbb{Z}_0 \setminus \{1\}$. $(\mathbb{Z}/k\mathbb{Z}, \overline{+}, \overline{\cdot})$ où $\overline{\cdot}$ est défini par $\overline{\cdot} : \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ tq $\overline{l} \overline{\cdot} \overline{l'} := \overline{l \cdot l'}$ est un anneau commutatif.

Dém À nouveau, il faut montrer que $\overline{\cdot}$ est bien défini. Soient $l, l', \widetilde{l}, \widetilde{l'} \in \mathbb{Z}$ tq $\overline{l} = \overline{\widetilde{l}}, \overline{l'} = \overline{\widetilde{l'}}$. Alors, $l - \widetilde{l} = kz_1 \in k\mathbb{Z}$ et $l' - \widetilde{l'} = kz_2 \in k\mathbb{Z}$ avec $z_1, z_2 \in \mathbb{Z}$. Donc, par définition :

$$\begin{aligned}\overline{\widetilde{l}} \overline{\cdot} \overline{\widetilde{l'}} := \overline{\widetilde{l} \cdot \widetilde{l'}} = \overline{(l - kz_1) \cdot (l' - kz_2)} &= \overline{l \cdot l' - k \cdot (z_1 \cdot l' + z_2 \cdot l) + k \cdot k \cdot z_1 \cdot z_2} \\ &= \overline{(l \cdot l') + k \cdot ((k \cdot z_1 \cdot z_2 - z_1 \cdot l - z_2 \cdot l') \in \mathbb{Z})} = \overline{l \cdot l'}.\end{aligned}$$

Les propriétés de commutativité découlent directement des propriétés des entiers $\in \mathbb{Z}$.

2.3 Interprétation des GCD, nombres premiers, nombres premiers entre eux

Def Soit $(A, +, \cdot)$, un anneau unital.

- $a \in A$ est inversible s'$\exists b \in A$ tq $a \cdot b = 1 = b \cdot a$;
- $a \in A \neq 0$ est un diviseur de 0 s'$\exists b \in A \neq 0$ tq $a \cdot b = 0$.

Exemple Soient $0 < a \leq b < k \in \mathbb{N}_0$ tq $a \cdot b = k$. Alors $\overline{a}$ et $\overline{b}$ sont des diviseurs de 0 dans $\mathbb{Z}/k\mathbb{Z}$.

Proposition Si $a \in A$ est un diviseur de 0, alors a n'est pas inversible.

Dém Soit $a \in A$. Par définition de a, $\exists b \in A \neq 0$ tq $a \cdot b = 0$. Supposons, par l'absurde, a inversible. Donc $\exists c \in A$ tq $ac = 1 = ca$. De là, $b(ac) = b \iff (ba)c = b \iff 0c = b \iff b = 0$. Or b doit être non nul, il y a contradiction. a n'est pas inversible.

Proposition Soient $k \in \mathbb{N}_0 \setminus \{1\}$, $k \in \mathbb{Z}$. $\overline{z}$ est inversible dans $\mathbb{Z}/k\mathbb{Z} \iff GCD(k, z) = 1$.

Dém Montrons que si k et z sont premiers entre eux, alors $\overline{z}$ est inversible.

$\overline{t} \overline{\cdot} \overline{z} = \overline{tz} = \overline{1 - sk} \in \mathbb{Z}/k\mathbb{Z} = \overline{1}$ car sk est un multiple de k, avec $t, s \in \mathbb{Z}$ tq $sk + tl = 1$ (par Euclide). On a donc $\overline{t}$, l'inverse de $\overline{z}$.

Montrons ensuite que si $\overline{z}$ est inversible, alors k et z sont premiers entre eux.

$\overline{z}$ est inversible $\Rightarrow \exists t \in \mathbb{Z}$ tq $\overline{t} \overline{\cdot} \overline{z} = \overline{1} = \overline{tl}$. Donc $\exists t, s \in \mathbb{Z}$ tq $tl - 1 = sk$ avec $s \in \mathbb{Z}$. Ou encore $tl + (-s)k = 1$. Par le lemme de Bézout, k et z sont premiers entre eux.

Remarque Nous avons vu l'algorithme qui permet de déterminer $s, t \in \mathbb{Z}$ tq $sk + tl = GCD(k, l)$. Si $GCD(k, l) = 1$, alors $\overline{t}$ est l'inverse de $\overline{z}$ dans $\mathbb{Z}/k\mathbb{Z}$.

Def $(\mathbb{K}, +, \cdot)$ est un champ si $(\mathbb{K}, +, \cdot)$ est un anneau unital commutatif tel que $\forall k \neq 0 \in \mathbb{K}, \exists k^{-1}$ tq $kk^{-1} = 1$.

Exemple $\mathbb{Z}/4\mathbb{Z}$ possède des diviseurs de 0 donc ce n'est pas un champ.

Proposition Soit $k \in \mathbb{N} \setminus \{1\}$. Alors $\mathbb{Z}/k\mathbb{Z}$ est un champ $\iff k$ est un nombre premier.

Dém Corollaire de la proposition précédente.

Remarque $\forall p \in \mathbb{Z}$ tq p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un champ à p éléments.

2.3.1 Relations de congruence

Def Soient $a, b, k \in \mathbb{Z}$ tq $|k| > 1$. On dit que a est *congru à b modulo k* et on note $a \equiv b \pmod{k} \iff a - b \in k\mathbb{Z} \iff \overline{a} = \overline{b}$ dans $\mathbb{Z}/k\mathbb{Z}$.

Propriétés

1. La congruence modulo k est une relation d'équivalence (réflexive, transitive et symétrique) ;
2. $\forall a_1, b_1, a_2, b_2 \in \mathbb{Z}, |k| > 1$, si $a_1 \equiv a_2 \pmod k$ et $b_1 \equiv b_2 \pmod k$, alors :
   - $a_1 + b_1 \equiv a_2 + b_2 \pmod k$;
   - $a_1 b_1 \equiv a_2 b_2 \pmod k$.

   En conséquence, $\forall c \in \mathbb{Z}, a_1 c \equiv a_2 c \pmod k$.

2.4 La cryptologie : le système RSA (Rivest, Shamir, Adlerman)

Lemme $\forall n \in \mathbb{N}, (n+1)^p \equiv n^p + 1 \pmod p$ si p est premier.

Dém Par le binôme de Newton,$(n+1)^p = \sum_{i=0}^{p} n^i \binom{p}{i} = n^p + 1 + \sum_{i=1}^{p-1} n^i \binom{p}{i}$.

Montrons maintenant par récurrence sur i que $p \mid \binom{p}{i} \forall 0 < i < p$.

Quand $i = 1$, $\binom{p}{i} = p$, or $p \mid p$, donc ok.

Supposons maintenant que $p \mid \binom{p}{i}$ et démontrons que donc $p \mid \binom{p}{i+1}$. $\binom{p}{i} = \frac{p!}{i!(p-i)!} \Rightarrow \binom{p}{i+1} = \frac{p!}{(i+1)!(p-i-1)!} = \frac{p!(p-i)}{i!(i+1)(p-i-1)!(p-i)} = \binom{p}{i}\frac{p-i}{i+1}$. Or $p \mid \binom{p}{i}$, donc $\exists \in \mathbb{N}$ tq $\binom{p}{i} = pb$. De là, on a $\binom{p}{i+1} = pb\frac{p-i}{i+1}$. Et $\binom{p}{i+1} \in \mathbb{N}$ par définition. Donc comme p est premier et $i < p$, on sait $(i+1) \not| p$ et donc qu'il faut que $(i+1) \mid b(p-i)$. Donc $\exists t \in \mathbb{N}$ tq $b(p-i) = t(i+1)$, ou encore $\binom{p}{i+1} = pt$. Et comme $p \mid pt$, on sait que $p \mid \binom{p}{i+1}$.

Comme $p \mid \binom{p}{i+1} \Leftrightarrow \binom{p}{i+1} \equiv 0 \pmod p$. Donc $n^p + 1 + \sum_{i=1}^{p-1} \binom{p}{i} n^i \equiv n^p + 1 \pmod p$.

Théorème (Petit théorème de Fermat) Soit $p \in \mathbb{N}$ un nombre premier. Et soit $a \in \mathbb{N}$ tq $p \not| a$. Alors $a^p \equiv 1 \pmod p$.

Dém Montrons par récurrence sur a que $a^p \equiv a \pmod p$.

Pour $a = 1$, on a $a^p = 1^p \equiv 1 \pmod p$, donc ok.

Supposons maintenant que $a^p \equiv a \pmod p$ et montrons que $(a+1)^p \equiv a + 1 \pmod p$. Par le lemme précédent, nous avons $(a+1)^p \equiv a^p + 1 \pmod p$. Et par hypothèse de récurrence, nous avons $a^p \equiv a \pmod p$. Donc, en combinant les deux, nous obtenons $(a+1)^p \equiv (a+1) \pmod p$.

Cela veut dire que dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a^p} = \overline{a}$. Mais comme $p \not| a$ et que $\mathbb{Z}/p\mathbb{Z}$ set un champ, $\exists \overline{b}$, un inverse de $\overline{a}$. Donc en multipliant par $\overline{b}$ de part et d'autre, on obtient $\overline{ba^p} = \overline{b}\overline{a}^p = \overline{ba}a^{p-1} = \overline{a}^{p-1} = \overline{ba} = \overline{1}$. Autrement dit, $a^{p-1} \equiv 1 \pmod p$.

Fonctionnement de RSA deux personnes Alice et Bob veulent communiquer de manière sûre. Alice choisit deux nombres premiers $p, q \in \mathbb{N}$. Ce couple est appelé la *clef privée*. Ensuite Alice calcule $N := pq$ et $\phi(N) := (p-1)(q-1) = N - (p+q+1)$. Alice choisit également $e \in \mathbb{Z}$ tq $GCD(\phi(N), e) = 1$. e est appelé *l'exposant de chiffrement*. Par le choix de e, $\exists 0 \leq s \leq \phi(N)$ tq $t\phi(N) + se = 1$. Attention, s doit rester secret pour la sécurité du fonctionnement ! Ensuite, Alice publie le couple (N, e).

Si Bob souhaite envoyer un message sûr à Alice, il doit transformer son message en un entier $M \in \mathbb{Z}$ tq $0 < M < N$. Il utilise ensuite la clef publique de pour publier à son tour $\widetilde{M} \equiv M^e \pmod N$.

Pour déchiffrer ce message, Alice utilise s (tel que $\overline{s}$ est l'inverse de $\overline{e}$ dans $\mathbb{Z}/\phi(N)\mathbb{Z}$) pour trouver $(\widetilde{M})^e \equiv M^{es} \pmod N \equiv M \pmod N$, par le théorème suivant.

Théorème $\forall 0 < M < N = pq \in \mathbb{N}$ tq p, q sont premiers, soit $u \equiv 1 \pmod{\phi(N)}$. Alors $M^u \equiv M \pmod N$.

Dém $(0 < M < N = pq) \Rightarrow (p \not| M) \vee (q \not| M)$. Soit u tq $u \equiv 1 \pmod{\phi(N)}$, donc $u = 1 + t\phi(n) = 1 + t(p-1)(q-1)$.

cas 1 : $(p \not| M) \wedge (q \not| M)$ $M^u = M^{1+t(p-1)(q-1)} = MM^{(p-1)(q-1)}$. Comme $p \not| M$, par le PTF[4], $(M^{t(q-1)})^{(p-1)} \equiv 1 \pmod p$, et comme $q \not| M$, par le PTF, $(M^{t(p-1)})^{(q-1)} \equiv 1 \pmod q$. Donc $(M^u \equiv M \pmod p) \wedge (M^u \equiv M \pmod q) \Rightarrow (p \mid (M^u - M)) \wedge (q \mid (M^u - M)) \Rightarrow (pq \mid (M^u - M))$. Donc $\exists m \in \mathbb{Z}$ tq $M^u - M = mpq \iff M^u = M + mpq \equiv M \pmod{pq = N}$.

[4] Petit Théorème de Fermat.

cas 2 : $(p \not| M) \wedge (q \,|\, M)\,(q \not| M) \Rightarrow (M^{t(p-1)})^{(q-1)} \equiv 1 \,(\mathrm{mod}\, q) \Rightarrow M^{t(p-1)(q-1)} = 1 + lq$, pour $l \in \mathbb{Z}$. Donc $M^u = M(1+lq) = M + Mlq$, et comme $p \,|M$, on a $M^u = M + pclq$ pour $c \in \mathbb{Z}$. En réorganisant, on obtient $M^u = M + lcN$, ou encore $M^u \equiv M \,(\mathrm{mod}\, N)$.

cas 3 : $(p \,|\, M) \wedge (q \not| M)$ Se prouve par symétrie du cas 2.

3 Combinatoire énumérative

3.1 Comptage élémentaire

3.1.1 Principes de base

Def Une fonction $f : A \to B$ est dite :

- injective si $\forall a, a' \in A, f(a) = f(a') \iff a = a'$;
- surjective si $\forall b \in B, \exists a \in A$ tq $f(a) = b$;
- bijective si elle est injective et surjective.

Remarque
- si $\#B < \#A$, $\nexists f : A \to B$ injective ;
- si $\#B > \#A$, $\nexists f : A \to B$ surjective ;
- si $\#B \neq \#A$, $\nexists f : A \to B$ bijective.

Théorème Soit $f : A \to B$. Alors f est bijective $\iff \exists g : B \to A$ tq $((g \circ f) = Id_A) \wedge ((f \circ g) = Id_B)$.

Dém
- $(\Rightarrow)$ Si f est bijective, elle admet un inverse f^{-1} tq $(f \circ f^{-1}) = Id_B$ et $(f^{-1} \circ f) = Id_A$.
- $(\Leftarrow)$ S'$\exists$ une telle fonction g, prouvons que f est bijective :
  - $\forall b \in B, \forall a, a' \in A, f(a) = f(a') \Rightarrow g(f(a)) = g(f(a')) \Rightarrow (g \circ f)(a) = (g \circ f)(a') \Rightarrow a = a'$
  - Posons $a = g(b)$. Donc $f(a) = f(g(b)) = (f \circ g)(b) = b$.

La fonction f est alors bien injective et surjective (donc bijective).

Def Soient deux ensembles A et B. On note B^A l'ensemble des fonctions allant de A dans B. $B^A := \{f : A \to B\}$.

Remarque Le nombre d'éléments de cet ensemble (donc le nombre de fonctions allant de A dans B est $\#(B^A) = (\#B)^{\#A}$.

3.1.2 Cardinalité

Def Pour $n \in \mathbb{N}_0$, on définit $[n] := \{k \in \mathbb{N}_0 \text{ tq } k \leq n\}$. On pose $[0] = \emptyset$.

Def Deux ensembles A et B sont de même cardinalité s'$\exists f : A \to B$ bijective. On note alors $\#A = \#B$ ou $|A| = |B|$.

Def Un ensemble E est fini s'il est de même cardinalité que $[n]$ pour $n \in \mathbb{N}$. On note alors $\#E = n$.

Théorème Soient A, B deux ensembles finis de même cardinalité, $f : A \to B$. Les conditions suivantes sont équivalentes :

(i) f est injective ;

(ii) f est surjective ;

(iii) f est bijective.

Dém Soient A et B deux ensembles de cardinalité n, et soit $f : A \to B$. Montrons d'abord que $(i) \Rightarrow (ii)$. Montrons ensuite que $(ii) \Rightarrow (i)$. Après avoir prouvé $(i) \iff (ii)$, il faut prouver que $(i) \wedge (ii) \iff (iii)$.

- Par définition, f injective $\Rightarrow \forall a, a' \in A, f(a) = f(a') \iff a = a'$. Donc $\forall a' \neq a \in A, f(a) \neq f(a')$. Ce qui veut dire que le nombre d'éléments $b \in B$ n'admettant pas de préimage dans A est $\#B - \#A$. Or $\#B = \#A$, donc $\forall b \in B, \exists a \in A$ tq $f(a) = b$, ce qui est la définition d'une fonction surjective.
- Par définition, f surjective $\Rightarrow \forall b \in B, \exists a \in A$ tq $f(a) = b$. Donc le nombre d'éléments $b \in B$ admettant strictement plus d'une préimage $a \in A$ est $\#A - \#B$. Or $\#B = \#A$, donc $\nexists b \in B$ tq $\exists a \neq a' \in A$ tq $f(a) = f(a') = b$. Autrement dit, $\forall a, a' \in A, f(a) = f(a') \iff a = a'$, ce qui est la définition d'une fonction injective.

- Par définition, f est bijective $\iff$ f est injective $\wedge$ f est surjective.

Théorème (principe d'addition) Soient $A_i, 0 < i \leq k$, des ensembles finis deux à deux disjoints. Alors $\# \left(\bigcup_{i=1}^{k} A_i \right) = \sum_{i=1}^{k} \# A_i$.

Dém Démontrons cela par récurrence sur k, le nombre d'ensembles.

Pour $i = 1$, $\# A_1 = \# A_1$, donc ok.

Supposons que $\# \cup_{i=1}^{k} A_i = \sum_{i=1}^{k} \# A_i$ et prouvons que $\# \cup_{i=1}^{k+1} = \sum_{i=1}^{k+1}$.

$\cup_{i=1}^{k+1} = \cup_{i=1}^{k} A_i \cup A_k$. Donc $\# \cup_{i=1}^{k+1} = \#(\cup_{i=1}^{k} A_i) + \# A_k - \#((\cup_{i=1}^{k} A_i) \cap A_{k+1})$. Or, par définition, les A_i sont disjoints deux à deux. Donc $((\cup_{i=1}^{k} A_i) \cap A_{k+1}) = \emptyset$. On a donc $\#(\cup_{i=1}^{k} A_i) + \# A_{k+1} - 0$. Et par hypothèse de récurrence, $\#(\cup_{i=1}^{k} A_i) = \sum_{i=1}^{k} \# A_i$. Donc $\#(\cup_{i=1}^{k} A_i) + \# A_{k+1} = \sum_{i=1}^{k} \# A_i + \# A_{k+1} = \sum_{i=1}^{k+1} \# A_i$.

Def Soient $A_i, 0 < i \leq k$, des ensembles. On définit leur produit cartésien par :

$$\prod_{i=1}^{k} A_i := A_1 \times A_2 \times \ldots \times A_k = \{(a_i)_{i \in [k]} \text{ tq } a_i \in A_i\}.$$

Théorème (principe de multiplication) Soient $A_i, 0 < i \leq k$ des ensembles finis, pour $k \in \mathbb{N}_0$. Alors : $\# \left(\prod_{i=1}^{k} A_i \right) = \prod_{i=1}^{k} \# A_i$.

3.1.3 Factorielle

Def La factorielle de $n \in \mathbb{N}_0$ est le nombre $n! := \prod_{i=0}^{n} i$. On pose $0! := 1$.

Théorème Soient A et B deux ensembles tels que $\# A = \# B = n$. Il existe $n!$ bijections $f : A \to B$.

Dém Soit $A = \{a_1, \ldots, a_n\}$. Pour construire une bijection $f : A \to B$, on choisit les images des éléments de A par f. Pour a_1, on a n choix ($\#B$). Pour a_2, on a $(n-1)$ choix ($\#(B \setminus \{a_1\})$). Pour a_i, le nombre de choix s'élève donc à $(n - i + 1)$. Le nombre de bijections est donc $\prod_{i=1}^{n} i = n!$.

Proposition Soient A et B deux ensembles finis de cardinalité respective k et n avec $k < n$. Alors le nombre de fonctions $f : A \to B$ injectives est $n(n-1)(n-2)\ldots(n-k+1) = \frac{n!}{(n-k)!}$.

Dém Soient $A = \{a_1, \ldots a_k\}$ et $B = \{b_1, \ldots a_n\}$ avec $k < n$. Pour construire une fonction $f : A \to B$, il faut choisir $\forall a \in A$ une image $b \in B$. Pour que la fonction soit injective, lors du choix de a_1, on a n choix, mais lors du choix de a_2, on n'a plus que $(n-1)$ choix (pour garantir la propriété d'injection). Donc pour a_k, il restera $(n - k + 1)$ choix. Le nombre total de fonctions injectives est donc $n(n-1)(n-2)\ldots(n-k+1) = \frac{n!}{(n-k)!}$.

Remarque Une injection $f : [k] \to [n]$ revient à choisir k éléments parmi n (en tenant compte de l'ordre).

Exemple Soit E un ensemble. Le nombre d'ordres totaux sur E est $(\#E)!$.

3.1.4 Croissance de $n!$

Remarque En regardant la fonction $n \mapsto (n!)^2 = n(n-1)\ldots 1 n(n-1)\ldots 1 = \prod_{k=1}^{n} k(n-k+1)$. Cette fonction est une fonction du second degré en k, donc une parabole. On sait donc déterminer son maximum (en $\frac{n+1}{2}$). De là, il est possible de borner le carré de la factorielle de la sorte :

$$\begin{aligned}
\forall k \in [n], n \leq (n-k+1) &\leq \left(\frac{n+1}{2}\right)^2 \\
n^n \leq \prod_{k=1}^{n} k(n-k+1) &\leq \left(\frac{n+1}{2}\right)^{2n} \\
n^n \leq (n!)^2 &\leq \left(\frac{n+1}{2}\right)^{2n} \\
n^{\frac{n}{2}} \leq n! &\leq \left(\frac{n+1}{2}\right)^{n}.
\end{aligned}$$

3.1.5 Coefficients binomiaux

Def Pour $n, k \in \mathbb{N}$ tq $k \leq n$, le coefficient binomial $\binom{k}{n}$ (se prononce n choose k) est défini par $\binom{k}{n} := \frac{n!}{k!(n-k)!}$ et représente le nombre de sous-ensembles à k éléments dans $[n]$ (l'ordre n'a pas d'importance).

Propriété (symétrie) $\forall k \leq n \in \mathbb{N}, \binom{k}{n} = \binom{n}{n-k}$.

Dém Par définition, $\binom{k}{n}$ est le nombre de sous-ensembles de $[n]$ à k éléments.

Soit $S \subseteq [n]$ tq $\#S = k$. Alors $T := [n] \setminus S \subseteq [n]$ tq $\#T = n - k$. Soit $A := \{S \subseteq [n] \text{ tq } \#S = k\}, B := \{T \subseteq [n] \text{ tq } \#T = n - k\}$. On construit $f : A \to B : S \mapsto f(S)$, où $f(S) := [n] \setminus S$. En vérifiant que f est bien une bijection, on a $\#A = \#B$, donc, par définition du coefficient binomial, $\binom{n}{k} = \binom{n}{n-k}$.

Propriété (induction) Pour $n, k \in \mathbb{N}_0, k < n$, $\binom{k}{n} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Dém Soient $S \subseteq [n]$, $e \in [n]$. Il y a donc deux cas possibles : soit $e \in S$, soit $e \notin S$.

On a :

$$\begin{aligned}
\{S \subseteq [n] \text{ tq } \#S = k\} &= \{S \subseteq [n] \text{ tq } (\#S = k) \wedge (e \in S)\} \cup \{S \subseteq [n] \text{ tq } (\#S = k) \wedge (e \notin S)\} \\
&= \{T \subseteq [n] \setminus \{e\} \text{ tq } \#T = k - 1\} \cup \{S \subseteq [n] \setminus \{e\} \text{ tq } \#S = k\}.
\end{aligned}$$

Si ces ensembles sont égaux, ils sont de même cardinalité. On a donc :

$$\#\{S \subseteq [n] \text{ tq } \#S = k\} = \#(\{T \subseteq [n] \setminus \{e\} \text{ tq } \#T = k - 1\} \cup \{S \subseteq [n] \setminus \{e\} \text{ tq } \#S = k\}).$$

Comme les deux ensembles à droite de l'égalité sont d'intersection vide, on a :

$$\begin{aligned}
\#\{S \subseteq [n] \text{ tq } \#S = k\} &= \#\{T \subseteq [n] \setminus \{e\} \text{ tq } \#T = k - 1\} &&+ \#\{S \subseteq [n] \setminus \{e\} \text{ tq } \#S = k\} \\
\binom{n}{k} &= \binom{n-1}{k-1} &&+ \binom{n-1}{k}.
\end{aligned}$$

Théorème (absorption) Soient $k, n \in \mathbb{N}_0, k \leq n$.

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

Dém Le membre de gauche est la cardinalité d'un ensemble $A := \{(S \subseteq [n], e) \text{ tq } \#S = k, e \in S\}$ et le membre de droite est la cardinalité d'un ensemble $B := \{(e, T) \text{ tq } e \in [n], T \subseteq [n] \setminus \{e\}, \#T = k - 1\}$. Construisons $f : A \to B$, une bijection afin de prouver l'égalité des cardinaux. Soit $f : A \to B : (S, e) \mapsto (e, S \setminus \{e\})$. Montrons maintenant que f est bijective :

- injectivité : montrons que $\forall S, S' \subseteq [n], e, e' \in [n], f(S, e) = f(S', e') \Rightarrow (S, e) = (S', e')$. Par définition de f, on sait $f(S, e) = (e, T := S \setminus \{e\})$ et $f(S', e') = (e', T' := S' \setminus \{e'\})$. Si $(e, T) = (e', T')$, alors il faut $e = e'$ (égalité membre à membre). Dans ce cas, on a $T = S \setminus \{e\} = S \setminus \{e'\} = T' = S' \setminus \{e'\}$. On a dès lors $S = S'$ en ajoutant e dans les deux ensembles.

- surjectivité : montrons que $\forall (e,T) \in B, \exists (S,e') \in A$ tq $f(S,e') = (e,T)$. Soient $e \in [n]$ et $S \subseteq [n]$. Prenons $e' = e$ et $S = T \cup \{e\}$. On a dès lors $f(S,e') = (e', S \setminus \{e'\}) = (e, S \setminus \{e\}) = (e,T)$.

Nous avons montré que f est bijective, donc $\#A = \#B$.

Théorème (somme parallèle) Soient $m, k \in \mathbb{N}, k \leq n$.

$$\sum_{n=k}^{m} \binom{n}{k} = \binom{m+1}{k+1}.$$

Dém Montrons ceci par récurrence sur m.

- $m = k$: $\binom{k}{k} = 1 = \binom{k+1}{k+1}$, donc ok.
- Supposons la propriété vraie pour m et montrons la pour $m+1$:

$$\sum_{n=k}^{m+1} \binom{n}{k} = \left(\sum_{n=k}^{m} \binom{n}{k} \right) + \binom{m+1}{k}.$$

Par hypothèse de récurrence, on a :

$$\sum_{n=k}^{m+1} \binom{n}{k} = \binom{m+1}{k+1} + \binom{m+1}{k} = \binom{m+2}{k+1}.$$

Théorème (binôme de Newton) Soient $x, y \in \mathbb{R}, n \in \mathbb{N}$.

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

Dém $(x+y)^n = (x+y)(x+y)\dots(x+y)$. Chaque terme $x^i y^{n-i}$ est donc un produit de n éléments tel qu'il faut choisir i fois l'élément x. Ce facteur $x^i y^{n-i}$ est donc choisi $\binom{n}{i}$ fois.

Remarque La preuve est également possible de manière plus algébrique par récurrence sur n.

Applications/interprétations du binôme de Newton

1. Le nombre de mots de n bits contenant k symboles 1 et $n-k$ symboles 0 est $\binom{n}{k}$;
2. soit un réseau routier quadrillé de routes parallèles ou perpendiculaires deux à deux. Comme un chemin de $(0,0)$ à $(a,b) \in \mathbb{N}^2$ peut être vu comme un mot binaire où le symbole 1 veut dire *haut* et le symbole 0 veut dire *droite*, on peut facilement se ramener au cas précédent et dire que le nombre de plus courts chemins est $\binom{a+b}{a} = \binom{a+b}{b}$;
3. le nombre de solutions $(x_1, \dots, x_d) \in \mathbb{N}^d, d \geq 1$ de l'équation suivante :

$$\sum_{i=1}^{d} x_i = s, s \in \mathbb{N}$$

est $\binom{s+d-1}{s}$ car on peut à nouveau se ramener au premier cas en remplaçant les symboles + par le symbole 1 et il reste s symboles 0 à répartir dans les d valeurs x_i. On cherche donc à faire un mot binaire avec s symboles 0 et $d-1$ symboles 1.

3.1.6 Coefficients multinomiaux

Def Pour $n, t \in \mathbb{N}, (k_i)_{i\in[t]}$ tq $\sum_{i=1}^{t} k_i = n$, on définit le le coefficient multinomial comme suit :

$$\binom{n}{k_1, k_2, \dots k_t} = \binom{n}{(k_i)_{i\in[t]}}.$$

Ce coefficient est le nombre de partitions ordonnées de l'ensemble $[n]$ en t sous-ensembles $S_1, S_2, \dots, S_t \subseteq [n]$ tels que $\forall i \in [t], \#S_i = k_i$.

Remarque la notion d'ordre des partitions veut dire que les sous-ensembles sont nommés et qu'échanger deux noms en laissant le contenu intact est une autre partition que la partition initiale. Par exemple pour $[2]$, les partitions suivantes : $\{S_1 = \{1\}, S_2 = \{2\}\}$ et $\{S_1 = \{2\}, S_2 = \{1\}\}$ ne sont pas équivalentes.

Remarque (bis) Le coefficient multinomial $\binom{n}{n,n-k}$ correspond au coefficient binomial $\binom{n}{k} = \binom{n}{n-k}$.

Interprétations du coefficient multinomial

- Le nombre de répartitions possibles de n objets dans t sacs distinguables en mettant k_i objets dans le sac $S_i \forall i \in [t]$ est donné par le coefficient multinomial $\binom{n}{(k_i)_{i\in[t]}}$ pour $n, t \in \mathbb{N}, k_1, \dots, k_t \in \mathbb{N}$;
- le nombre de fonctions $f : [n] \to [t]$ telles que $\#f^{-1}(\{i\}) = k_i \forall i \in [t]$ est donné par le même coefficient multinomial ;
- le nombre de mots de longueur n faits dans un alphabet $\Sigma = \{\sigma^{(1)}, \sigma^{(2)}, \dots, \sigma^{(t)}\}$ tels que le nombre d'occurrences du symbole $\sigma^{(i)}$ est $k_i \forall i \in [t]$.

Def Pour $n, t \in \mathbb{N}, (k_i)_{i\in[t]}$ tq $\sum_{i=1}^{t} k_i = n$, on définit le coefficients multinomial comme suit :

$$\binom{n}{k_1, \dots, k_t} = \binom{n}{(k_i)_{i\in[t]}} = \frac{n!}{\prod_{j=1}^{t}(k_j)!}.$$

Propriétés $\forall n, t \in \mathbb{N}, (k_i)_{i\in[t]}$ tq $\sum_{i=1}^{t} k_i = n$:

- Soit $\pi : [t] \to [t]$ bijective (une permutation de $[t]$).

$$\binom{n}{(k_i) i \in [t]} = \binom{n}{(k_{\pi(i)})_{i\in[t]}}.$$

- $$\forall i \in [t], k_i \neq 0 \Rightarrow \binom{n}{(k_i)_{i\in[t]}} = \frac{k}{k_i}\binom{n-1}{k_1, k_2, \dots, k_{i-1}, k_i - 1, k_{i+1}, \dots, k_t}.$$

- Si $\forall j \in [t], k_j \neq 0$, alors

$$\binom{n}{k_1, \dots, k_t} = \sum_{j=1}^{t} \binom{n-1}{(k_i)_{i\in[t]\setminus\{j\}}, k_j - 1}.$$

Théorème Soient $n, t \in \mathbb{N}, (x_i)_{i\in[t]} \in \mathbb{R}^t$. Alors

$$\left(\sum_{i=1}^{t} x_i\right)^n = \sum_{\substack{(k_1,\dots,k_t)\in\mathbb{N}^t \\ \text{tq } \sum_i k_i = n}} \left[\binom{n}{(k_i)_{i\in[t]}} \prod_{j=1}^{t} x_j^{k_j}\right].$$

3.2 Preuves bijectives

Intuition Lorsque l'on a un ensemble fini A d'objets mathématiques, et que l'on veut connaitre son cardinal, on peut trouver un autre ensemble que l'on sait dénombrer, puis créer une bijection $f : A \to B$ afin de conclure $\#A = \#B$.

3.2.1 Arbres étiquetés

Def Un arbre étiqueté à n sommets est un arbre à n sommets dont les sommets sont numérotés de 1 à n.

Def Un graphe orienté $\vec{\Gamma} = (V, E)$ est un ensemble de sommets $v \in V$ et d'*arcs* $e \in E \subseteq V \times V$ où un arc est une arête orientée (pour $a, b \in V$, $\neg((a, b) \in E \Rightarrow (b, a) \in E)$).

Théorème (de Cayley) Le nombre d'arbres étiquetés à n sommets est n^{n-2}.

Dém Soient a_n, le nombre d'arbres étiquetés à n sommets, $\mathcal{A}_n :=$ {arbres étiquetés à n sommets avec deux sommets spéciaux notés $\bigcirc$ et $\square$ (possiblement les mêmes)} $= \{\Gamma = ((V, E), \bigcirc, \square)\}$. Les sommets $\bigcirc$ et $\square$ sont appelés respectivement extrémité gauche et droite.

On a de manière évidente $\#\mathcal{A}_N \geq a_n$ voire même $\#\mathcal{A}_n = n^2 a_n$. En effet, chaque arbre étiqueté à n sommet a n^2 possibilités pour placer $\bigcirc$ et $\square$. Maintenant montrons qu'il existe une bijection $f : [n]^{[n]} \to \mathcal{A}_n$. Ainsi, on aura $\#\mathcal{A}_n = n^n$ ou encore $a_n = n^{n-2}$. Il faut construire un arbre étiqueté à n sommets dont deux spéciaux notés $\bigcirc$ et $\square \in \mathcal{A}_n$ à partir d'une fonction $F \in [n]^{[n]}$.

Construisons l'arbre en deux étapes : d'abord construisons un graphe dirigé à partir de la fonction puis supprimons les cycles afin d'en faire un arbre.

Étape 1 : On pose $\vec{\Gamma_F} = ([n], \{(i, F(i)) \text{ tq } i \in [n]\})$, un graphe ayant pour sommets les naturels $\in [n]$ et pour arêtes les couples de la fonction F. Un tel graphe a les propriétés suivantes :

- (i) $\vec{\Gamma_F}$ a exactement n sommets ;
- (ii) $\forall v \in V, \exists! e \in E$ tq $e = (v, x)$ pour $x \in V$;
- (iii) $\forall v \in V, \#\{(x, v) \in E \text{ pour } x \in V\} \leq n$;
- (iv) Chaque composante a exactement un cycle dirigé. En effet, chaque sommet a exactement un arc sortant donc il n'y a pas de cycle non dirigé. De plus, $\vec{\Gamma_F}$ a n sommets et n arêtes, il ne peut donc être un arbre ou acyclique.
- (v) Si $\widetilde{C}$ est un cycle, alors $f_{|_{\{\text{sommets de } \tilde{C}\}}}$ est une bijection.

Étape 2 : On définit $\mathcal{M} := \{i_1, i_2, \ldots, i_t\}$ tel que $\forall j \in [m], i_j$ est un cycle dirigé dans $\vec{\Gamma_F}$ avec $i_1 < i_2 < \ldots < i_m$. La restriction $F_{|_{\mathcal{M}}} : \mathcal{M} \to \mathcal{M}$ est une bijection définie par :

$$F_{|_{\mathcal{M}}} = \begin{pmatrix} i_1 & i_2 & \ldots & i_m \\ f(i_1) & f(i_2) & \ldots & f(i_m) \end{pmatrix}.$$

De là, on construit un graphe dirigé $\vec{\Gamma_F}$:

- on enlève les arcs $\mathcal{M} \times F(\mathcal{M})$;
- on construit un chemin d'arcs $\{(F(i_j), F(i_{j+1})) \text{ tq } i_j \in [\#\mathcal{M} - 1]\}$ (cela permet de réduire de 1 le nombre d'arêtes et de connecter le graphe) ;
- on marque $F(i_1)$ par $\bigcirc$ et $F(i_m)$ par $\square$;
- on supprime l'orientation des arcs.

$\vec{\Gamma_F}$ a donc $n - 1$ arêtes, n sommets et est simple (un arbre). Il est étiqueté (par la fonction F) et a 2 sommets particuliers ($\bigcirc$ et $\square$).

Les deux étapes qui viennent d'être décrites donnent donc une fonction $f : [n]^{[n]} \to \mathcal{A}_n$. Il reste à montrer que cette fonction est bijective. Pour cela, construisons $g : \mathcal{A}_n \to [n]^{[n]}$ telle que $(f \circ g) = Id_{\mathcal{A}_n}$ et $(g \circ f) = Id_{[n]^{[n]}}$.

construction de la fonction g : On prend C, l'unique chemin entre $\square$ et $\bigcirc$.On en construit la matrice Δ de dimension $2 \times m$ où la première ligne est la permutation ordonnée de C et la seconde est C dans l'ordre de $\bigcirc$ à $\square$. On enlève tous les arcs de C. On crée des arcs allant de Δ_{1j} à $\Delta_{2j} \forall j$. Il reste à orienter les arêtes restantes en direction des cycles. On a alors $\vec{\Gamma_F}$. Définissons donc maintenant $G : [n] \to [n] : \Delta_{1j} \mapsto \Delta_{2j} \forall j$.

On a donc bien construit $g : \mathcal{A}_n \to [n]^{[n]}$ respectant les bonnes propriétés d'identité. On en déduit $\#\mathcal{A}_n = \#[n]^{[n]} = n^n$, ou encore $a_n = n^{n-2}$.

3.2.2 Arbres binaires enracinés

Def Un arbre binaire enraciné est un arbre dont tous les sommets sont de degré 1, 2 ou 3 tel qu'un et un seul sommet soit de degré 2, chaque arête a un label $l \in \{G, D\}$ et on peut représenter un tel arbre dans le plan en rangeant les sommets par étage :

- étage 1 : le sommet de degré 2 appelé racine ;
- étage $k > 1$:
  - un sommet n'est adjacent qu'à un et un seul sommet de l'étage $(k-1)$;
  - un sommet est adjacent à 0 ou 2 sommets de l'étage $(k+1)$;
  - il n'y a pas d'autre adjacence.

Def Les sommets de degré 1 sont appelés feuilles et les sommets de degré 3 sont appelés sommets internes.

Def Une triangulation d'un polygone à $(n+1)$ côtés est une découpe du polygone en triangles dont les sommets sont les sommets du polygone.

Théorème Le nombre d'arbres binaires enracinés à n sommets est égal au nombre de triangulations d'un polygone à $(n+1)$ côtés.

Dém Soient $\mathcal{A}_n := \{$ arbres binaires enracinés à n feuilles $\}$, $\mathcal{T}_n := \{$ triangulation d'un polygone à $(n+1)$ côtés $\}$. Construisons $f : \mathcal{T}_n \to \mathcal{A}_n$ bijective.

- Nommons les côtés de $\tau \in \mathcal{T}_n$ par c_0 (sur le côté supérieur), $c_1, \dots, c_n$ dans le sens anti-horlogique ;
- plaçons la racine de $a \in \mathcal{A}_n$ dans le triangle adjacent à c_0 ;
- plaçons un sommet interne ($\deg v = 3$) dans chaque autre triangle ;
- plaçons les feuilles sur les côtés $c_1, \dots, c_n$ ($(n+1)$ faces et n feuilles) ;
- les arêtes vont relier les sommets placés dans des triangles adjacents. Et les arêtes vont relier les sommets internes aux feuilles dans un même triangle.

Reste à montrer que f est bijective.

Remarque $\mathcal{T}_n = \frac{1}{n}\binom{2(n-1)}{n-1}$ (démonstration plus tard).

3.3 Relations de récurrence

3.3.1 Le tri fusion

Intro Le tri fusion applique la notion de *Divide & conquer*, à savoir diviser le set de données à traiter afin de traiter séparément des cas plus petits et unifier la solution à la fin.

Rappel Le principe du tri fusion (*merge sort*) est de diviser le vecteur à trier en deux, trier les deux sous-vecteur et unifier les deux sous-veceturs de manière à avoir l'union des deux triées. Pour trier chaque sous-vecteur, le principe est récursif jusqu'à obtenir un sous-vecteur déjà trié (de taille unitaire).

Proposition Le nombre de copies exécutées lors d'un merge sort sur un vecteur de taille $N = 2^n$ avec $m \in \mathbb{N}$ est $N \log_2 N$.

Dém Comptons C_N, le nombre de copies effectuées. On sait que si le vecteur est de taille unitaire, il est déjà trié, il n'y a donc aucune copie. De plus, lors de la récursion, les sous-vecteurs sont de taille respective $\left\lceil \frac{N}{2} \right\rceil$ et $\left\lfloor \frac{N}{2} \right\rfloor$. Cependant comme $N = 2^n$, on sait que $2 \mid N$. Dès lors, $\left\lceil \frac{N}{2} \right\rceil = \frac{N}{2} = \left\lfloor \frac{N}{2} \right\rfloor$. On trouve donc :

$$\begin{cases} C_N = 2C_{\frac{N}{2}} + N & \forall n \geq 2 \\ C_1 = 0 \end{cases}$$

Si on pose $a_n := \frac{C_{2^n}}{2^n}$, on obtient :

$$\begin{cases} a_n = a_{n-1} + 1 \\ a_0 = 0 \end{cases}$$

Cette relation de récurrence peut être simplifiée en $a_n = n$, ou encore $C_{2^n} = 2^n n$. Et comme $N = 2^n$, on a $C_N = N \log_2 N$.

Prop Le nombre de copies effectuées par le tri fusion pour trier un vecteur V de taille 2^n est $C_N = N \log_2 N$.

Def Un ensemble de droites du plan est en position générale si toute paire de droites s'intersecte en exactement un point et tout triplet de droites a une intersection vide.

Def $\Phi_2(n) : \mathbb{N} \to \mathbb{N}$ est le nombre de régions du plan délimitées par un ensemble de n droites en position générale.

Exemple

n	$\Phi_2(n)$
0	1
1	2
2	4
3	7
4	11

On "devine" $\Phi_2(n) = \Phi(n-1) + n$.

Remarque Montrons que $\Phi_2(n)$ ne dépend pas de la position des n droites.

Théorème $\forall n \in \mathbb{N}$, le nombre de régions du plan délimitées par n droites en position générale ne dépend pas du choix des droites. $\Phi_2(n)$ est donc bien défini. De plus $\forall n \in \mathbb{N}$:

$$\begin{cases} \Phi_2(n) = \Phi_2(n-1) + n & \text{si } n \geq 1, \\ \Phi_2(n) = 1. \end{cases}$$

Dém Montrons que $\Phi_2(n)$ est bien définie :

- $\Phi_2(0) = 1$ est bien défini car sans droite, le plan n'est pas séparé ;
- $\Phi_2(1) = 2$ est bien défini car une droite coupe le plan en deux ;
- Supposons $n \geq 2$ et que $\Phi_2(n-1)$ est bien défini et montrons que $\Phi_2(n)$ est bien définie.

  Soient $D_1, D_2, \ldots, D_{n-1}$ $(n-1)$ droites dans le plan en position générale. Le plan est donc subdivisé en $\Phi_2(n-1)$ régions (par hypothèse). Soit D_n une droite du plan telle que $D_1, \ldots, D_n$ sont en position générale. La droite D_n admet donc $(n-1)$ points d'intersection et est donc séparée en n intervalles. Ces intervalles "coupent" chacun une région en 2 parties. Les n droites $D_1, \ldots, D_n$ séparent donc le plan en $\Phi_2(n-1) + n$ régions.

Remarque $\Phi_2(n) = \Phi_2(n-1) + n = \Phi_2(n-2) + (n-1) + n = \Phi_2(0) + 1 + 2 + \ldots + n = 1 + \sum_{k=1}^{n} k = 1 + \frac{n(n+1)}{2} = 1 + \binom{n+1}{2} = 1 + \binom{n}{1} + \binom{n}{2} = \sum_{k=0}^{2} \binom{n}{k}$.

3.4 Récurrences linéaires

3.4.1 Récurrence linéaire de premier ordre

Def

- Une récurrence linéaire de premier ordre est une récurrence de la forme :

$$\begin{cases} x_n = c_n x_{n-1} + d_n & \text{si } x \geq 1 \\ x_0 = 0 \end{cases} \qquad (*).$$

- Une solution d'une telle récurrence linéaire est une suite $(x_n)_{n \in \mathbb{N}}$.

Théorème La récurrence $(*)$ a pour solution explicite la suite $(x_n)_{n \in \mathbb{N}}$ où x_n est définie ainsi :

$$x_n = \sum_{i=1}^{n} d_i \prod_{j=i+1}^{n} c_j = d_1 c_2 c_3 \ldots c_n + d_2 c_3 c_4 \ldots c_n + \ldots + d_{n-1} c_n + d_n.$$

Dém Prouvons-le par récurrence sur n.

- $n = 1$: $x_1 = c_n x_0 + d_1$, ok.
- $n \geq 2$: supposons que ce soit vrai pour x_{n-1} et démontrons pour x_n :

$$\begin{aligned} x_n &= c_n x_{n-1} + d_n \\ &= c_n \left[\sum_{i=1}^{n-1} d_i \prod_{j=i+1}^{n-1} c_j \right] + d_n \\ &= \left[\sum_{i=1}^{n-1} d_i c_n \prod_{j=i+1}^{n-1} c_j \right] + d_n \\ &= \left[\sum_{i=1}^{n-1} d_i \prod_{j=i+1}^{n} c_j \right] + d_n \\ &= \sum_{i=1}^{n} d_i \prod_{j=i+1}^{n} c_j. \qquad \square \end{aligned}$$

3.4.2 Récurrences linéaires à coefficients constants

Exemple De combien de manières différentes peut-on paver un rectangle de dimensions $2 \times n$ avec des dominos (non-numérotés) ?

Def Notons $P_n :=$ le nombre de tels pavages d'un rectangle $2 \times n$. Dès lors :

$$\begin{cases} P_n = P_{n-1} + P_{n-2} & \text{si } n \geq 3, \\ P_1 = 1, P_2 = 2. \end{cases}$$

On trouve :

n	P_n
0	non défini
1	1
2	2
3	3
4	5
5	8

Def La suite de Fibonacci est l'unique suite $(F_n)_{n \in \mathbb{N}}$ telle que :

$$\begin{cases} F_n = F_{n-1} + F_{n-2} & \text{si } n \geq 3, \\ F_0 = 0, F_1 = 1. \end{cases}$$

Def

- Une récurrence linéaire homogène à coefficient constants est un système d'équations de la forme :

$$x_n = c_{d-1} x_{n-1} + c_{d-2} x_{d-2} + \ldots + c_0 x_{n-d} \tag{1}$$

  où $c_i \in \mathbb{C} \ \ \forall i \in \{0, 1, \ldots, d-1\}$;
- si $c_0 \neq 0$, l'ordre de récurrence est $d \in \mathbb{N}$;
- une solution est une suite $(x_n) \in \mathbb{C}^{\mathbb{N}}$ qui satisfait l'équation (1).

Rappel $\mathbb{C}^{\mathbb{N}}$ peut être muni d'une structure d'espace vectoriel :

- addition : $\forall (x_n), (y_n) \in \mathbb{C}^{\mathbb{N}}, (x_n) + (y_n) = (x_n + y_n)$;
- multiplication : $\forall (x_n) \in \mathbb{C}^{\mathbb{N}}, \lambda \in \mathbb{C}, \lambda(x_n) = (\lambda x_n)$.

Remarque $\dim \mathbb{C}^{\mathbb{N}} = +\infty$.

Def Le polynôme caractéristique de la récurrence linéaire homogène à coefficients constants (1) est un polynôme $P(t)$ de degré d est défini par :

$$P(t) = -t^d + c_{d-1}t^{d-1} = c_{d-2}t^{d-2} + \ldots + c_0 = \sum_{i=0}^{d} c_i t^i \text{ avec } c_d = -1.$$

Rappel On cherche, pour Fibonacci, des solutions de la forme $F_n = \beta$ pour $\beta \in \mathbb{C}$. L'équation $F_n = F_{n-1} + F_{n-2}$ devient donc $\beta^n = \beta^{n-1} + \beta^{n-2} \iff \beta^2 = \beta + 1 \iff \beta^2 - \beta - 1 = 0$. Cette équation du second degré est de discriminant $\Delta = 5$ et a donc pour solutions $\beta_1 = \frac{1+\sqrt{5}}{2}$ et $\beta_2 = \frac{1-\sqrt{5}}{2}$. Par construction, on sait donc que les suites (φ^n) et $(\bar{\varphi}^n)$ sont des solutions de la RLCC des nombres de Fibonacci où $\varphi = \frac{1+\sqrt{5}}{2}$ est le nombre d'or et où $\bar{\varphi} = \frac{1-\sqrt{5}}{2}$ est son conjugué.

Remarque Si $(\varphi)^n$ et $(\bar{\varphi}^n)$ sont des solutions de la RLCC de Fibonacci, alors $\forall \lambda, \mu \in \mathbb{C}, (\lambda\varphi^n + \mu\bar{\varphi}^n)$ est également une solution.

Théorème Notons W l'ensemble des solutions de la RLCC (avec $c_0 \neq 0$). Alors :

(i) W est un sous-espace vectoriel de $\mathbb{C}^{\mathbb{N}}$;

(ii) $\dim W = d$.

Dém Pour montrer le point (i), il faut montrer que la somme et le produit par un scalaire sont stables et que $(0) \in W$.

- $(0) \in W$ est trivial (en insérant 0 pour tous les c_i dans la définition de la RLCC, on voit que $(0) \in W$) ;
- $\lambda(x_n) + \mu(y_n) \coloneqq (\lambda x_n + \mu y_n)$. Donc soit $n \geq d$. On a :

$$\lambda x_n + \mu y_n = \lambda(c_{d-1}x_{n-1} + \ldots + c_0 x_{n-d}) + \mu(c_{n-1}y_{n-1} + \ldots + c_0 y_{n-d}) = \sum_{i=1}^{d} c_{d-i}(\lambda x_{n-i} + \mu y_{n-i}).$$

Or $(\lambda x_n + \mu y_n)$ est une racine du polynôme caractéristique et est onc une solution de (1). Dès lors, $(\lambda x_n + \mu y_n) \in W$

Pour montrer le point (ii), il faut trouver une bijection linéaire $f : \mathbb{C}^d \to W$ pour montrer que W et $\mathbb{C}^d$ sont isomorphes.

Soit $f : W \to \mathbb{C}^d : (x_n)_n \mapsto (x_i)_{i\in[d-1]}$. Montrons que f est un isomorphisme :

- montrons que f est linéaire :

$$f(\lambda(x_n) + \mu(y_n)) = f((\lambda x_n + \mu y_n)_n) = (\lambda x_i + \mu y_i)_{i\in[d-1]} = \lambda(x_i)_{i\in[d-1]} + \mu(y_i)_{i\in[d-1]} = \lambda f((x_n)) + \mu f((y_n)).$$

- montrons que f est bijective :
  - surjectif : $\forall (x_0, \ldots, x_{d-1}) \in \mathbb{C}^d : \exists (\tilde{x}_n) \in W$ tq $f((x_n)) = (x_0, \ldots, x_{d-1})$. Construisons $(\tilde{x}_n)$ comme suit :

$$\tilde{x}_i = \begin{cases} x_i & \text{si } i < d \\ \displaystyle\sum_{i=j}^{d} c_{n-j}x_{i-j} & \text{si } i \geq d \end{cases}$$

– injectif : $\forall (x_n), (y_n) \in W : f((x_n)) = f((y_n)) \Rightarrow (x_n) = (y_n)$. On sait que deux suites $(x_n), (y_n)$ sont égales si et seulement si $x_i = y_i \forall i$. Ici, $f((x_n)) = f((y_n)) \iff x_i = y_i \forall i \in [d-1]$ car les termes suivants sont construits sur base des précédents. Dès lors :

$$x_d = c_{d-1}x_{d-1} + c_{d-2}x_{d-2} + \ldots + c_0x_0 = c_{d-1}y_{d-1} + c_{d-2}y_{d-2} + \ldots + c_0y_0 = y_d$$
$$x_t = c_{d-1}x_{t-1} + c_{d-2}x_{t-2} + \ldots + c_0x_{t-d} = c_{d-1}y_{t-1} + c_{d-2}y_{t-2} + \ldots + c_0y_{t-d} = y_t.$$

□

Def Soient $P(t)$ un polynôme à coefficients complexes, $a \in \mathbb{C}$ une racine de P est de multiplicité $m(a)$ si $P(t)$ est divisible par $(t-a)^{m(a)}$ mais pas par $(t-a)^{m(a)+1}$.

Théorème Construisons la RLCC homogène d'ordre $d > 1$:

$$-x_n + c_{d-1}x_{n-1} + \ldots + c_0x_{n-d} = 0 \quad \forall n \geq d$$

où $c_i \in \mathbb{C}\ \forall i \in [d-1]$ et $c_0 \neq 0$. Notons $P(t)$ son polynôme caractéristique. Toute solution de cette RLCC est une combinaison linéaire des d suites de la forme $(n^j\beta^n)$ où β est une racine de $P(t)$ et $j \in [m(\beta)-1]$. Soient $\beta_1, \beta_2, \ldots, \beta_k \in \mathbb{C}$ les racines de $P(t)$ deux à deux distinctes de multiplicité respective $m(\beta_1), m(\beta_2), \ldots, m(\beta_k)$. C'est-à-dire :

$$P(t) = -\prod_{i=1}^{k}(t-\beta_i)^{m(\beta_k)}.$$

Donc toute solution (y_n) s'écrit :

$$y_n = \sum_{\delta=1}^{k}\sum_{j_\delta=0}^{m(\beta_\delta)-1}\lambda_{j\delta}n^{j\delta}\beta^n.$$

où les λ_{j_i} sont des constantes ne dépendant pas de n.

Exemple

1. $F_n = F_{n-1} + F_{n-2}\ \forall n \geq 2$. Donc $P(t) = -t^2 + t + 1$. Les racines sont φ et $\bar{\varphi}$. Dès lors, les solutions de la RLCC sont (φ^n) et $(\bar{\varphi}^n)$. L'ensemble des solutions est donc $\{(\lambda\varphi^n + \mu\bar{\varphi}^n) : \lambda, \mu \in \mathbb{C}\}$. Pour retomber sur les conditions initiales $(F_0 = 0, F_1 = 1)$, on a :

$$\begin{cases} \lambda + \mu = 0 \\ \lambda\varphi + \mu\bar{\varphi} = 1 \end{cases}$$

   La solution est donc $(\lambda, \mu) = (\frac{\sqrt{5}}{5}, -\frac{\sqrt{5}}{5})$. Dès lors, on peut déterminer :

$$F_n = \frac{\sqrt{5}}{5}(\varphi^n - \bar{\varphi}^n).$$

2. Soit la relation suivante : $x_n = -(x_{n-1} + x_{n-2})$ où $x_0 = 0$ et $x_1 = 1$. Le polynôme caractéristique est $P(t) = t^2 + t + 1$ et admet pour racines : $\frac{-1\pm\sqrt{3}i}{2}$. Dès lors les solutions sont sous la forme :

$$\left(\lambda\left(\frac{-1+\sqrt{3}i}{2}\right)^n + \mu\left(\frac{-1-\sqrt{3}i}{2}\right)^n\right).$$

   Afin de retomber sur les conditions initiales, il faut $(\lambda, \mu) = \left(\frac{-i}{\sqrt{3}}, \frac{i}{\sqrt{3}}\right)$. La solution à cette RLCC est donc :

$$\left(\frac{i}{\sqrt{3}}\left(\left(\frac{-1-\sqrt{3}i}{2}\right)^n-\left(\frac{-1+\sqrt{3}i}{2}\right)^n\right)\right)_n.$$

3. $x_n = 2x_{n-1} - x_{n-2}\ \forall n \geq 2$. Le polynôme caractéristique est donc $P(t) = t^2 - 2t + 1 = (t-1)^2)$. Dès lors les solutions sont sous la forme (x_n) où $x_n = \lambda 1^n + \mu(n \cdot 1^n)$ avec $\lambda, \mu \in \mathbb{C}$.

Résolution générale d'une RLCC Une RLCC non-homogène st un système d'équation sous la forme :

$$-x_n + c_{d-1}x_{n-1} + c_{d-2}x_{n-2} + \ldots + c_1 x_{n-d+1} + c_0 x_{n-d} = a_n \tag{2}$$

où $(a_n) \in \mathbb{C}^{\mathbb{N}}$. Et se résout de la manière suivante :

1. déterminer S^{EHA}, l'ensemble des solutions de l'équation homogène associée (**??**);
2. trouver une solution particulière $(x_n^{SP}) \in \mathbb{C}^{\mathbb{N}}$ de la RLCC non-homogène (2) ;
3. exprimer l'ensemble des solutions de la RLCC non-homogène :

$$S \coloneqq S^{EHA} + ((x_n^{SP})).$$

Donc toute suite (z_n) est une solution de la RLCC non homogène si elle s'écrit demanière unique comme :

$$(z_n) = (y_n) + (x_n^{SP}) \text{ où } (y_n) \in S^{EHA}.$$

3.4.3 Récurrences *Divide and Conquer*

Exemple Le tri fusion : $C_N = C_{\lfloor \frac{N}{2} \rfloor} + C_{\lceil \frac{N}{2} \rceil} + N$.

Recherche binaire

Objectif Localiser x dans un vecteur trié de taille N.

Algorithme Comparer x au $\left\lceil \frac{N}{2} \right\rceil$ élément du vecteur (appelé *pivot*). Si $x =$ pivot, ok. Si $x <$ pivot, l'algo s'appelle récursivement sur le sous-vecteur des éléments 1 à $\left\lceil \frac{N}{2} \right\rceil - 1$. Si $x >$ pivot, pareil mais sur $\left\lceil \frac{N}{2} \right\rceil + 1$ à N.

Théorème Le nombre de comparaisons , dans le pire des cas, effectuées par par la recherche binaire dans un vecteur de taille N est B_N, solution de :

$$\begin{cases} B_N = B_{\lfloor \frac{N}{2} \rfloor} + 1 \\ B_1 = 1 \end{cases}$$

On a $B_N = \lfloor \log_2 N \rfloor + 1$, qui représente le nombre de bits nécessaires à l'encodage binaire du nombre N.

Dém Soit $\widetilde{B}_N$, le nombre de bits dans la représentation binaire de N. Montrons que $\widetilde{B}_N = \widetilde{B}_{\lfloor \frac{N}{2} \rfloor} + 1$. On sait :

$$N = \sum_{i=0}^{\widetilde{B}_N - 1} a_i 2^i \text{ où } a_i \in \{0,1\}, a_{\widetilde{B}_N} = 1.$$

De plus, on sait que :

$$\left\lfloor \frac{N}{2} \right\rfloor = \left\lfloor \frac{1}{2} \sum_{i=1}^{\widetilde{B}_N - 1} a_i 2^i \right\rfloor = \left\lfloor \sum_{i=1}^{\widetilde{B}_N - 1} a_i 2^{i-1} + \frac{a_0}{2} \right\rfloor = \sum_{i=0}^{\widetilde{B}_N - 2} a_{i+1} 2^i.$$

Donc $\left\lfloor \frac{N}{2} \right\rfloor$ nécessite autant de bits que $\sum_{i=0}^{\widetilde{B}_N-2} a_{i+1}2^i$. Le nombre de bits dans le premier est $\widetilde{B}_{\lfloor \frac{N}{2} \rfloor}$ et le nombre de bits du second est $B_N - 1$. Comme le nombre 1 s'écrit de la même manière en toute base, on sait $\widetilde{B}_1 = 1$. Le nombre de bits nécessaires à l'encodage binaire du nombre N est bien $\widetilde{B}_N$, une solution à la relation de récurrence précédente.

Montrons maintenant que $\widetilde{B}_N = \lfloor \log_2 N \rfloor + 1$. Soit $N = 2^b + a_1 2^{b-1} + \ldots + a_b 2^0$. On voit que $\widetilde{B}_N = b + 1$. De plus, on sait que $\frac{N}{2^b} = 1 + \frac{a_1}{2} + \ldots + \frac{a_b}{2^b}$. Si $1 < \frac{N}{2^b} < 2$, alors $0 < \log_2 N - b < 1$, ou encore $b < \log_2 N < b + 1$. De là, $\lfloor \log_2 N \rfloor = b$. Dès lors, $\widetilde{B}_N = b + 1 = \lfloor \log_2 N \rfloor + 1$. $\square$

Tri fusion

Def Soit un vecteur de taille N. On définit C_N par le nombre de copies effectuée par le tri fusion sur ce vecteur. C_N est une solution de la relation suivante :

$$\begin{cases} C_1 = 0 \\ C_N = C_{\lfloor \frac{N}{2} \rfloor} + C_{\lceil \frac{N}{2} \rceil} + N \end{cases}$$

Proposition On peut déterminer $C_N = (N-1) + \sum_{i=1}^{N-1} \widetilde{B}_i$.

Dém Soient C_N, C_{N+1}. On pose $D_N \coloneqq C_{N+1} - C_N$. On a donc :

$$\begin{aligned} D_N = C_{N+1} - C_N &= \left(C_{\lceil \frac{N+1}{2} \rceil} + C_{\lfloor \frac{N+1}{2} \rfloor} + (N+1) \right) - \left(C_{\lceil \frac{N}{2} \rceil} + C_{\lfloor \frac{N}{2} \rfloor} + N \right) \\ &= C_{\lceil \frac{N+1}{2} \rceil} - C_{\lceil \frac{N}{2} \rceil} + C_{\lfloor \frac{N+1}{2} \rfloor} - C_{\lfloor \frac{N}{2} \rfloor} + 1 = C_{\lceil \frac{N+1}{2} \rceil} - C_{\lfloor \frac{N}{2} \rfloor} + 1 \\ &= C_{\lfloor \frac{N}{2} \rfloor + 1} - C_{\lfloor \frac{N}{2} \rfloor} + 1 = D_{\lfloor \frac{N}{2} \rfloor} + 1. \end{aligned}$$

Avec $D_1 = C_2 - C_1 = 2 - 0 = 2$. En posant $n \coloneqq \lfloor \log_2 N \rfloor$, on peut définir $\alpha_n \coloneqq D_N$. De là, on sait que $\alpha_n = \alpha_{n-1} + 1$ qui peut se simplifier en $\alpha_n = n + k$ où $k = 2$ selon les conditions initiales. On en déduit $D_N = \alpha_n = n + 2 = \lfloor \log_2 N \rfloor + 2$. Maintenant, on sait :

$$\begin{aligned} C_N = C_N - 0 = C_N - C_1 = C_N + \sum_{i=2}^{N-1} (-C_i + C_i) - C_1 = \sum_{i=2}^{N} (C_i - C_{i-1}) = \sum_{i=2}^{N} D_{i-1} = \sum_{i=1}^{N-1} D_i \\ = \sum_{i=1}^{N-1} (\lfloor \log_2 N \rfloor + 2) = \sum_{i=1}^{N-1} (\lfloor \log_2 N + 1 \rfloor) + \sum_{i=1}^{N-1} 1 = (N-1) + \sum_{i=1}^{N-1} \widetilde{B}_i. \ \square \end{aligned}$$

Théorème Le nombre de copies effectuées par le tri fusion pour un vecteur de taille N est exactement :

$$C_N = N \lfloor \log_2 N \rfloor + 2N - 2^{\lfloor \log_2 N \rfloor + 1}.$$

Remarque Ce nombre est également un majorant du nombre de comparaisons.

Dém Premièrement, montrons que $\sum_{i=1}^{N} \widetilde{B}_i = \sum_{i=0}^{\lfloor \log_2 N \rfloor} (N - 2^i)$. En effet, dans l'ensemble des nombres de 1 à $N-1$, ils contiennent tous un bit sur le bit de poids le plus faible ($= (N-1) = (N-2^0)$), tous sauf le premier contiennent le second bit ($= (N-1) = (N-2^1)$), tous sauf le premier et les deux suivants contiennent le troisième bit ($= (N-4) = (N-2^2)$), etc. De manière plus générale, les $2^i - 1$ premiers nombres ne contiennent pas le i^e bit. Le nombre de nombres contenant le i^e bit est donc $((N-1) - (2^i - 1)) = (N - 2^i)$. Et le nombre de bits est $\widetilde{B}_i = \lfloor \log_2 N \rfloor + 1$. On a donc $\sum_{i=1}^{N-1} (\lfloor \log_2 N \rfloor + 1) = \sum_{i=0}^{\lfloor \log_2 N \rfloor} (N - 2^i) = N(\lfloor \log_2 N \rfloor + 1) - \sum_{i=0}^{\lfloor \log_2 N \rfloor} 2^i$.

Dès lors :

$$C_N = (N-1) + \sum_{i=1}^{N-1}(N-2^i) = (N-1) + N\lfloor log_2 N\rfloor + N - (2^{\lfloor \log_2 N\rfloor+1} - 1)$$
$$= 2N - 1 + N\lfloor \log_2 N\rfloor - 2^{\lfloor \log_2 N\rfloor+1} + 1 = 2N + N\lfloor \log_2 N\rfloor + 2^{\lfloor \log_2 N\rfloor+1}. \quad \square$$

Comportements asymptotiques

Considérons deux fonctions $f, g : \mathbb{N} \to \mathbb{R}^+$ s'annulant en un nombre fini de valeurs.

Def

1. Si $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$, on dit que f et g sont *asymptotiquement équivalents*, ce qui se note $f \sim g$;
2. si $\exists C > 0, n_0 \in \mathbb{N}$ tq $f(n) \leq Cg(n) \ \ \forall n \geq n_0$, on dit que f est un grand O de g, ce qui se note $f = O(g)$;
3. si $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$, on dit que f est un petit o de g, ce qui se note $f = o(g)$;
4. si $f = O(g)$, alors $g = \Omega(f)$;
5. si $f = o(g)$, alors $g = \omega(f)$;
6. si $f = O(g)$ et $g = O(f)$, on dit que f et g ont un même comportement asymptotique, ce qui se note $f = \Theta(g)$.

Remarque Si $f = o(g)$, alors $f = O(g)$. De même, si $g = \omega(f)$, alors $g = \Omega(f)$.

Exemple Chaque fonction ci-dessous est un $o(\cdot)$ de la précédente :

$$n^n, 2^n, n^2, n, \sqrt{n}, \log(n)^2, \log(n), \log(\log(n)).$$

3.4.4 Récurrences *Divide and Conquer* générales

Objectif Obtenir le comportement asymptotique de coût en temps (ou en espace) d'un algorithme qui résout un problème de taille N en :

- produisant un certain nombre α de sous-problèmes de taille $\left\lfloor \frac{N}{\beta} \right\rfloor$ ou $\left\lceil \frac{N}{\beta} \right\rceil$;
- s'appliquant récursivement sur chaque problème ;
- recombinant les solutions des α sous-problèmes pour trouver une solution du problème original.

Ce qui se note $a_N = \alpha a_{\frac{N}{\beta}} + f(N) \ \ \forall N \in \mathbb{N}$ avec $f : \mathbb{N} \to \mathbb{R}^+$et où $\frac{N}{\beta}$ est interprété tantôt comme $\left\lfloor \frac{N}{\beta} \right\rfloor$, tantôt comme $\left\lceil \frac{N}{\beta} \right\rceil$.

Commençons par étudier l'équation fonctionnelle suivante :

$$\begin{cases} a(x) = \alpha a\left(\frac{N}{\beta}\right) + x & \text{si } x > 1 \\ a(x) = 0 & \text{si } x \leq 1 \end{cases} \tag{3}$$

avec $\alpha, \beta \in \mathbb{R}$ tels que $\alpha > 0$ et $\beta > 1$.

Théorème Si la fonction $a : \mathbb{R}^+ \to \mathbb{R}^+$ est une solution de de (3), alors :

1. si $\alpha > \beta$:

$$a(x) = \Theta\left(x^{\log_\beta \alpha}\right);$$

2. si $\alpha = \beta$:

$$a(x) \sim x \log_\beta x = \Theta(x \log_2 x);$$

3. si $\alpha < \beta$:

$$a(x) \sim \frac{\beta}{\beta - \alpha} x = \Theta(x).$$

Exemple Soit un tri fusion sur un vecteur de taille $N = 2^n$, où $\alpha = \beta = 2$, alors $C_N = N \log_2 N$.

Dém Soit une fonction $a : \mathbb{R}^+ \to \mathbb{R}^+$, solution de (3). Dès lors :

$$\begin{aligned} a(x) &= x + \alpha a\left(\frac{x}{\beta}\right) = x + \alpha\left[\frac{x}{\beta} + \alpha a\left(\frac{x}{\beta^2}\right)\right] = x + \frac{\alpha}{\beta}x + \alpha^2 a\left(\frac{x}{\beta^2}\right) = x + \frac{\alpha}{\beta}x + \frac{\alpha^2}{\beta^2}x + \alpha^3 a\left(\frac{x}{\beta^3}\right) \\ &= \ldots = \left[1 + \frac{\alpha}{\beta} + \frac{\alpha^2}{\beta^2} + \ldots + \frac{\alpha^{t-1}}{\beta^{t-1}}\right] x = \left[\sum_{i=0}^{t-1} \frac{\alpha^i}{\beta^i}\right] x = \left[\frac{1 - \frac{\alpha^t}{\beta^t}}{1 - \frac{\alpha}{\beta}}\right] x. \end{aligned}$$

Où $t := \left\lceil \log_\beta x \right\rceil$ tel que $t \overset{x \to +\infty}{\longrightarrow} +\infty$.

<u>cas 3 :</u> $\alpha < \beta$, on a :

$$a(x) = \left[\frac{1 - \frac{\alpha^t}{\beta^t}}{1 - \frac{\alpha}{\beta}}\right] x \overset{x \to +\infty}{\longrightarrow} \left[\frac{1 - 0}{1 - \frac{\alpha}{\beta}}\right] x = \frac{\beta}{\beta - \alpha} x.$$

À l'aide de cette convergence, on peut exprimer $a(x) = \Theta\left(\frac{\beta}{\beta - \alpha} x\right) = \Theta(x)$.

<u>cas 2 :</u> $\alpha = \beta$, on a :

$$a(x) = x \sum_{i=0}^{t-1} \frac{\alpha^i}{\beta^i} = x \sum_{i=0}^{t-1} 1 = xt = x\left\lceil \log_\beta x \right\rceil = \Theta(x \log_2 x).$$

<u>cas 1 :</u> $\alpha > \beta$, on a :

$$\begin{aligned} a(x) &= \left[\frac{1 - \frac{\alpha^t}{\beta^t}}{1 - \frac{\alpha}{\beta}}\right] x = \frac{\alpha^t}{\beta^t}\left[\frac{\frac{\beta^t}{\alpha^t} - 1}{1 - \frac{\alpha}{\beta}}\right] x = \left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil}\left[\frac{\left(\frac{\beta}{\alpha}\right)^t - 1}{1 - \frac{\alpha}{\beta}}\right] x = \left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil + \log_\beta x - \log_\beta x}\left[\frac{\left(\frac{\beta}{\alpha}\right) - 1}{1 - \frac{\alpha}{\beta}}\right] x \\ &= \left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil - \log_\beta x} \frac{\alpha^{\log_\beta x}}{\beta^{\log_\beta x}}\left[\frac{\left(\frac{\alpha}{\beta}\right)^t - 1}{1 - \frac{\alpha}{\beta}}\right] x = \left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil - \log_\beta x} \frac{\alpha^{\log_\beta x}}{x}\left[\frac{\left(\frac{\beta}{\alpha}\right)^t - 1}{1 - \frac{\alpha}{\beta}}\right] x. \end{aligned}$$

Comme $\left(\frac{\beta}{\alpha}\right)^t \to 0$ quand $t \to +\infty$ et que la formule de changement de base d'une puissance est $\alpha^{\psi(x)} = \left(\beta^{\psi(x)}\right)^{\log_\beta \alpha}$, l'expression devient :

$$a(x) \sim \left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil - \log_\beta x}\left(\beta^{\log_\beta x}\right)^{\log_\beta \alpha}\left[\frac{-1}{1 - \frac{\alpha}{\beta}}\right] = \left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil - \log_\beta x} x^{\log_\beta \alpha}\left[\frac{\beta}{\alpha - \beta}\right]$$

De plus, $\left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil - \log_\beta x}$ est toujours borné par $\frac{\alpha}{\beta}$. Dès lors, on peut dire que :

$$a(x) = \Theta\left(\frac{\alpha}{\beta} x^{\log_\beta \alpha} \frac{\beta}{\alpha - \beta}\right) = \Theta\left(x^{\log_\beta \alpha}\right).$$

□

Théorème (Master Thorem) Soient $\alpha \geq 1, \beta > 1$ deux réels, $f : \mathbb{N} \to \mathbb{R}^+$ et $(a_N)_{N \in \mathbb{N}}$, une solution de la récurrence *Divide and Conquer* suivante :

$$a_N = \alpha a_{\frac{N}{\beta}} + f(N).$$

cas 1 : si $f(N) = O\left(N^{\log_\beta(\alpha) - \epsilon}\right)$ pour $\epsilon > 0$, alors :

$$a_N = O\left(N^{\log_\beta \alpha}\right).$$

cas 2 : si $f(N) = \Theta\left(N^{\log_\beta \alpha}\right)$, alors :

$$a_N = O\left(N^{\log_\beta \alpha} \log_2 N\right).$$

cas 3 : si $f(N) = \Omega\left(N^{\log_\beta(\alpha) + \epsilon}\right)$ pour $\epsilon > 0$, et si $\alpha f\left(\frac{N}{\beta}\right) \leq C f(N)$ pour $C < 1$ et si N est *suffisamment* grand, alors :

$$a_N = \Theta(f(N)).$$

Exemple La recherche binaire (dichotomique) : $B_N = {}_{\lfloor \frac{N}{2} \rfloor} + 1$. On a : $\alpha = 1, \beta = 2$ et $f(N) = 1 = \Theta\left(N^{\log_\beta \alpha}\right)$ (car $\log_2 1 = 0$). Dès lors, on sait par le M.T. que $O\left(N^{\log_\beta \alpha} \log_2 N\right) = O(\log_2 N)$. En effet, $B_N = \lfloor \log_2 N \rfloor + 1$.

Application (algorithme de Strassen)

Ojectif Calculer le produit de deux matrices avec un comportement asymptotique meilleur que $O(n^3)$. Soient deux matrices carrées $A, B \in M_{n \times n}(\mathbb{R})$. Soit C leur produit. Le nombre d'opérations pour déterminer les valeurs de C est $2n^3 - n^2$.
En effet, vu que :

$$C_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj},$$

pour chacun des n^2 coefficients, il y a n produits et les n termes doivent être additionnés ($(n-1)$ sommes). Le nombre d'opérations est donc $n^2(n-1) + n^2 n = n^3 - n^2 + n^3 = 2n^3 - n^2$.

L'algorithme de Strassen

Idée pour $n = 2$l'algo *usuel* de multiplication ferait donc $2 \cdot 2^3 - 2^2 = 12$ opérations (8 multiplications et 4 additions). L'algo de Strassen calcule préalablement 7 valeurs :

$$\begin{aligned}
S_1 &= (A_{11} - A_{22})(B_{21} + B_{22}) \\
S_2 &= (A_{11} + A_{22})(B_{11} + B_{22}) \\
S_3 &= (A_{11} - A_{21})(B_{11} + B_{12}) \\
S_4 &= (A_{11} + A_{12}) B_{22} \\
S_5 &= A_{11}(B_{12} - B_{22}) \\
S_6 &= A_{22}(B_{21} - B_{11}) \\
S_7 &= (A_{21} + A_{22}) B_{11}
\end{aligned}$$

Ensuite, on définit :

$$\begin{aligned} C_{11} &= S_1 + S_2 - S_4 + S_6 \\ C_{12} &= S_4 + S_5 \\ C_{21} &= S_6 + S_7 \\ C_{22} &= -S_3 + S_4 + S_5 - S_7 \end{aligned}$$

Principe général de l'algo Soit un corps $\mathbb{K}$. Soit deux matrices $\in M_{n\times n}(\mathbb{K})$:

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}.$$

On définit leur produit par une nouvelle matrice $C \in M_{n\times n}(\mathbb{K})$:

$$C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & {}_{22} \end{pmatrix}.$$

Ici, A_{ij}, B_{ij} et C_{ij} sont les sous-matrices $\in M_{\frac{n}{2}\times\frac{n}{2}}(\mathbb{K})$. L'algo de Strassen s'applique exactement de la même manière que pour e cas où $n = 2$ sauf que les additions et les produits ne se font plus sur de scalaires $\in \mathbb{K}$ mais bien des sous-matrices.

Dans le cas où $n = 2^k$, on a la relation de récurrence suivante sur $T(n) :=$ le nombre total d'opérations arithmétiques pour multiplier deux matrices $\in M_{n\times n}(\mathbb{K})$ à l'aide de l'algorithme de Strassen :

$$T(n) = 7T\left(\frac{n}{2}\right) + 18n^2.$$

Selon le M.T., on sait $f(n) = 18n^2 = \Theta(n^2), \alpha = 7, \beta = 2$. Soit $\epsilon = \log_\beta \alpha - 2$. On a donc $f(n) = O(n^2) = O\left(n^{\log_\beta(\alpha)-\epsilon}\right)$. On sait dès ors que $T(n) = \Theta\left(n^{\log_\beta \alpha}\right) \simeq \Theta(n^{2.81})$.

Remarque Si $n \neq 2^k$, on rajoute des 0 de padding.

Remarque L'algorithme de Strassen est **asymptotiquement** meilleur que l'algorithme usuel pour calculer le produit de deux matrices. Cependant, pour des petites valeurs de n, il est bien pire. Il existe d'autres algorithmes (le plus *intéressant asymptotiquement* actuellement est l'algorithme de Coppersmith-Winograd qui est en $O(n^{2.376})$, mais ces algorithmes ne sont efficaces que sur des matrices de plus en plus grande au point qu'ils ne puissent être utilisés en pratique).

Conjecture Il existe des algorithmes pour la multiplication de deux matrices $n \times n$ qui sont en $O(n^{2+\epsilon})$ pour tout $\epsilon > 0$. En effet, l'exposant doit être au moins égal à deux car tous les éléments de la matrices doivent se voir assigner une valeur et il y en a n^2.

3.5 Fonctions génératrices

Idée Transformer une suite (a_n) en une fonction définie par une série.

Objectif Trouver des formules pour les termes de la suite (a_n).

3.5.1 Exemple introductif

La suite de Fibonacci est représentée par la RLCC suivante :

$$\begin{cases} F_n = F_{n-1} + F_{n-2} \ \ \forall n \geq 2 \\ F_0 = 0, F_1 = 1 \end{cases}$$

On associe une fonction à la suite de Fibonacci $(F_n)_n$:

$$f(x) = \sum_{n=0}^{+\infty} F_n x^n.$$

Cette fonction est une *série formelle*, à savoir une série dont on ne se soucie pas de la convergence.

On peut étendre cette fonction :

$$f(x) = \sum_{n=0}^{+\infty} F_n x^n = 0 + x + \sum_{n=2}^{+\infty} F_n x^n = x + \sum_{n=2}^{+\infty} (F_{n-1} + F_{n-2}) x^n = x + x \sum_{n=0}^{+\infty} F_n x^n + x^2 \sum_{n=0}^{+\infty} F_n x^n = x + xf(x) + x^2 f(x).$$

Dès lors, on peut exprimer, en isolant $f(x)$:

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

Remarque Soit $\mathbb{R}[X]$ l'anneau des polynômes réels, soit $\mathbb{R}[X)$ l'anneau des séries formelles. Il existe des polynômes ($1 - \lambda x$ par exemple) n'admettant pas d'inverse multiplicatif dans $\mathbb{R}[X]$ mais qui admettent un inverse multiplicatif dans $\mathbb{R}[X)$. En effet, $(1 - x)(1 + \lambda x + \lambda^2 x^2 + \ldots) = 1 + \lambda x - \lambda x + \lambda^2 x^2 - \lambda^2 x^2 + \ldots = 1$.

Dès lors, on note $\frac{1}{1-\lambda x} = 1 + \lambda x + \lambda^2 x^2 + \ldots$.

Trouvons maintenant un autre moyen d'exprimer $f(x)$:

$$f(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \varphi x)(1 - \bar{\varphi} x)} = \frac{A}{1 - \varphi x} + \frac{B}{1 - \bar{\varphi} x}.$$

On trouve $A = \frac{1}{\sqrt{5}}$ et $B = \frac{-1}{\sqrt{5}}$. Dès lors :

$$f(x) = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \varphi x} - \frac{1}{1 - \bar{\varphi} x} \right).$$

Or on sait que $\frac{1}{1-\varphi x} = \sum_{n=0}^{\infty} (\varphi x)^n$ et $\frac{1}{1-\bar{\varphi} x} = \sum_{n=0}^{\infty} (\bar{\varphi} x)^n$. Donc :

$$f(x) = \frac{1}{\sqrt{5}} \left(\sum_{n=0}^{\infty} (\varphi x)^n - \sum_{n=0}^{\infty} (\bar{\varphi} x)^n \right) = \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} (\varphi^n - \bar{\varphi}^n) x^n.$$

Or on sait que $f(x) = \sum_{n=0}^{\infty} F_N x^n$. Dès lors, on sait que $F_n = (\varphi^n - \bar{\varphi}^n)$.

3.5.2 Fonctions génératrices ordinaires

Def La fonction génératrice ordinaire (FGO) de la suite $(a_n)_n$ est définie par $A(x) = \sum_{n=0}^{\infty} a_n x^n$. On note $[x^n]A(x)$ le coefficient de $A(x)$ devant x^n.

Remarque
- Dans les séries formelles, on ignore les question sur la convergence ;
- on manipule les séries formellement (comme des polynômes) ;
- certaines suites vont converger pour certaines valeurs de x.

Théorème Soient $A(x), B(x)$, les FGOs des suites $(a_n), (b_n)$. Alors :

(i) $A(x) + B(x)$ est la FGO de la suite $(a_n + b_n)$;

(ii) $xA(x)$ est la FGO de la suite $(a_{n-1})_{n\in\mathbb{N}^*}$;

(iii) $\int_0^x A(t)\,\mathrm{d}t$ est la FGO de la suite $\left(\frac{a_{n-1}}{n}\right)_{n\in\mathbb{N}^*}$;

(iv) $\frac{A(x)-a_0}{x}$ est la FGO de la suite $(a_{n+1})_n$;

(v) $\frac{\partial x}{\partial A}(x)$ est la FGO de $(na_n)_{n\in\mathbb{N}^*}$;

(vi) $A(x)B(x)$ est la FGO de la suite $\left(\sum_{k=0}^n a_k b_{n-k}\right)_n$;

(vii) $(1-x)A(x)$ est la FGO de la suite $(a_n - a_{n-1})_{n\in\mathbb{N}^*}$;

$(viii)$ $\frac{A(x)}{1-x}$ est la FGO de $\left(\sum_{k=0}^n a_k\right)_n$.

Démonstration (partielle) du théorème

(iii) Étant donné que les séries sont traitées comme des séries formelles, les hypothèses de convergences ne sont pas considérées. Dès lors :

$$\int_0^x A(t)\,\mathrm{d}t = \int_0^x \sum_{n=0}^{\infty} a_n t^n\,\mathrm{d}t = \sum_{n=0}^{\infty}\int_0^x a_n t^n\,\mathrm{d}t = \sum_{n=0}^{\infty}\frac{a_n}{n+1}x^{n+1}.$$

La suite est donc $\left(0, a_0, \frac{a_1}{2}, \frac{a_2}{3}, \ldots\right) = \left(\frac{a_n}{n+1}\right)_{n\in\mathbb{N}^*}$.

(v) $\frac{\partial x}{\partial A}(x) = \sum_{n=0}^{\infty} a_n \frac{\partial x}{\partial x}^n = \sum_{i=1}^{\infty} n a_n x^{n-1}$. La suite est donc $(a_1, 2a_2, \ldots) = ((n+1)a_{n+1})_n$.

(vi)

$$A(x)B(x) = \left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)x^n.$$

La suite est donc $\left(\sum_{k=0}^n a_k b_{n-k}\right)_n$.

$(viii)$ En partant du fait que $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ et que $A(x) = \sum_{n=0}^{\infty} a_n x^n$, par le point (vi), on a la suite :

$$\left(\sum_{k=0}^{n} a_k \beta_{n-k}\right)_n = \left(\sum_{k=0}^{n} a_k\right)_n.$$

□

Exemple Déterminer la FGO de la suite $(n)_n$. On sait que $\frac{1}{1-x}$ est la FGO de $(1)_n$. Par le point $(viii)$ du théorème, on sait que $\left(\frac{1}{1-x}\right)^2$ est la FGO de $\left(\sum_{k=0}^n 1\right)_n = (n)_n$.

Proposition Soit $k \in \mathbb{N}$ fixé. La FGO de la suite $\left(\binom{n}{k}\right)_n$ où $\binom{n}{k} \coloneqq 0$ si $n < k$ est :

$$\frac{x^k}{(1-x)^{k+1}}.$$

Dém Prouvons-le par récurrence sur k.

<u>cas de base :</u> $k = 0$. Alors $\binom{n}{k} = 1\ \forall n$. La FGO est donc $\frac{1}{1-x} = \frac{x^0}{(1-x)^{0+1}}$.

<u>Pas de récurrence :</u> supposons la propriété vraie pour k et prouvons-la pour $(k+1)$.

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

Soient $A(x) = \frac{x}{1-x}$ et $B(x) = \frac{x^k}{(1-x)^{k+1}}$. Par hypothèse, $B(x) = \sum_{n=0}^{\infty} \binom{n}{k} x^n$. Et par le théorème précédent, on sait que $A(x) = \sum_{n=1}^{\infty} x^n$. Dès lors, $C(x) = A(x)B(x)$ est donné par :

$$C(x) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_k b_{b-i} \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_k b_{n-i} \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{i=1}^{n} b_{n-i} \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n-1} \binom{i}{k} \right) x^n = \sum_{n=0}^{\infty} \binom{n}{k+1} x^n$$

La fonction $C(x) = \frac{x^{k+1}}{(1-x)^{k+2}}$ est donc bien la FGO de la suite $\left(\binom{n}{n+1} \right)_n$.

□

Les nombres harmoniques

Def Pour $n \in \mathbb{N}$, on définit :

$$H_n \coloneqq \begin{cases} 0 & \text{si } n = 0 \\ \displaystyle\sum_{k=1}^{\infty} \frac{1}{x^k} & \text{si } n > 0 \end{cases}$$

Proposition La FGO de la suite $(H_n)_n$ est :

$$H(x) = \left(\frac{1}{1-x} \right) \ln \left(\frac{1}{1-x} \right).$$

Dém Partons de la fonction $x \mapsto \frac{1}{1-x}$, FGO de $(1)_n$. Par le point (iii), on sait que :

$$\int_0^x \frac{1}{1-t} \, \mathrm{d}t = -\ln(1-x) = \ln \left(\frac{1}{1-x} \right)$$

est la FGO de la suite $\left(0, 1, \frac{1}{2}, \frac{1}{3}, \ldots\right)$. On a tous les termes de la suite, il faut maintenant les sommer. Par le point $(viii)$, on sait que :

$$\frac{1}{1-x} \ln \left(\frac{1}{1-x} \right)$$

est la FGO de $\left(\sum_{k=1}^{n} \frac{1}{x^k} \right)$, qui est ce que l'on voulait.

□

Les nombres de Catalan

Def Le n^e nombre de Catalan, noté C_n est le nombre de parenthésages possibles pour un produit de n facteurs $x_1, x_2, \ldots, x_n$ (avec $C_0 = 0$).

Lien avec les arbres enracinés à n feuilles On construit l'arbre et on associe un facteur à chaque feuille. Chaque nœud interne correspond à un produit parenthésé.

Proposition $(C_n)_n$ est la solution de la récurrence :

$$C_n = C_1 C_{n-1} + C_2 C_{n-2} + \ldots + C_{n-1} C_1 = \sum_{k=1}^{n-1} C_k C_{n-k}.$$

De plus, $C_n = \frac{1}{n} \binom{2(n-1)}{n-1}$ pour tout $n \geq 1$.

Dém Montrons que $C_n = \sum_{k=1}^{n-1} C_k C_{n-k}$.

Soit $C(x) \coloneqq \sum_{n=0}^{\infty} C_n x^n$, la FGO de la suite des nombres de Catalan. On a :

$$C(x) = C_1 x + C_2 x^2 + \ldots = x + (C_1 C_1)x^2 + (C_1 C_2 + C_2 C_1)x^3 + \ldots = x + C(x)C(x).$$

On a donc $C(x) = x + C(x)^2$, ou encore $(C(x))^2 - C(x) + x = 0$. Cette équation du second degré a deux solutions possibles : $C_1(x) = \frac{1+\sqrt{1-4x}}{2}$ et $C_2(x) = \frac{1-\sqrt{1-4x}}{2}$. Or il faut $C(0) = 0$, donc la solution est $C(x) = C_2(x)$. Par la formule de Taylor de $C(x)$ autours du $x = 0$, on a (en prenant $f(x) = \sqrt{1-4x}$) :

$$C(x) = \frac{1}{2} - \frac{1}{2}\sum_{n=0}^{\infty} f^{(n)}(0)\frac{x^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{2}(-1)^{n+1}\binom{\frac{1}{2}}{n}(-4x)^n.$$

Où $\binom{\frac{1}{2}}{n}$ est défini par :

$$\binom{\frac{1}{2}}{n} \coloneqq \begin{cases} 1 & \text{si } n = 0 \\ \dfrac{1}{n!}\displaystyle\prod_{k=1}^{n-1}\left(\frac{1}{2} - k\right) & \text{si } n > 0 \end{cases}$$

Or $C(x) = \sum_{n=0}^{\infty} C_n x^n$. Dès lors, on sait que :

$$C_n = (-1)^{n+1}\binom{\frac{1}{2}}{n}\frac{1}{2}4^n = (-1)^{n+1}2^{2n}\frac{1}{2n!}\prod_{k=0}^{n-1}\left(\frac{1}{2} - k\right) = 2^{2n}(-1)^{n+1}\frac{1}{4n!}\prod_{k=1}^{n-1}\left(\frac{1}{2} - k\right).$$

Or tous les termes du produit (il y en a $(n-1)$) sont négatifs. Dès lors, en rentrant le $(-1)^{n+1} = (-1)^{n-1}$ dans le produit, et en mettant $\frac{1}{2}$ en évidence à chaque terme, on obtient :

$$C(x) = \frac{2^{2n}}{4n!}\left(\frac{1}{2}\right)^{n-1}\prod_{k=1}^{n-1}(2k-1) = \frac{2^n}{2n!}\prod_{k=1}^{n-1}(2k-1).$$

En utilisant $\frac{n!}{n!}$ pour artifice de calcul, on obtient $n!2^n = 2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2n$ au numérateur. Dès lors, on a :

$$\frac{2n}{2n!n!}\prod_{k=1}^{2n-2} k = \frac{1}{n}\frac{(2n-2)!}{(n-1)!(n-1)!} = \frac{1}{n}\binom{2(n-1)}{n-1}.$$