Introduction à la théorie de l'informatique

Pierre Geurts

Version du 8 décembre 2011

E-mail	:	p.geurts@ulg.ac.be
URL	:	http://www.montefiore.ulg.ac.be/~geurts/iti.html
Bureau	:	R 73 a (Montefiore)
Téléphone	:	04.366.48.15 — 04.366.99.64

Notes de cours

Ouvrage de référence :
Mathematics for Computer Science
Eric Lehman et Tom Leighton, 2004.

Disponible à l'adresse suivante :
`http ://www.cs.princeton.edu/courses/archive/fall06/cos341/handouts/mathcs.pdf`

Transparents :
Mis en ligne au fur et à mesure de l'avancement du cours
`http ://www.montefiore.ulg.ac.be/~geurts/iti.html`

(transparents préparés par Julien Brusten en 2010-2011, légèrement adaptés par Pierre Geurts)

Organisation du cours

Tous les mercredis de 9h à 12h30 (+ quelques vendredis matin)

Cours théorique ($\pm$1h30, Pierre Geurts) suivi d'une séance d'exercice ($\pm$1h30, Julien Brusten/Thomas Leuther)

Examen écrit uniquement (en janvier et septembre). A livre ouvert.

Objectif du cours

Former à l'écriture de preuves et aux raisonnements utilisés dans la théorie de l'informatique.

Différents champs mathématiques seront utilisés comme outils/illustrations :

- Notion de preuves
- Théorie des nombres
- Théorie des graphes
- Sommations et comportements asymptotiques
- Récurrences
- Technique de dénombrement
- Fonctions génératrices
- ...

L'accent sera mis sur l'exploitation des concepts vus au cours pour écrire de nouvelles preuves plus que sur la restitution de la matière théorique.

Chapitre 1

Preuves

Définition : Une *démonstration* est une vérification d'une *proposition* par une séquence de *déductions logiques* à partir d'un ensemble d'*axiomes*.

Propositions

Définition : Une *proposition* est un énoncé qui est *soit vrai*, *soit faux*.

Exemples :

- $2 + 3 = 5$. Proposition vraie.
- $(\forall n \in \mathbb{N})$ $n^2 + n + 41$ est un nombre premier. Proposition fausse : pour $n = 40$, on a $n^2 + n + 41 = 40^2 + 40 + 41 = 41^2$.
- (Conjecture d'Euler, 1769) $a^4 + b^4 + c^4 = d^4$ n'a pas de solution quand $a, b, c, d \in \mathbb{N}^+$. Proposition fausse (Elkies, 1988). Contre-exemple : $a = 95800, b = 217519, c = 414560, d = 422481$.
- $(\exists a, b, c, d \in \mathbb{N}^+)$ $a^4 + b^4 + c^4 = d^4$. Proposition vraie.

- $(\forall n \in \mathbb{Z})\ (n \geq 2) \Rightarrow (n^2 \geq 4)$. Proposition vraie.
- $1 = 0 \Rightarrow (\forall n \in \mathbb{N})\ n^2 + n + 41$ est un nombre premier. Proposition vraie.
- $(\forall n \in \mathbb{Z})\ (n \geq 2) \Leftrightarrow (n^2 \geq 4)$. Proposition fausse.

Axiomes

- Définition : Un *axiome* est une proposition qui est *supposée vraie*.
- Exemple : $(\forall a, b, c \in \mathbb{Z})\ (a = b \text{ et } b = c) \Rightarrow (a = c)$.
- Un ensemble d'axiomes est *consistant* s'il n'existe pas de proposition dont on peut démontrer qu'elle est *à la fois vraie et fausse*.
- Un ensemble d'axiomes est *complet* si, pour toute proposition, il est possible de démontrer qu'elle est vraie ou fausse.
- Théorème d'incomplétude de Gödel (1931) : tout ensemble consistant d'axiomes pour l'arithmétique sur les entiers est nécessairement incomplet.
- Dans ce cours, on considérera comme axiomes les notions des mathématiques de base.

Autres types de proposition

- Un *théorème* est une proposition qui peut être démontrée
- Un *lemme* est une proposition préliminaire utile pour faire la démonstration d'autres propositions plus importantes
- Un *corrolaire* est une proposition qui peut se déduire d'un théorème en quelques étapes logiques
- Une *conjecture* est une proposition pour laquelle on ne connaît pas encore de démonstration mais que l'on soupçonne d'être vraie, en l'absence de contre-exemple. Exemple : tout entier pair strictement plus grand que 2 est la somme de deux nombres premiers (Conjecture de Golbach).

Déductions logiques

- Définition : Les *règles de déductions logiques*, ou *règles d'inférence*, sont des règles permettant de combiner des axiomes et des propositions vraies pour établir de nouvelles propositions vraies.
- Exemple : $\boxed{\dfrac{P \quad P \Rightarrow Q}{Q}}$ (modus ponens).

  Le modus ponens est fortement lié à la proposition $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$, qui est une *tautologie*.
  (= une proposition qui est toujours vraie quelles que soient les valeurs de ses variables)

Exemples de démonstrations

Théorème : La proposition suivante est une tautologie :

$$(X \Rightarrow Y) \Leftrightarrow (\neg Y \Rightarrow \neg X).$$

Démonstration : Montrons que $(X \Rightarrow Y)$ est logiquement équivalent à sa *contraposée* $(\neg Y \Rightarrow \neg X)$, quelles que soient les valeurs booléennes des variables X et Y.

X	Y	$X \Rightarrow Y$	$\neg Y \Rightarrow \neg X$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

La proposition $(X \Rightarrow Y) \Leftrightarrow (\neg Y \Rightarrow \neg X)$ est donc vraie dans tous les cas, ce qui implique qu'elle est une tautologie. □

Les deux règles suivantes sont donc des règles d'inférence.

$$\frac{P \Rightarrow Q}{\neg Q \Rightarrow \neg P} \qquad \frac{\neg Q \Rightarrow \neg P}{P \Rightarrow Q.}$$

Théorème : $(\forall a \in \mathbb{Z})$ (a est pair) $\Leftrightarrow$ (a^2 est pair).

Démonstration : Soit a un entier quelconque.

$\boxed{a \text{ est pair} \Rightarrow a^2 \text{ est pair}}$ Supposons que a soit pair. On a donc $a = 2b$, avec $b \in \mathbb{Z}$. Dès lors, on obtient $a^2 = (2b)^2 = 4b^2 = 2(2b^2)$. Le nombre a^2 est donc pair.

$\boxed{a^2 \text{ est pair} \Rightarrow a \text{ est pair}}$ Par le théorème précédent, il suffit de démontrer que a est impair $\Rightarrow$ a^2 est impair. Supposons que a soit impair. On a donc $a = 2b + 1$, avec $b \in \mathbb{Z}$. Dès lors, on obtient $a^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1$. Le nombre a^2 est donc impair. □

Démonstrations par l'absurde

Principe :

- On veut démontrer qu'une proposition P est vraie.
- On suppose que $\neg P$ est vraie, et on montre que cette hypothèse conduit à une *contradiction*.
- Ainsi, $\neg P$ est fausse, ce qui implique que P est vraie.

Règle d'inférence correspondante :

$$\frac{\neg P \Rightarrow \text{faux}}{P}$$

Exemple

Théorème : $\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$.

Démonstration : Par l'absurde, supposons que $\sqrt{2} \in \mathbb{Q}$. On a donc

$$\sqrt{2} = \frac{a}{b},$$

où $a, b \in \mathbb{Z}$, $b \neq 0$ et où cette fraction est réduite. Cela implique $2 = \frac{a^2}{b^2}$, et donc

$$2b^2 = a^2.$$

Par conséquent, le nombre a^2 est pair, ce qui implique que a est lui-même pair.

Il existe donc $a' \in \mathbb{Z}$ tel que $a = 2a'$. On a donc $a^2 = 4a'^2$. Donc, on a $2b^2 = 4a'^2$, ce qui implique que

$$b^2 = 2a'^2.$$

Dès lors, b^2 est pair, et donc b est lui-même pair. Il existe donc $b' \in \mathbb{Z}$ tel que $b = 2b'$. La fraction

$$\frac{a}{b} = \frac{2a'}{2b'}$$

n'est donc pas réduite. C'est une contradiction. Par conséquent, l'hypothèse selon laquelle $\sqrt{2} \in \mathbb{Q}$ est fausse. Donc, on a $\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$. □

Écrire de bonnes démonstrations

En plus d'être logiquement correcte, une bonne démonstration doit être *claire*.

Conseils pour l'écriture de bonnes démonstrations :

- Expliquez la manière dont vous allez procéder (par l'absurde, contraposition, induction, ...) ;
- Donnez une explication séquentielle ;
- Expliquez votre raisonnement (passages d'une étape à l'autre, arithmétique, induction, ...) ;
- N'utilisez pas trop de symboles ; utiliser du texte lorsque c'est possible ;
- Simplifiez ;

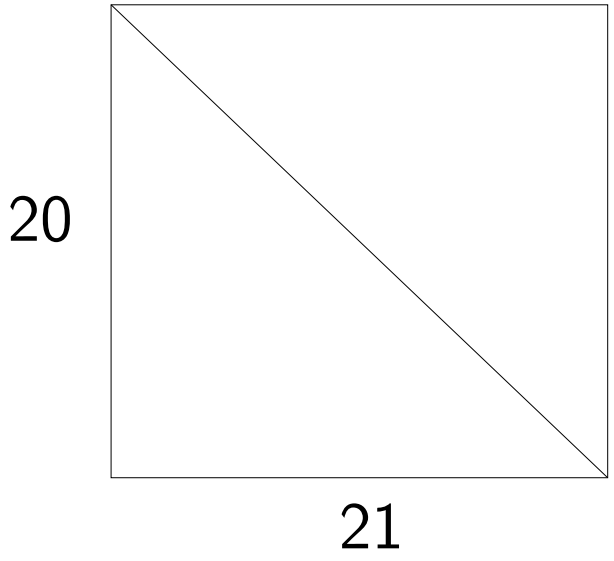
- Introduisez des notations judicieusement, en prenant soin définir leur signification ;
- Si la démonstration est trop longue, structurez-la (par exemple établissez à l'aide de *lemmes* les faits dont vous aurez souvent besoin) ;
- N'essayez pas de camoufler les passages que vous avez du mal à justifier ;
- Terminez en expliquant à quelles conclusions on peut arriver.

Un faux théorème

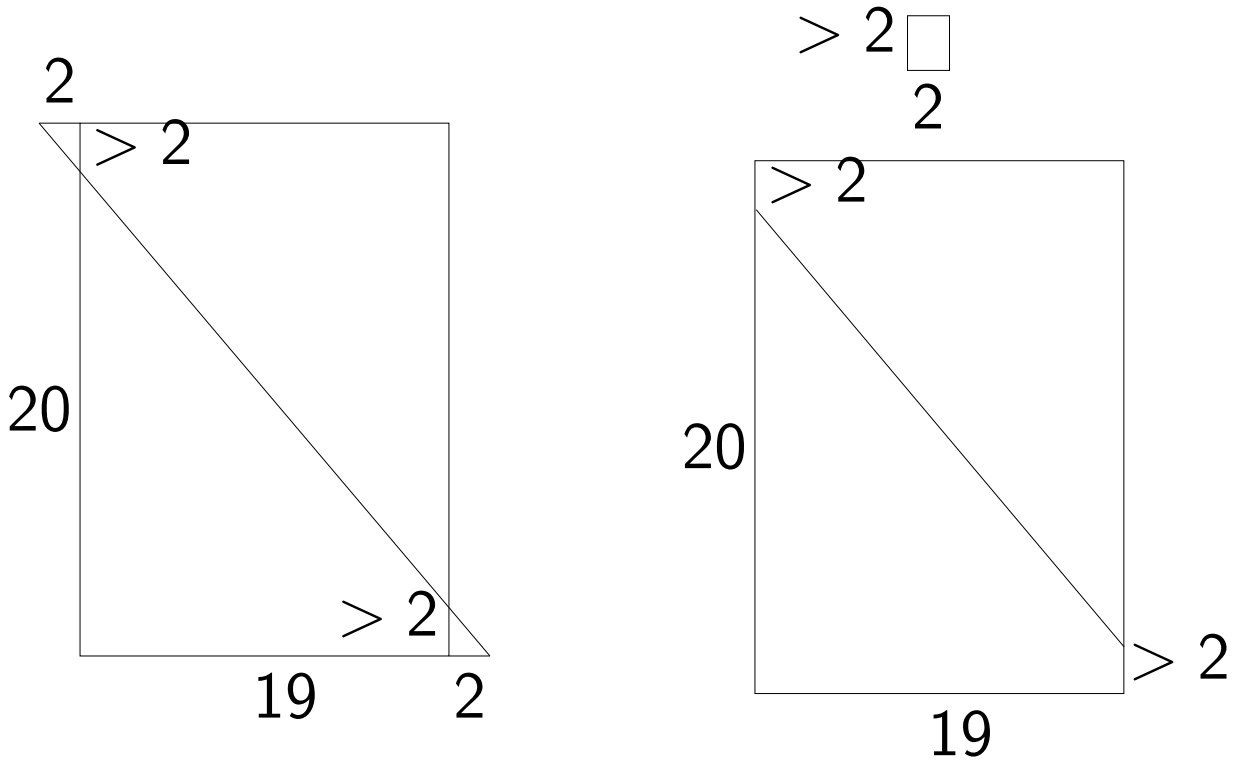
Quelle est l'erreur dans la démonstration suivante ?

Faux théorème : $420 > 422$.

Démonstration erronée : Démonstration géométrique. Soit un rectangle de dimension 20×21. Son aire vaut donc 420.



Découpage + glissement de 2 unités vers la gauche :



- Aire du petit rectangle : > 4.
- Aire du grand rectangle : $> (20 + 2) \times 19 = 418$.
- $\Rightarrow$ Aire totale : > 422. Par conservation d'aire, on a donc $420 > 422$. □

Chapitre 2

Inductions

Principe d'induction

Principe d'induction :

Soit $P(n)$ un prédicat. Si

- $P(0)$ est vrai, et si
- pour tout $n \in \mathbb{N}$, $P(n)$ implique $P(n+1)$,

alors $P(n)$ est vrai pour tout $n \in \mathbb{N}$.

Variante :

Soit $P(n)$ un prédicat, et soit $k \in \mathbb{N}$. Si

- $P(k)$ est vrai, et si
- pour tout $n \geq k$, $P(n)$ implique $P(n+1)$,

alors $P(n)$ est vrai pour tout $n \geq k$.

Un modèle pour les démonstrations par induction

1. Annoncer que la démonstration utilise une induction ;
2. Définir un prédicat approprié $P(n)$;
3. Démontrer que $P(0)$ est vrai (“cas de base”) ;
4. Démontrer que $P(n)$ implique $P(n+1)$ pour tout $n \in \mathbb{N}$ (“cas inductif”) ;
5. Invoquer l’induction (cette étape est souvent implicite).

Illustration

Théorème : Pour tout $n \in \mathbb{N}$, on a

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

Démonstration :

La démonstration fonctionne par induction.
Soit $P(n)$ le prédicat qui est vrai si et seulement si $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Cas de base : $P(0)$ est vrai car $\sum_{i=1}^{0} i = 0 = \frac{0(0+1)}{2}$.

Cas inductif : Supposons que $P(n)$ soit vrai, où n est un nombre naturel quelconque, et démontrons que cette hypothèse implique la validité de $P(n+1)$. On a

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i\right) + (n+1).$$

Comme $P(n)$ (l'"hypothèse d'induction") est vraie, cette expression est égale à $\dfrac{n(n+1)}{2} + (n+1)$. On obtient donc

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

Dès lors, par induction, $P(n)$ est vrai quel que soit le nombre naturel n, et le théorème est démontré. □

Un théorème de divisibilité

Définition : Un nombre entier a *divise* un nombre entier b si b est un multiple de a. Lorsque a divise b, on écrit $a \mid b$.

Exemple : On a $3 \mid (5^3 - 5)$ car $5^3 - 5 = 120$ est un multiple de 3.

On souhaite démontrer par induction que, quel que soit $n \in \mathbb{N}$, on a $3 \mid (n^3 - n)$.

Soit $P(n)$ le prédicat "$3 \mid (n^3 - n)$".

Le cas de base $P(0)$ est immédiat. Pour démontrer le cas inductif, il faut supposer que $3 \mid (n^3 - n)$ et en déduire que $3 \mid ((n+1)^3 - (n+1))$.

On a

$$\begin{aligned}(n+1)^3-(n+1) &= n^3+3n+2n \\ &= (n^3-n)+(3n^2+3n).\end{aligned}$$

Comme 3 divise (n^3-n) par hypothèse d'induction, et que $3n^2+3n$ est un multiple de 3, la somme $(n^3-n)+(3n^2+3n)$ est un multiple de 3.

Réorganisons ce raisonnement dans une démonstration claire.

Théorème : $(\forall n \in \mathbb{N})\ 3 \mid (n^3-n)$.

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(n)$ la proposition $3 \mid (n^3 - n)$.
- *Cas de base :* $P(0)$ est vrai car $3 \mid (0^3 - 0)$.
- *Cas inductif :* Supposons que $P(n)$ soit vrai, où $n \in \mathbb{N}$. On a

$$\begin{aligned} 3 \mid (n^3 - n) &\Rightarrow 3 \mid ((n^3 - n) + 3(n^2 + n)) \\ &\Rightarrow 3 \mid (n^3 + 3n^2 + 3n + 1 - n - 1) \\ &\Rightarrow 3 \mid ((n+1)^3 - (n+1)). \end{aligned}$$

  Première implication : $3(n^2 + n)$ est divisible par 3.
  Autres implications : réécriture de l'expression de droite.
  On a prouvé que $P(n)$ implique $P(n+1)$ pour tout $n \in \mathbb{N}$.
- Dès lors, par induction, $P(n)$ est vrai quel que soit $n \in \mathbb{N}$, et le théorème et démontré. □

Une démonstration par induction erronée

Faux théorème : Tous les chevaux ont la même couleur.

Démonstration erronée : *(Où est l'erreur ?)*

- La démonstration fonctionne par induction.
- $P(n)$: "pour tout ensemble de n chevaux, tous ces chevaux ont la même couleur".
- *Cas de base :* $P(1)$ est vrai car tous les chevaux dans un ensemble de 1 cheval ont la même couleur.
- *Cas inductif :* Supposons que $P(n)$ soit vrai. Soit un ensemble de $n+1$ chevaux :

$$c_1, c_2, \ldots, c_n, c_{n+1}.$$

Par hypothèse, les n premiers chevaux ont la même couleur. Il en est de même pour les n derniers :

$$\underbrace{c_1, c_2, \ldots, c_n}_{\text{même couleur}}, c_{n+1}.$$

$$c_1, \underbrace{c_2, \ldots, c_n, c_{n+1}}_{\text{même couleur}}.$$

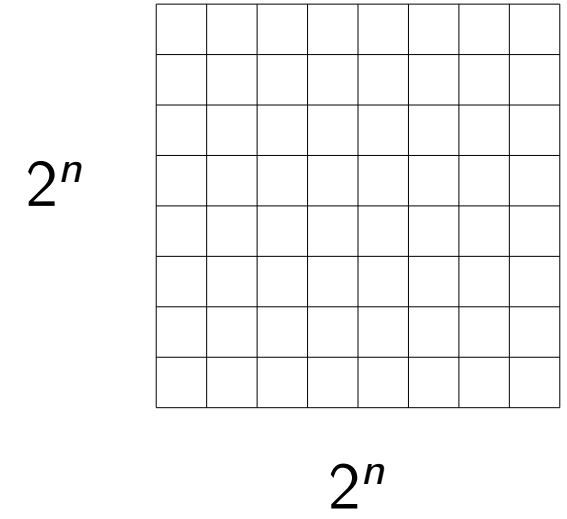
Dès lors, les chevaux $c_1, c_2, \ldots, c_{n+1}$ ont la même couleur, i.e., $P(n+1)$ est vrai. Donc, $P(n)$ implique $P(n+1)$.

- Par induction, $P(n)$ est vrai pour tout $n \geq 1$. Le théorème est un cas particulier de ce résultat : celui où n vaut le nombre total de chevaux dans le monde. □

Dallage

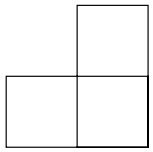
On souhaite créer une terrasse de dimension $2^n \times 2^n$ à la place de la pelouse située au centre du bâtiment B28.

Photo : ©ULg - M. Houet

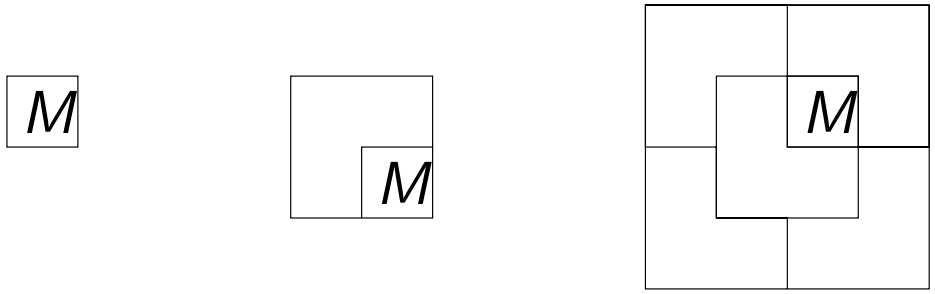


Contraintes :

- Sur un des emplacements situés au centre de la terrasse, on doit ériger une statue de Georges Montefiore (M).
- Tous les autres emplacements doivent être couverts par des dalles en "L", sans que ces dalles ne se recouvrent.



Remarque : Pour $n = 0$, $n = 1$ et $n = 2$, un dallage existe :



On demande de démontrer qu'un tel dallage existe quelle que soit la valeur $n \in \mathbb{N}$.

Problème : Choisir $P(n) =$ "il existe un dallage d'une terrasse $2^n \times 2^n$ avec M au centre" n'est pas adéquat : un dallage pour une terrasse de dimension $2^n \times 2^n$ ne permet pas de construire facilement un dallage pour une terrasse de dimension $2^{n+1} \times 2^{n+1}$.

Solution : Choisir une hypothèse d'induction *plus générale*.

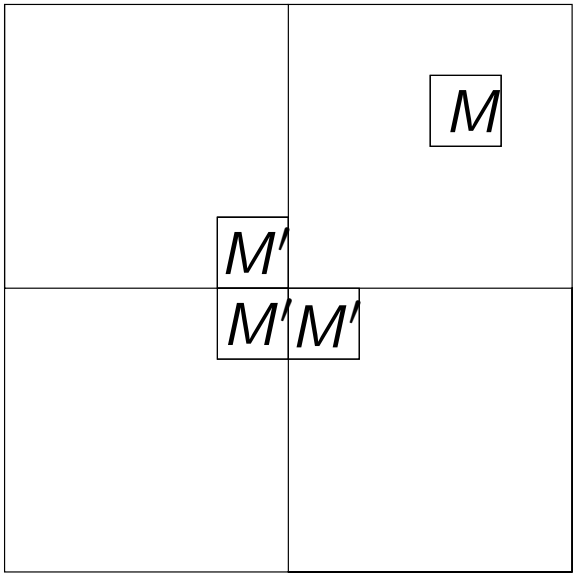
$P(n) =$ "Pour *tout* emplacement de M sur une terrasse de dimension $2^n \times 2^n$, il y a une possibilité de dallage pour le reste de la terrasse."

Théorème : Pour tout $n \in \mathbb{N}$, il existe un dallage d'une terrasse de dimension $2^n \times 2^n$ avec M au centre.

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(n) =$ "Pour *tout* emplacement de M sur une terrasse de dimension $2^n \times 2^n$, il y a une possibilité de dallage pour le reste de la terrasse."
- *Cas de base :* $P(0)$ est vrai car M couvre toute la terrasse.
- *Cas inductif :* Supposons que $P(n)$ soit vrai pour un $n \in \mathbb{N}$.
  Soit une terrasse de dimension $2^{n+1} \times 2^{n+1}$, et supposons que M se trouve sur un quelconque emplacement de celle-ci.

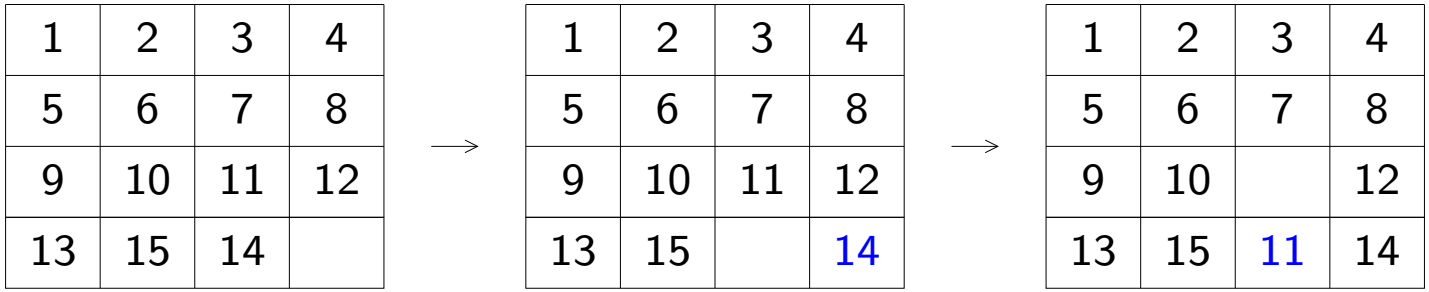
Divisons la terrasse en 4 quadrants, chacun de dimension $2^n \times 2^n$. Un d'entre-eux contient M. Plaçons un M temporaire (M' sur le schéma) sur chacun des 3 emplacements centraux situés dans les 3 autres quadrants.



Par l'hypothèse d'induction, chacun des 4 quadrants admet un dallage. Remplacer les 3 emplacements de M' par une dalle en "L" permet de terminer le travail. Donc $P(n)$ implique $P(n+1)$ pour tout $n \in \mathbb{N}$.

- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}$. Le théorème en est un cas particulier. □

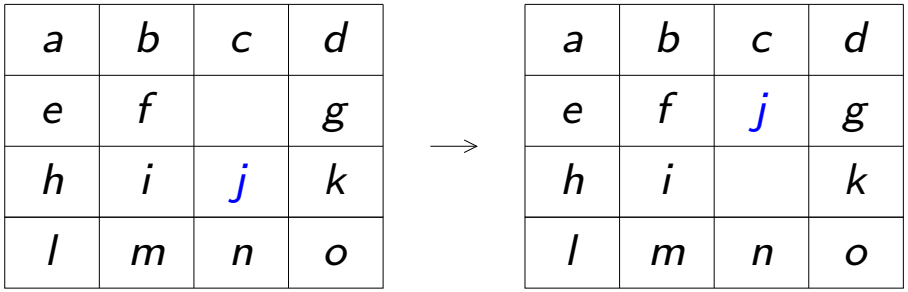
L'énigme du Taquin (Sam Lloyd, ±1870)



Existe-t-il une séquence de mouvements qui permet d'échanger les pièces 15 et 14 de la configuration de gauche, sans modifier l'emplacement des autres pièces ?

Nous allons établir un invariant du problème, c'est-à dire une propriété qui est toujours vraie, quelle que soit la façon dont les pièces sont déplacées.

- Deux types de mouvements : mouvement de ligne et mouvement de colonne.
- Lemme 1 : Un mouvement de ligne ne modifie pas l'ordre des pièces.
  Démonstration : C'est immédiat. □
- Lemme 2 : Un mouvement de colonne modifie l'ordre relatif d'exactement 3 paires de pièces.



  Démonstration : Faire glisser une pièce vers le bas la déplace après les 3 pièces suivantes. Faire glisser une pièce vers le haut la déplace avant les 3 pièces précédentes. □

- Lemme 3 : Un mouvement de ligne ne modifie jamais la parité du nombre d'inversions. Un mouvement de colonne modifie toujours la parité du nombre d'inversions.

  Démonstration : Par le lemme 1, un mouvement de ligne ne modifie pas l'ordre des pièces. En particulier, il ne modifie pas le nombre d'inversions.

  Par le lemme 2, un mouvement de colonne modifie l'ordre relatif d'exactement 3 paires de pièces. Donc, un nombre pair d'inversions devient impair, et vice-versa. □

- Lemme 4 : Dans toute configuration accessible à partir de la configuration ci-dessous, la parité du nombre d'inversions est différente de la parité du numéro de la ligne contenant la case vide.

ligne 1	1	2	3	4
ligne 2	5	6	7	8
ligne 3	9	10	11	12
ligne 4	13	15	14	

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(n) =$ "Après n mouvements, la parité du nombre d'inversions est différente de la parité du numéro de la ligne contenant la case vide".
- *Cas de base :* $P(0)$ est vrai, car, initialement, le nombre d'inversions vaut 1, tandis que le numéro de la ligne contenant la case vide vaut 4.

- *Cas inductif :* Supposons que $P(n)$ soit vrai pour un $n \in \mathbb{N}$.
  - Si le mouvement $n+1$ est un mouvement de ligne, alors $P(n+1)$ est vrai car, la ligne contenant la case vide n'a pas changé, et par le lemme 3 la parité du nombre d'inversions n'est pas modifiée.
  - Si le mouvement $n+1$ est un mouvement de colonne, alors, par le lemme 3, la parité du nombre total d'inversions a été modifiée. De plus, la parité du numéro de la ligne contenant la case vide a été modifiée également. Donc, $P(n+1)$ est vrai.
- Dès lors, $P(n)$ implique $P(n+1)$ pour tout $n \in \mathbb{N}$.
- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}$. □

- Théorème : Aucune séquence de mouvements de permet d'obtenir la configuration de droite à partir de la configuration de gauche :

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Démonstration : Dans la configuration de droite, le nombre total d'inversions est de 0, tandis que la case vide est dans la ligne 4. Par le lemme 4, cette configuration n'est pas accessible. □

Induction forte

Principe d'induction forte :

Soit $P(n)$ un prédicat. Si

- $P(0)$ est vrai, et si
- pour tout $n \in \mathbb{N}$, $P(0) \wedge P(1) \wedge \cdots \wedge P(n)$ implique $P(n+1)$,

alors $P(n)$ est vrai pour tout $n \in \mathbb{N}$.

Variante :

Soit $P(n)$ un prédicat, et soit $k \in \mathbb{N}$. Si

- $P(k)$ est vrai, et si
- pour tout $n \geq k$, $P(k) \wedge P(k+1) \wedge \cdots \wedge P(n)$ implique $P(n+1)$,

alors $P(n)$ est vrai pour tout $n \geq k$.

Remarques :

- Tout théorème qui peut être démontré par induction forte peut aussi être démontré par induction simple.
- Utiliser l'induction forte rend parfois les preuves plus simples.
- Cependant, si $P(n)$ permet de démontrer facilement que $P(n+1)$ est vrai, alors, par soucis de simplicité, il est préférable d'utiliser l'induction simple.

Application : jeu de dépilage

Règles du jeu :

- On commence avec une pile de n boîtes.
- A chaque étape, on divise une pile en deux piles non vides.
- Le jeu s'arrête lorsque l'on obtient n piles, chacune contenant une seule pile.
- Une division où l'on transforme une pile de hauteur $a + b$ en deux piles d'hauteurs a et b permet d'obtenir ab points.

Exemple :

hauteurs des piles										score
10										
5	5									25 points
5	3	2								6
4	3	2	1							4
2	3	2	1	2						4
2	2	2	1	2	1					2
1	2	2	1	2	1	1				1
1	1	2	1	2	1	1	1			1
1	1	1	1	2	1	1	1	1		1
1	1	1	1	1	1	1	1	1	1	1
									score total =	45 points

Est-il possible de trouver une meilleure stratégie ?

Théorème : Toute manière de dépiler n blocs conduit à un score de $n(n-1)/2$ points.

Démonstration :

- La démonstration fonctionne par induction forte.
- Soit $P(n) =$ "Toute manière de dépiler n blocs conduit à un score de $n(n-1)/2$ points".
- *Cas de base :* $P(1)$ est vrai car une pile de 1 bloc est déjà dépilée. Le score est donc de $0 = 1(1-1)/2$.
- *Cas inductif :* Supposons que $P(1)$, $P(2)$, ..., $P(n)$ soient vrais, avec $n \geq 1$, et supposons que nous disposions d'une pile de $n+1$ blocs.
  - Premier mouvement : divise la pile initiale en deux piles de tailles k et $n+1-k$, avec $1 \leq k < n+1$.

- On obtient :

$$\begin{aligned}
\text{s. total} &= \text{score du premier mouvement} \\
&\quad + \text{score du dépliage de } k \text{ blocs} \\
&\quad + \text{score du dépliage de } n+1-k \text{ blocs} \\
&= k(n+1-k) + \frac{k(k-1)}{2} + \frac{(n+1-k)(n-k)}{2} \\
&= \frac{2kn + 2k - 2k^2 + k^2 - k + n^2 - kn + n - k - kn + k^2}{2} \\
&= \frac{(n+1)n}{2}
\end{aligned}$$

- La conjonction $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$ implique donc $P(n+1)$ quel que soit $n \geq 1$.
- Par induction forte, on a donc $P(n)$ pour tout $n \geq 1$. □

Induction structurelle

L'induction ordinaire est basée sur les entiers naturels :

$$P(0) \Rightarrow P(1) \Rightarrow P(2) \Rightarrow \ldots \Rightarrow P(n)$$

Induction structurelle : induction plus générale basée sur des ensembles/types de données définis de manière récursive

Nombreuses applications en informatique

Définition récursive

Un *type de données récursif* R est défini par :

- des règles de base qui affirment que des éléments appartiennent à R
- des règles inductives de construction de nouveaux éléments de R à partir de ceux déjà construits

Exemples :

- L'ensemble $M \in \{], [\}^*$ des chaînes de crochets appariés :
  - cas de base : $\lambda \in M$ (chaîne vide)
  - constructeur : si $s, t \in M$, alors $[s]t \in M$
- L'ensemble $Aexp$ des expressions mathématiques définies sur une seule variable x :
  - cas de base : x et $k, \forall k \in \mathbb{N}$, sont dans $Aexp$
  - constructeurs : si $e, f \in Aexp$, alors $[e + f]$, $[e * f]$, et $-[e]$ sont dans $Aexp$.

Induction structurelle

Principe d'induction structurelle :

Soit P un prédicat défini sur un type de données récursif R. Si

- $P(b)$ est vrai pour chaque élément de base $b \in R$, et
- pour toute règle de construction $c(x_1, \ldots, x_m)$, $P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_m)$ implique $P(c(x_1, \ldots, x_m))$ pour tout x_1, x_2,$\ldots$,$x_m \in R$,

alors $P(r)$ est vrai pour tout $r \in R$.

Illustration 1

Théorème : toute chaîne dans M a un nombre égal de crochets droits et gauches.

Démonstration :

- La démonstration fonctionne par induction structurelle
- Soit $P(s) = (\#_{[}(s) = \#_{]}(s))$.
- *Cas de base :* $P(\lambda)$ est vrai car $\#_{[}(\lambda) = \#_{]}(\lambda) = 0$
- *Cas inductif :* Supposons que $P(s)$ et $P(t)$ soient vrais et montrons que $P([s]t)$ est vrai :

$$\begin{aligned} \#_{[}([s]t) &= \#_{[}(r) + \#_{[}(s) + 1 \\ &= \#_{]}(r) + \#_{]}(s) + 1 \\ &= \#_{]}([s]t) \end{aligned}$$

- Par induction structurelle, on a donc $P(s)$ pour tout $s \in M$. □

Illustration 2

Soit F, un ensemble des fonctions définies sur $\mathbb{R}$, tel que :

- $Id_{\mathbb{R}}(::= x)$, les fonctions constantes, et $\sin(x)$ sont dans F *(règles de base)*
- Si $f, g \in F$, alors :
  - $f + g$, $f.g$, e^f, (the constant e)
  - the inverse, $f^{(-1)}$, of f, and
  - $f \circ g$

  sont dans F.
  (règles inductives)

Exemples : $-x$ $(= (-1)x)$, $\sqrt{x}$ $(= (x^2)^{(-1)})$, $\cos(x)$ $(= 1 - (\sin(x).\sin(x))^{1/2})$

Théorème : Si $f \in F$, alors $f' \in F$
(F est fermé par rapport à la dérivée)

L'induction structurelle généralise l'induction simple

L'ensemble $\mathbb{N}$ peut être défini récursivement par :

- $0 \in \mathbb{N}$ *(règle de base)*
- si $n \in N$, alors le successeur, $n + 1$, de n est dans $\mathbb{N}$ *(règle inductive)*

Top 10 des techniques de démonstrations non autorisées

1. Démonstration en noyant le poisson ;
2. Démonstration par l'exemple
3. Démonstration par argumentation orale ;
4. Démonstration par notations obscures ;
5. Démonstration par épuisement ;
6. Démonstration par omission ;
7. Démonstration par dessin ;
8. Démonstration par affirmation assurée ;
9. Démonstration par intuition ;
10. Démonstration par référence à l'autorité éminente.

Chapitre 3

Théorie des nombres

Introduction

Définition : La *théorie des nombres* consiste en l'étude des nombres entiers.

Application dans ce cours : Cryptographie.

Recrutement Google en 2004

Google a diffusé le message crypté suivant en 2004 :
{FIRST 10 DIGIT PRIME IN CONSECUTIVE DIGITS OF E}.COM

$$
\begin{aligned}
e \;=\; & 2.7182818284590452353602874713526624977572470936999595749669 \\
& 6762772407663035354759457138217852516642742746639193200305 \\
& 9921817413596629043572900334295260595630738132328627943 4\ldots
\end{aligned}
$$

7427466391.com pointait vers la page de recrutement de Google.

(Lehman, Leighton, Meyer, 2011)

Rappels

Définitions :

- $a \in \mathbb{Z}$ *divise* $b \in \mathbb{Z}$ s'il existe $k \in \mathbb{Z}$ tel que $ak = b$.
- Lorsque a divise b, on écrit $a \mid b$.
- Si a *divise* b, alors on dit de façon équivalente :
  - a est un *diviseur* de b
  - a est un *facteur* de b
  - b est *divisible* par a
  - b est un *multiple* de a.
- $\forall a \neq 0$, on a $a \mid 0$, $a \mid a$, $1 \mid a$.

- $p \in \mathbb{Z}$ est *premier* si $p > 1$ et si p n'admet aucun autre diviseur entier positif que 1 et lui-même.

Problèmes difficiles célèbres

- Conjecture de Goldbach : Tout entier pair strictement plus grand que 2 est égal à la somme de deux nombres premiers
- Test de primalité : Il existe un algorithme efficace pour déterminer si un entier est premier. Meilleur algorithme à ce jour : $O((\log n)^{12})$.
- Factorisation : Etant donné le produit de deux nombres premiers $n = pq$, il n'existe pas d'algorithme efficace pour retrouver p et q.
- Dernier théorème de Fermat : Il n'existe pas d'entiers positifs x, y, z tel que

$$x^n + y^n = z^n$$

pour un entier $n > 2$. Posé par Fermat en 1630. Résolu par Willes en 1994.

Propriétés de divisibilité

Propriété : Soient $a, b \in \mathbb{Z}$. Si $a \mid b$, alors $a \mid bc$ pour tout $c \in \mathbb{Z}$.

Démonstration :

- Comme $a \mid b$, il existe $k_1 \in \mathbb{Z}$ tel que $ak_1 = b$.
- En multipliant par c, on obtient $ack_1 = bc$.
- Donc, $a \mid bc$. □

Propriété : Soient $a, b, c \in \mathbb{Z}$. Si $a \mid b$ et $b \mid c$, alors $a \mid c$.

Démonstration :

- Comme $\begin{cases} a \mid b \\ b \mid c \end{cases}$, il existe $\begin{cases} k_1 \\ k_2 \end{cases} \in \mathbb{Z}$ tels que $\begin{cases} ak_1 = b \\ bk_2 = c \end{cases}$.
- En substituant b par ak_1 dans la seconde égalité, on obtient $ak_1k_2 = c$.
- Donc, $a \mid c$. □

Propriété : Soient $a, b, c \in \mathbb{Z}$. Si $a \mid b$ et $a \mid c$, alors $a \mid (sb + tc)$ pour tous $s, t \in \mathbb{Z}$.

Démonstration :

- Comme $\begin{cases} a \mid b \\ a \mid c \end{cases}$, on a, grâce à la première propriété, $\begin{cases} a \mid sb \\ a \mid tc \end{cases}$.
- Donc, il existe $\begin{cases} k_1 \\ k_2 \end{cases} \in \mathbb{Z}$ tels que $\begin{cases} ak_1 = sb \\ ak_2 = tc \end{cases}$.
- On obtient $a(k_1 + k_2) = sb + tc$.
- Donc, $a \mid (sb + tc)$. □

Combinaison linéaire

Définition : Un entier n est une *combinaison linéaire* des nombres $b_0, \ldots, b_k$ si et seulement si

$$n = s_0 b_0 + s_1 b_1 + \ldots + s_k b_k$$

pour des entiers $s_0, \ldots, s_k$.

Propriété : Soient $a, b \in \mathbb{Z}$. Pour tout $c \in \mathbb{Z}_0$, on a $(a \mid b) \Leftrightarrow (ca \mid cb)$.

Démonstration : Pour $c \neq 0$, on a successivement

$$\begin{aligned} & a \mid b \\ \Leftrightarrow \quad & (\exists k)\ ak = b \\ \Leftrightarrow \quad & (\exists k)\ cak = cb \\ \Leftrightarrow \quad & ca \mid cb. \end{aligned}$$

□

Division euclidienne

Théorème (division euclidienne) : Soient $n \in \mathbb{Z}$ et $d \in \mathbb{N}_0$. Il existe une unique paire $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ telle que

$$n = qd + r \text{ et } 0 \leq r < d.$$

(q est le *quotient* de la division, r est le *reste* de la division)

Exemple : $\underbrace{2716}_{n} = \underbrace{271}_{q} \cdot \underbrace{10}_{d} + \underbrace{6}_{r}$

Notation : Soient $n \in \mathbb{Z}$ et $d \in \mathbb{N}_0$. Le reste r de la division euclidienne de n par d est noté $n \bmod d$.
(n rem d dans le bouquin de référence)

Exemples :

- $32 \bmod 5 = 2$ car $32 = 6 \cdot 5 + 2$.
- $-11 \bmod 7 = 3$ car $-11 = (-2) \cdot 7 + 3$.

L'énigme des cruches

Données :

- une fontaine ;
- deux cruches non graduées et initialement vides, de contenances respectives de 3 et 6 litres.

Est-il possible de remplir l'une des cruches avec exactement 4 litres ?

Problème général

Théorème : Soient deux cruches non graduées et initialement vides, de contenances respectives $a, b \in \mathbb{N}$ litres. Après une suite quelconque d'opérations parmi

1. remplissage d'une cruche via la fontaine,
2. vidage d'une cruche dans la fontaine,
3. transvasement d'une cruche vers l'autre jusqu'à ce que l'une soit remplie ou que l'autre soit vide,

la quantité d'eau dans chaque cruche est toujours une combinaison linéaire de a et b, et au moins l'une des cruches est soit vide soit pleine.

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(n) =$ “Après n étapes la quantité d'eau dans chaque cruche est une combinaison linéaire de a et b, et au moins l'une des cruches est soit vide, soit pleine”.
- *Cas de base :* $P(0)$ est vrai car initialement les cruches sont tous les deux vides, et $0a + 0b = 0$.

- *Cas inductif :* Supposons que $P(n)$ soit vrai, et considérons la $(n+1)$ème étape.
  - Opération 1 ou 2 : une des deux cruches devient vide ou pleine, et les quantités restent des combinaisons linéaires de a et b.
  - Opération 3 :
    - Avant la $(n+1)$ème étape : soient $j_1 = s_1 a + t_1 b$ et $j_2 = s_2 a + t_2 b$ les quantités dans les cruches.
    - Après cette étape : l'une des cruches est soit vide (0), soit pleine (a ou b), et l'autre contient soit $j_1 + j_2$, soit $j_1 + j_2 - a$, soit $j_1 + j_2 - b$ litres.
  - Dans les trois cas, $P(n+1)$ est vrai.
- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}$. □

Corollaire : Il est impossible de mesurer 4 litres avec des cruches de 3 et 6 litres, car à tout moment les quantités d'eau ont la forme $3s + 6t$. Or, 4 n'est pas un multiple de 3.

Le plus grand commun diviseur

Le *plus grand commun diviseur (pgcd)* de $a, b \in \mathbb{Z}_0$ est le plus grand entier c tel que $c \mid a$ et $c \mid b$.

Pour $n \in \mathbb{Z}$, on définit $\text{pgcd}(0, n) = \text{pgcd}(n, 0) = n$.

Propriété : Si $b > 0$, alors $\text{pgcd}(a, b) = \text{pgcd}(a \bmod b, b)$.

Démonstration :

- Par le théorème de la division euclidienne, on a $a = qb + r$ avec $r = a \bmod b$.
- a est donc une combinaison linéaire de b et r, ce qui implique que tout diviseur de b et r est un diviseur de a (par la propriété du transparent 64).
- $r = a - qb$ est aussi une combinaison linéaire de a et b et donc tout diviseur de a et de b est aussi un diviseur de r.
- a et b ont donc les mêmes diviseurs que b et r et donc également le même plus grand commun diviseur. □

Algorithme d'Euclide

Cette propriété permet de calculer rapidement le pgcd de deux nombres.

Exemple :

$$
\begin{aligned}
\mathrm{pgcd}(1001, 777) &= \mathrm{pgcd}(\underbrace{1001 \bmod 777}_{=224}, 777) \\
&= \mathrm{pgcd}(\underbrace{777 \bmod 224}_{=105}, 224) \\
&= \mathrm{pgcd}(\underbrace{224 \bmod 105}_{=14}, 105) \\
&= \mathrm{pgcd}(\underbrace{105 \bmod 14}_{=7}, 14) \\
&= \mathrm{pgcd}(\underbrace{14 \bmod 7}_{=0}, 7) \\
&= 7.
\end{aligned}
$$

Propriétés

Théorème : Soient $a, b \in \mathbb{Z}_0$. On a $\text{pgcd}(a, b) =$ la plus petite combinaison linéaire strictement positive de a et b.

Démonstration :

- Soit m la plus petite combinaison linéaire strictement positive de a et b.
- $\boxed{\text{pgcd}(a, b) \leq m}$
  - On a $\text{pgcd}(a, b) \mid a$ et $\text{pgcd}(a, b) \mid b$.
  - Donc, $\text{pgcd}(a, b) \mid (sa + tb)$ pour tous $s, t \in \mathbb{Z}$.
  - En particulier, $\text{pgcd}(a, b) \mid m$, donc $\text{pgcd}(a, b) \leq m$.

- $\boxed{m \leq \text{pgcd}(a, b)}$
  - Montrons que $m \mid a$. Un raisonnement analogue permet de prouver que $m \mid b$. Ainsi, $m \leq \text{pgcd}(a, b)$.
  - Par le théorème de la division euclidienne, il existe q et r tels que $a = qm + r$, avec $0 \leq r < m$.
  - m s'écrit $m = sa + tb$ pour des entiers s et t.
  - On obtient $a = q(sa + tb) + r$, et donc $r = (1 - qs)a + (-qt)b$.
  - r est donc une combinaison linéaire positive de a et b.
  - Or, m est la plus petite combinaison linéaire strictement positive de a et b.
  - Donc, $r = 0$ et $m \mid a$. □

Deux corrolaires

Corrolaire 1 : Un entier n est une combinaison linéaire de a et b si et seulement si n est un multiple de $\text{pgcd}(a, b)$.

Corrolaire 2 : Soient deux cruches de capacités a et b. La quantité d'eau dans chaque cruche est toujours un multiple de $\text{pgcd}(a, b)$.

Le “pulvérisateur”

Algorithme pour calculer s et t tels que $sa + tb = \text{pgcd}(a, b)$.

Exemple : $\text{pgcd}(259, 70)$

a	b	$a \bmod b$	$=$	$a - q \cdot b$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

Résolution de l'énigme des cruches

Soient deux cruches de capacités a et b avec $a < b$. Soit un entier $0 < v < b$ multiple de $\text{pgcd}(a, b)$. La procédure suivante permet d'obtenir v litres dans la cruche la plus grande :

1. Calculer s et t tels que $v = s \cdot a - t \cdot b$ avec $s, t \geq 0$
2. Répéter s fois les deux étapes suivantes :
   - 2.1 remplir la cruche la plus petite
   - 2.2 déverser le contenu de la petite cruche dans la grande. Si la grande cruche est remplie, la vider et continuer à déverser le contenu de la petite dans la grande.

Exemple : $a = 5, b = 3, v = 4 = 3 \cdot 3 - 1 \cdot 5$

$(0/3, 0/5) \xrightarrow{1} (3/3, 0/5) \xrightarrow{2} (0/3, 3/5) \xrightarrow{1} (3/3, 3/5) \xrightarrow{2}$
$(0/3, 1/5) \xrightarrow{1} (3/3, 1/5) \xrightarrow{2} (0/3, 4/5)$

Pourquoi ça marche ?

(démonstration intuitive seulement)

- L'étape 1 est toujours possible (en utilisant le pulvérisateur)
- Au terme des s itérations des étapes 1.1 et 1.2 :
  - La cruche a a été remplie s fois
  - La cruche b a été vidée t fois exactement :
    - Si elle avait été vidée $t+1$ fois ou plus, on aurait $s \cdot a - (t+1) \cdot b = v - b < 0$ litres ou moins dans la cruche b, ce qui est impossible.
    - Si elle avait été vidée $t-1$ fois ou moins, on aurait $s \cdot a - (t-1) \cdot b = v + b > b$ litres ou plus dans la cruche b, ce qui est impossible.
- Il y a donc au final exactement $v = s \cdot a - t \cdot b$ litres dans la cruche b.

Propriétés du plus grand commun diviseur

Soient $a, b, c \in \mathbb{Z}_0$.

Propriété : Tout diviseur commun de a et b divise $\text{pgcd}(a, b)$.

Démonstration :

- Soient $s, t \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) = sa + tb$.
- Soit $d \in \mathbb{Z}$ tel que $d \mid a$ et $d \mid b$.
- On a $d \mid (sa + tb) = \text{pgcd}(a, b)$. □

Propriété : $\text{pgcd}(ka, kb) = k \cdot \text{pgcd}(a, b)$ pour tout $k \in \mathbb{N}_0$.

Démonstration :

- Soient $s, t \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) = sa + tb$.
- Soient $s', t' \in \mathbb{Z}$ tels que $\text{pgcd}(ka, kb) = s'ka + t'kb$.
- On a d'une part

$$\begin{aligned} \text{pgcd}(ka, kb) &= s'ka + t'kb \\ &= k(s'a + t'b) \quad \geq \quad k \cdot \text{pgcd}(a, b). \end{aligned}$$

- On a d'autre part

$$\begin{aligned} k \cdot \text{pgcd}(a, b) &= k(sa + tb) \\ &= s(ka) + t(kb) \quad \geq \quad \text{pgcd}(ka, kb). \end{aligned}$$

(par le théorème du transparent 75) □

Propriété : Si $\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1$, alors $\text{pgcd}(a, bc) = 1$.

Démonstration :

- Il existe $s, t \in \mathbb{Z}$ tels que $\text{pgcd}(a, b) = sa + tb = 1$.
- Il existe $s', t' \in \mathbb{Z}$ tels que $\text{pgcd}(a, c) = s'a + t'c = 1$.
- Dès lors, on a

$$\begin{aligned}(sa + tb)(s'a + t'c) &= 1 \\ &= (ass' + cst' + bs't)a + (tt')bc,\end{aligned}$$

  qui est une combinaison linéaire de a et bc.
- Donc, $\text{pgcd}(a, bc) = 1$. □

Propriété : Si $a \mid bc$ et $\text{pgcd}(a, b) = 1$, alors $a \mid c$.

Démonstration :

- On a $a \mid ac$ et $a \mid bc$.
- Donc, a divise toutes les combinaisons linéaires de ac et de bc.
- En particulier, on a $a \mid \text{pgcd}(ac, bc)$.
- Or, $\text{pgcd}(ac, bc) = c \cdot \text{pgcd}(a, b) = c$.
- Donc, $a \mid c$. □

Théorème fondamental de l'arithmétique

Lemme : Soit p un nombre premier, et $a, b \in \mathbb{Z}$. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Démonstration : Les seuls diviseurs de p sont 1 et p. Donc, $\text{pgcd}(a, p) = 1$ ou $\text{pgcd}(a, p) = p$.

- Si $\text{pgcd}(a, p) = p$, on a $p \mid a$.
- Si $\text{pgcd}(a, p) = 1$, on a $p \mid b$ grâce à la propriété du transparent 84. □

Corollaire : Soit p un nombre premier, et $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Si $p \mid a_1 a_2 \ldots a_n$, alors p divise un des a_i.

Théorème fondamental de l'arithmétique : Tout nombre $n \in \mathbb{N}_0$ peut être écrit de façon unique comme un produit de nombres premiers $n = p_1 p_2 \dots p_j$.

Démonstration :

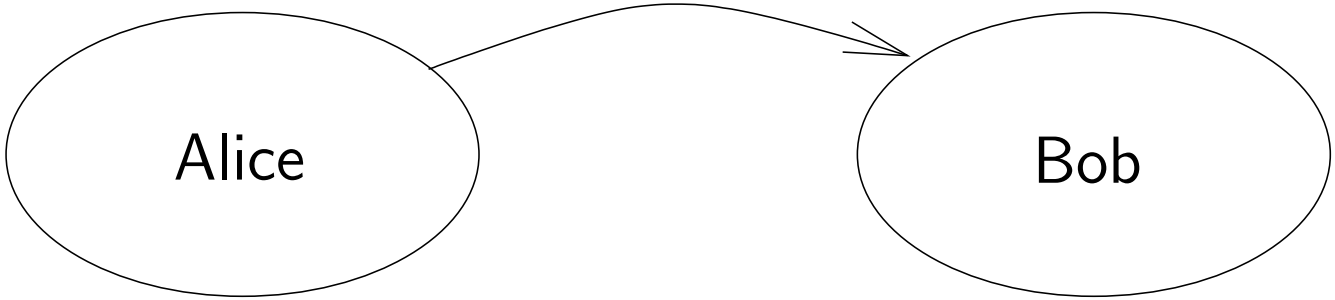
Tout $n \in \mathbb{N}_0$ s'écrit comme un produit de nombres premiers.

- La démonstration fonctionne par induction forte.
- $P(n) =$ "n s'écrit comme un produit de nombres premiers".
- *Cas de base :* $P(1)$ est vrai car il s'écrit comme le produit d'un ensemble vide de nombres premiers.
- *Cas inductif :* Supposons $P(1) \wedge P(2) \wedge \dots \wedge P(n)$.
  - Si $n+1$ est premier, $P(n+1)$ est vrai.
  - Sinon, $n+1 = ab$, avec $2 \leq a, b \leq n$.
  - Par induction, a et b sont des produits de nombres premiers. Donc, $P(n+1)$ est vrai.
- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}_0$.

Cette écriture est unique.

- Par l'absurde, supposons qu'il existe un $n \in \mathbb{N}_0$ qui s'écrive de plusieurs façons comme produit de nombres premiers.
- Considérons le plus petit n possible.
- Soient $n = p_1 p_2 \dots p_j = q_1 q_2 \dots q_k$ deux de ces écritures.
- On a $p_1 \mid n$ et donc $p_1 \mid q_1 q_2 \dots q_k$.
- p_1 divise au moins un des nombres premiers q_i.
- Comme p_1 et q_i sont premiers, on doit avoir $p_1 = q_i$.
- En supprimant p_1 du premier produit et q_i du second, on obtient que $\frac{n}{p_1} < n$. Or, $\frac{n}{p_1} \in \mathbb{N}$ et s'écrit comme un produit de nombres premiers de plusieurs façons.
- C'est une contradiction avec le choix de n, donc l'écriture est unique. □

Code de Turing (version 1)



Principes :

- Soit m le message qu'Alice doit envoyer à Bob. Le message m doit être encodé sous la forme d'un nombre premier.
  Exemple d'encodage : A=01, B=02, C=03, ...

v	i	c	t	o	r	y	
22	09	03	20	15	18	25	13

- Alice et Bob ont en commun une *clé secrète*, qui est un grand nombre premier p.
- Alice crypte le message m en calculant

$$m' = mp,$$

  et l'envoie à Bob.
- Bob décrypte m' en calculant

$$\frac{m'}{p} = \frac{mp}{p} = m.$$

Exemple : Supposons que la clé secrète soit le nombre premier 22801763489 et que le message à envoyer soit "victory". Le message crypté est

$$\begin{aligned} m' &= mp \\ &= 2209032015182513 \cdot 22801763489 \\ &= 50369825549820718594667857. \end{aligned}$$

Problème : Comment peut-on s'assurer que m et p soient des nombres premiers ?

Solution : Il existe des algorithmes permettant de tester si un nombre est premier. Notamment, un algorithme de Agrawal, Kayal et Saxena (2002) permet de tester si n est premier en approximativement $(\log n)^{12}$ étapes.

Question : Le code de Turing est-il sécurisé ?

Réponse : Si $m' = mp$ est intercepté, il faut le factoriser pour trouver m. La factorisation étant un problème difficile, il est très difficile de trouver m (et p), pour autant qu'ils soient suffisamment grands.

Problème : Il reste tout de même un défaut de conception majeur dans le code de Turing.

Cassage du code de Turing

- Si les messages m_1 et m_2 doivent être envoyés grâce à la clé secrète p, Alice calcule les messages cryptés $m'_1 = m_1 p$ et $m'_2 = m_2 p$, et les envoie à Bob.
- Si m'_1 et m'_2 sont interceptés, la clé p peut être calculée par $\text{pgcd}(m'_1, m'_2)$, et les messages m_1 et m_2 peuvent alors être retrouvés par $m_1 = \dfrac{m'_1}{p}$ et $m_2 = \dfrac{m'_2}{p}$.

Arithmétique modulaire

Définition : Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}_0$. On dit que *a et b sont congrus modulo c* si $c \mid (a - b)$. On note cela $a \equiv b \pmod{c}$.

Exemples :

- $29 \equiv 15 \pmod{7}$ car $7 \mid (29 - 15)$.
-

$\#$:	$\ldots$	-4	-3	-2	-1	0	1	2	3	4	5	$\ldots$
$\#$ mod 3 :	$\ldots$	2	0	1	2	0	1	2	0	1	2	$\ldots$

- Définit une partition des entiers en n ensembles :

$$\begin{array}{lllllllll} \{ & \ldots, & -6, & -3, & 0, & 3, & 6, & 9, & \ldots \} \\ \{ & \ldots, & -5, & -2, & 1, & 4, & 7, & 10, & \ldots \} \\ \{ & \ldots, & -4, & -1, & 2, & 5, & 8, & 11, & \ldots \} \end{array}$$

Lemme : Soient $a, b \in \mathbb{Z}$ et $c \in \mathbb{N}_0$. On a

$$a \equiv b \pmod{c} \Leftrightarrow (a \bmod c) = (b \bmod c).$$

Démonstration :

- Par le théorème de division euclidienne, il existe des uniques paires $(q_1, r_1), (q_2, r_2) \in \mathbb{Z} \times \mathbb{Z}$ telles que
  - $a = q_1 c + r_1$ (avec $0 \leq r_1 < c$) (1)
  - $b = q_2 c + r_2$ (avec $0 \leq r_2 < c$) (2)
- En soustrayant (2) de (1), on obtient $a - b = (q_1 - q_2)c + (r_1 - r_2)$, avec $-c < r_1 - r_2 < c$.
- Comme $-c < r_1 - r_2 < c$, on a

$$\begin{aligned} a \equiv b \pmod{c} &\Leftrightarrow c \mid (a - b) \\ &\Leftrightarrow c \mid (r_1 - r_2) \\ &\Leftrightarrow r_1 = r_2. \end{aligned}$$

- On conclut grâce à $(a \bmod c) = r_1$ et $(b \bmod c) = r_2$. □

Remarque : Plusieurs propriétés de l'arithmétique sur les entiers sont valables en arithmétique modulaire, mais ce n'est pas toujours le cas.

Exemples :

- Soient $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}_0$.
  - $a \equiv b \pmod{n}$ implique $a + c \equiv b + c \pmod{n}$.
  - $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ implique $a \equiv c \pmod{n}$.
- En arithmétique, $ac = bc$ implique $a = b$ (si $c \neq 0$). Ce n'est pas le cas en arithmétique modulaire : $2 \cdot 3 \equiv 4 \cdot 3 \pmod{6}$ mais $2 \not\equiv 4 \pmod{6}$.

Propriétés de l'arithmétique modulaire

Soient $k, n \in \mathbb{N}_0$, et $a, a_1, b_1, a_2, b_2, \ldots, a_k, b_k \in \mathbb{Z}$.

Propriété : Si $a_1 \equiv b_1 \pmod{n}$ et si $a_2 \equiv b_2 \pmod{n}$, alors

1. $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$,
2. $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Démonstration de 2 :
On a $n \mid (a_1 - b_1)$ et $n \mid (a_2 - b_2)$. Par la propriété du transparent 64, on obtient

$$n \mid (a_2(a_1 - b_1) + b_1(a_2 - b_2)),$$

ce qui se simplifie en $n \mid (a_1 a_2 - b_1 b_2)$. □

Propriété : Si pour tout i tel que $1 \leq i \leq k$ on a $a_i \equiv b_i \pmod{n}$, alors $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{n}$.

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(k) =$ "Si pour tout i tel que $1 \leq i \leq k$ on a $a_i \equiv b_i \pmod{n}$, alors $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{n}$".
- *Cas de base :* $P(1)$ est vrai.
- *Cas inductif :*
  - Supposons que $P(k)$ soit vrai.
  - Supposons que pour tout i tel que $1 \leq i \leq k+1$ on ait $a_i \equiv b_i \pmod{n}$.
  - On a $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{n}$.
  - Comme $a_{k+1} \equiv b_{k+1} \pmod{n}$, $P(k+1)$ est vrai grâce à la propriété précédente.
- Par induction, $P(k)$ est vrai pour tout $k \in \mathbb{N}_0$. □

Propriété : $(a \bmod n) \equiv a \pmod{n}$.

Démonstration : $a \bmod n$ est égal à $a - qn$ pour un certain quotient $q \in \mathbb{Z}$. On a successivement

$$\begin{aligned} n \mid qn &\Rightarrow n \mid (a - (a - qn)) \\ &\Rightarrow n \mid (a - (a \bmod n)) \\ &\Rightarrow (a \bmod n) \equiv a \pmod{n}. \end{aligned}$$

□

Propriété : $\prod_{i=1}^{k} (a_i \bmod n) \equiv \prod_{i=1}^{k} a_i \pmod{n}$.

Démonstration : Pour tout i tel que $1 \leq i \leq k$, on a $(a_i \bmod n) \equiv a_i \pmod{n}$ grâce à la propriété précédente. La conclusion découle de la propriété du transparent 96. □

Code de Turing (version 2)

Principes :

- Alice et Bob ont en commun
  - un grand nombre premier p, qui peut être public, et
  - une clé secrète $k \in \{1, 2, \ldots, p-1\}$.
- Le message m est supposé être un nombre de l'ensemble $\{1, 2, \ldots, p-1\}$. Alice l'encrypte en calculant

$$m' = mk \bmod p, \qquad (*)$$

  et l'envoie à Bob.
- Bob décrypte m' en trouvant un message m qui respecte l'égalité $(*)$.

Problèmes : Comment effectuer l'opération de décryptage ?

Simplification modulo un nombre premier

Lemme : Supposons que p soit un nombre premier et que k ne soit pas un multiple de p. Si

$$ak \equiv bk \pmod{p},$$

alors

$$a \equiv b \pmod{p}.$$

Démonstration :

- Si $ak \equiv bk \pmod{p}$, alors $p \mid (ak - bk)$. On a donc $p \mid k(a - b)$.
- Donc, $p \mid k$ ou $p \mid (a - b)$.
- Comme k n'est pas un multiple de p, on a $p \mid (a - b)$, ce qui implique $a \equiv b \pmod{p}$. □

Messages cryptés identiques

- Soient a, b deux messages.
- Les messages encryptés sont identiques si et seulement si $(ak \bmod p) = (bk \bmod p)$, c'est-à-dire si $ak \equiv bk \pmod{p}$.
- Comme k n'est pas un multiple de p ($k \in \{1, 2, \ldots, p-1\}$), cela se produit exactement lorsque $a \equiv b \pmod{p}$.
- Comme $a, b \in \{1, 2, \ldots, p-1\}$, cela signifie $a = b$.

Conclusion : Deux messages cryptés représentent le même message non-crypté si et seulement s'ils sont identiques.

Corollaire : Supposons que p soit un nombre premier et que k ne soit pas multiple de p. La séquence

$$(0k) \bmod p,\ (1k) \bmod p,\ (2k) \bmod p,\ \ldots,\ ((p-1)k) \bmod p$$

est une permutation de la séquence

$$0,\ 1,\ 2,\ \ldots,\ p-1.$$

Démonstration :

- Chacun des p nombres de la première séquence appartient à $\{0, 1, \ldots, p-1\}$.
- Par le lemme précédent, et comme $(ak \bmod p) = (bk \bmod p) \Leftrightarrow ak \equiv bk \pmod p$, la première séquence contient tous les nombres de 0 à $p-1$ dans un ordre donné. □

Inverses multiplicatifs

Tout $x \in \mathbb{R}_0$ admet un inverse multiplicatif x^{-1} tel que $x \cdot x^{-1} = 1$.

Cependant, la plupart des nombres entiers n'admettent pas d'inverses multiplicatifs dans $\mathbb{Z}$ (seul 1 et -1 ont un inverse).

Exemple : L'inverse multiplicatif de 5 est $\frac{1}{5}$, qui n'est pas entier.

Dans une arithmétique modulo un nombre premier p, la plupart des entiers admettent un inverse multiplicatif.

Exemple : $5 \cdot 9 \equiv 1 \pmod{11}$.

Théorème : Soit p un nombre premier. Si $k \in \mathbb{Z}$ n'est pas un multiple de p, alors il existe $k^{-1} \in \{1, 2, \ldots, p-1\}$ tel que $k \cdot k^{-1} \equiv 1 \pmod{p}$.

Démonstration :

- Lorsque m varie dans $\{1, 2, \ldots, p-1\}$, l'expression $(mk \bmod p)$ prend toutes les valeurs de $\{1, 2, \ldots, p-1\}$.
- En particulier, $(mk \bmod p) = 1$ pour un m donné, et donc $\underbrace{m}_{k^{-1}} k \equiv 1 \pmod{p}$. □

Application : Pour décoder un message crypté m' obtenu à partir d'un message m par le code Turing (version 2) en utilisant la clé secrète k, il suffit de multiplier m' par k^{-1}. En effet,

$$\begin{aligned} m'k^{-1} \bmod p &\equiv m'k^{-1} \pmod{p} \\ &\equiv (mk \bmod p)k^{-1} \pmod{p} \\ &\equiv mkk^{-1} \pmod{p} \\ &\equiv m \pmod{p}. \end{aligned}$$

Calcul d'inverses

Autre démonstration du théorème du transparent 103 :

- Puisque p est premier, il a seulement deux diviseurs : 1 et p. Puisque k n'est pas un multiple de p, on doit avoir $\text{pgcd}(k, p) = 1$.
- Par la caractérisation du pgcd, on sait qu'il existe s, t tels que $\text{pgcd}(k, p) = 1 = sk + tp$.
- Dès lors, on a $tp = 1 - sk$, ce qui implique $p|(1 - sk)$.
- Par la définition de la congruence, on en déduit $\underbrace{s}_{k^{-1}} k \equiv 1 \pmod{p}$. □

Calcul d'inverses avec le pulvérisateur

Par la démonstration précédente, on peut donc obtenir un inverse multiplicatif s de $k \pmod p$ en utilisant le pulvérisateur pour calculer une décomposition $\text{pgcd}(k, p) = sk + tp$. L'algorithme demande $O(\log(p))$ opérations.

Exemple : $p = 17$ et $k = 6$

a	b	$a \bmod b$	$=$	$a - q \cdot b$
17	6	5	$=$	$17 - 2 \cdot 6$
6	5	1	$=$	$6 - 1 \cdot 5$
			$=$	$6 - 1 \cdot (17 - 2 \cdot 6)$
			$=$	$-1 \cdot 17 + \boxed{3} \cdot 6$

$\Rightarrow$ l'inverse multiplicatif de $6 \pmod{17}$ est 3 :

$$3.6 \equiv 1 \pmod{17}.$$

Théorème de Fermat

(Petit) Théorème de Fermat : Supposons que p soit un nombre premier et que k ne soit pas un multiple de p. Alors, $k^{p-1} \equiv 1 \pmod{p}$.

Démonstration :

$$\begin{aligned} & 1 \cdot 2 \cdots (p-1) \\ \equiv\ & (k \bmod p) \cdot (2k \bmod p) \cdots ((p-1)k \bmod p) \pmod{p} \\ \equiv\ & k \cdot 2k \cdots ((p-1)k) \pmod{p} \\ \equiv\ & (p-1)! \cdot k^{p-1} \pmod{p}. \end{aligned}$$

$(p-1)!$ n'est pas un multiple de p car p est premier et ne divise ni 1, ni 2, ..., ni $p-1$. Donc, on peut simplifier par $(p-1)!$. □

Calcul d'inverses avec le théorème de Fermat

Supposons que p soit un nombre premier et que k ne soit pas un multiple de p.

Par le théorème de Fermat, on a $k^{p-2}k \equiv 1 \pmod{p}$. Le nombre k^{p-2} est donc un inverse multiplicatif de k.

Exemple de calcul (logarithmique en temps) : Si l'on veut calculer l'inverse multiplicatif de 6 modulo 17, il suffit de calculer $6^{15} \pmod{17}$: (toutes les congruences qui suivent sont modulo 17)

$$6^2 \equiv 36 \equiv 2$$

$$6^4 \equiv (6^2)^2 \equiv 2^2 \equiv 4$$

$$6^8 \equiv (6^4)^2 \equiv 4^2 \equiv 16$$

$$6^{15} \equiv 6^8 \cdot 6^4 \cdot 6^2 \cdot 6 \equiv 16 \cdot 4 \cdot 2 \cdot 6 \equiv 3$$

Vérification : $3 \cdot 6 \equiv 1 \pmod{17}$.

Cassage du code de Turing

A l'aide d'une paire (message, message encrypté), et du nombre p, il est possible de retrouver la clé k.

Supposons que l'on connaisse m et m', qui satisfont l'égalité $m' = (mk \bmod p)$.

On a

$$\begin{aligned} m^{p-2}m' &\equiv m^{p-2}mk \pmod{p} \\ &\equiv m^{p-1}k \pmod{p} \\ &\equiv k \pmod{p}. \end{aligned}$$

Arithmétique avec des modulo arbitraires

Le code de Turing (version 2) est basé sur une arithmétique modulo un nombre *premier* p.

Le RSA (algorithme de cryptographie à *clé publique*) fonctionne en arithmétique modulo le produit de *deux* grands nombres premiers.

Définition : Les nombres $a, b \in \mathbb{Z}_0$ sont *premiers entre eux* si $\text{pgcd}(a, b) = 1$.

Exemple : 8 et 15 sont premiers entre eux.

Inverses multiplicatifs et modulo arbitraires

Lemme : Soit $n \in \mathbb{N}_0$. Si $k \in \mathbb{Z}_0$ est premier avec n, alors il existe $k^{-1} \in \mathbb{Z}$ tel que $k \cdot k^{-1} \equiv 1 \pmod{n}$.

Démonstration :

- Il existe $s, t \in \mathbb{Z}$ tels que $sk + tn = \text{pgcd}(k, n) = 1$.
- Dès lors on a $tn = 1 - sk$, ce qui implique $n \mid (1 - sk)$.
- On en déduit $\underbrace{s}_{k^{-1}} k \equiv 1 \pmod{n}$. □

Corollaire : Soit $n \in \mathbb{N}_0$, et soit $k \in \mathbb{Z}$ premier avec n. Si $ak \equiv bk \pmod{n}$, alors $a \equiv b \pmod{n}$.

Démonstration : Il suffit de multiplier à droite et à gauche par k^{-1}. □

Lemme

Lemme : Soient $n \in \mathbb{N}_0$ et $k \in \mathbb{Z}_0$ premier avec n. Soit $\{k_1, k_2, \ldots, k_r\}$ l'ensemble des entiers (distincts) de l'intervalle $\{0, 1, \ldots, n-1\}$ qui sont premiers avec n. La séquence

$$(k_1 k) \bmod n,\ (k_2 k) \bmod n,\ \ldots,\ (k_r k) \bmod n$$

est une permutation de la séquence

$$k_1,\ k_2,\ \ldots,\ k_r.$$

Démonstration :

Les nombres de la première séquence sont tous distincts

- Soient $i, j \in \{1, 2, \ldots, r\}$ tels que $((k_i k) \bmod n) = ((k_j k) \bmod n)$.
- On a $k_i k \equiv k_j k \pmod{n}$, ce qui implique $k_i \equiv k_j \pmod{n}$ car k est premier avec n.
- On en déduit $k_i = k_j$ car $k_i, k_j \in \{0, 1, \ldots, n-1\}$.

Tout nombre de la première séquence apparaît dans la deuxième

- Soit $i \in \{1, 2, \ldots, r\}$.
- On a $\text{pgcd}(k_i, n) = 1$ et $\text{pgcd}(k, n) = 1$.
- Par la propriété du transparent 83, on a $\text{pgcd}(k_i k, n) = 1$.
- Par la propriété du transparent 73, on obtient $\text{pgcd}(k_i k \bmod n, n) = 1$.
- Donc, $k_i k \bmod n \in \{0, 1, \ldots, n-1\}$ est premier avec n.
- On en déduit que $k_i k \bmod n$ apparaît dans la deuxième séquence. □

Fonction indicatrice d'Euler

Définition : Soit $n \in \mathbb{N}_0$. La *fonction indicatrice d'Euler* $\phi(n)$ désigne le nombre d'entiers de $\{1, 2, \ldots, n-1\}$ qui sont premiers avec n.

Exemples :

- $\phi(7) = 6$ car 1, 2, 3, 4, 5, et 6 sont premiers avec 7.
- $\phi(12) = 4$, car seuls 1, 5, 7 et 11 sont premiers avec 12.

Théorème d'Euler : Soient $n \in \mathbb{N}_0$ et $k \in \mathbb{Z}_0$ premier avec n. On a $k^{\phi(n)} \equiv 1 \pmod{n}$.

Démonstration :

- Soit $\{k_1, k_2, \ldots, k_r\}$ l'ensemble des entiers (distincts) de l'intervalle $\{0, 1, \ldots, n-1\}$ qui sont premiers avec n.
- Par définition de $\phi(n)$, on a $r = \phi(n)$.
- On a successivement

$$\begin{aligned} & k_1 k_2 \ldots k_r \\ \equiv\ & (k_1 k \bmod n)(k_2 k \bmod n) \ldots (k_r k \bmod n) \pmod{n} \\ \equiv\ & (k_1 k)(k_2 k) \ldots (k_r k) \pmod{n} \\ \equiv\ & (k_1 k_2 \ldots k_r) k^r \pmod{n}. \end{aligned}$$

- $k_1 k_2 \ldots k_r$ est premier avec n grâce à la propriété du transparent 83. On peut donc simplifier par $k_1 k_2 \ldots k_r$.
- On obtient $k^{\phi(n)} \equiv 1 \pmod{n}$. □

Calcul d'inverse

- Le théorème d'Euler permet de calculer l'inverse d'un entier k premier avec n :

$$k^{-1} = k^{\phi(n)-1}.$$

- Le calcul demande cependant de calculer d'abord $\phi(n)$, ce qui n'est pas trivial

.

Propriétés de la fonction d'Euler

Théorème :

$$\phi(pq) = (p-1)(q-1)$$

pour des premiers $p \neq q$.

Démonstration :

- Puisque p et q sont premiers, tout nombre qui n'est pas premier avec pq est soit un multiple de p, soit un multiple de q.
- Dans $\{0, 1, \ldots, pq-1\}$, il y a q multiples de p et p multiple de q et seul 0 est un multiple de p et de q.
- Il y a donc $p+q-1$ nombres dans $\{0, 1, \ldots, pq-1\}$ qui ne sont pas premiers avec pq et on a :

$$\begin{aligned} \phi(pq) &= pq - (p+q-1) \\ &= (p-1)(q-1). \end{aligned}$$

□

Propriétés de la fonction d'Euler

Théorème :

1. Si $a, b \in \mathbb{N}_0$ sont premiers entre eux, alors $\phi(ab) = \phi(a)\phi(b)$. (admis)
2. Si p est un nombre premier, alors $\phi(p^k) = p^k - p^{k-1}$ pour tout $k \in \mathbb{N}_0$.

Démonstration de 2 :

- Chaque p-ème nombre parmi les p^k nombres dans $\{0, 1, \ldots, p^k - 1\}$ est divisible par p et ce sont les seuls.
- On a donc $1/p$ des nombres entre 0 et p^k qui sont divisibles par p, les autres ne l'étant pas :

$$\phi(p^k) = p^k - \frac{1}{p}p^k = p^k - p^{k-1}.$$

En connaissant la factorisation de $n \in \mathbb{N}_0$, la nombre $\phi(n)$ se calcule aisément grâce au théorème précédent.

Exemple : $300 = 2^2 \cdot 3 \cdot 5^2$ et

$$\begin{aligned}
\phi(300) &= \phi(2^2 \cdot 3 \cdot 5^2) \\
&= \phi(2^2) \cdot \phi(3) \cdot \phi(5^2) \\
&= \underbrace{(2^2 - 2^1)}_{2}\underbrace{(3^1 - 3^0)}_{2}\underbrace{(5^2 - 5^1)}_{20} \\
&= 80
\end{aligned}$$

Note :

- Factoriser n n'est pas un problème facile
- Par le théorème du transparent 112, le pulvérisateur permet aussi de calculer k^{-1} comme le coefficient de k dans le calcul de $\text{pgcd}(k, n)$.

RSA (Rivest Shamir Adleman)

Préparation (au niveau du récepteur) :

- Générer des entiers premiers p,q et définir $n = p \cdot q$.
- Choisir e tel que $\text{pgcd}(e, (p-1)(q-1)) = 1$. La *clé publique* est la paire (e, n) qui doit être distribuée.
- Calculer d tel que $de \equiv 1 \pmod{(p-1)(q-1)}$. La *clé secrète* est la paire (d, n).

Encodage d'un message m $(0 \leq m < n)$:

- Encoder le message avec un entier m tel que $\text{pgcd}(m, n) = 1$.
- Le destinateur code alors son message comme suit :

$$m' = m^e \bmod n.$$

Décodage de m' :

- Le récepteur décode le message en calculant :

$$m = m'^d \bmod n.$$

Exemple

Soient $p = 13$, $q = 7$ ($n = pq = 91$) et $e = 5$ ($\text{pgcd}((13-1)(7-1), 5) = 1$).

Décoder le message $m' = 2$.

Mise en œuvre pratique

- Trouver deux (grands) premiers p et q
  - Il existe beaucoup de premiers
  - Il existe des tests rapide de primalité
- Trouver e tel que $\text{pgcd}(e, (p-1)(q-1)) = 1$
  - Il est existe beaucoup de premiers avec $(p-1)(q-1)$
  - Le pgcd est facile à calculer (algorithme d'Euclide par exemple)
- Trouver l'inverse de e modulo $(p-1)(q-1)$
  - Facile avec le pulvérisateur ou Euler
- Encodage/décodage
  - Facile en utilisant l'exponentiation rapide

Pourquoi ça marche ?

Lemme : Soient p et q tels que $\text{pgcd}(p, q) = 1$. Si $a \equiv b \pmod{p}$ et $a \equiv b \pmod{q}$, alors $a \equiv b \pmod{pq}$.

Démonstration :

- Si $a \equiv b \pmod{p}$ et $a \equiv b \pmod{q}$, on a par définition $p|(a - b)$ et $q|(a - b)$.
- p et q étant premiers entre eux, on a donc $pq|(a - b)$ et donc $a \equiv b \pmod{pq}$.

Pourquoi ça marche ?

Nous devons montrer que

$$m = (m')^d \bmod n = (m^e \bmod n)^d \bmod n.$$

Démonstration :

- Par la deuxième propriété du transparent 97, il suffit de démontrer que

$$m = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n.$$

- On va démontrer que $m \equiv m^{ed} \pmod{p}$. Par symétrie, on aura $m \equiv m^{ed} \pmod{q}$ et par le lemme précédent $m \equiv m^{ed} \pmod{n}$.
- Comme $m \in \{0, 1, \ldots, n-1\}$, on aura démontré que :

$$m = m^{ed} \bmod n.$$

Montrons que $m \equiv m^{ed} \pmod{p}$

- Puisque $ed \equiv 1 \pmod{(p-1)(q-1)}$, on a $(p-1)(q-1) | (ed-1)$ et donc il existe un entier k tel que $(ed-1) = k(p-1)$.
- On a

$$\begin{aligned} m^{ed} &\equiv m^{ed-1+1} \pmod{p} \\ &\equiv (m^{ed-1}).m \pmod{p} \\ &\equiv (m^{k(p-1)}).m \pmod{p}. \end{aligned}$$

- Comme p est premier, soit $\text{pgcd}(m, p) = 1$, soit $\text{pgcd}(m, p) = p$.

- Si $\text{pgcd}(m, p) = 1$:
  - Par le petit théorème de Fermat, on a $m^{p-1} \equiv 1 \pmod{p}$ et donc $m^{k(p-1)} \equiv 1^k \equiv 1 \pmod{p}$
  - Finalement, on a

$$m^{ed} \equiv 1 \cdot m \equiv m \pmod{p}.$$

- Si $\text{pgcd}(m, p) = p$:
  - $m = kp$ et donc $m^{ed} = k'p$ et $m^{ed} \equiv 0 \pmod{p}$
  - Or $m \equiv 0 \pmod{p}$
  - D'où $m^{ed} \equiv m \pmod{p}$.

□

Sécurité

- Casser ce code est facile si on peut factoriser n en un produit pq où p et q sont premiers.
- On peut alors trouver d à partir de e et $(p-1)(q-1)$ par le pulvérisateur.
- Il n'existe cependant pas de méthode efficace pour faire ça.
- RSA n'a toujours pas été cassé en 30 ans.

Chapitre 4

Théorie des graphes

Introduction

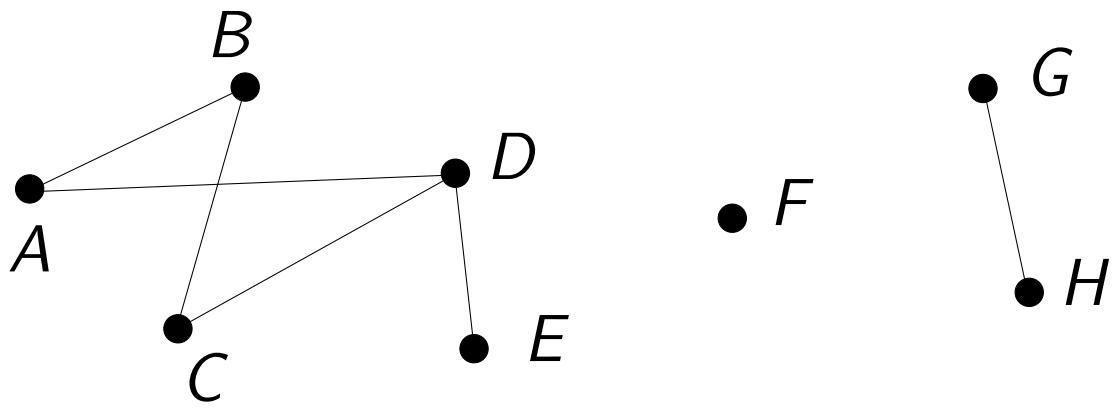
Définition : Un *graphe* est une paire $G = (V, E)$ où

- V est un ensemble fini mais non vide de *sommets*,
- E est un ensemble d'*arêtes*, chacune d'entre-elles étant un ensemble de deux sommets.

Remarques : Les sommets sont parfois appelés des *nœuds* et les arêtes des *arcs*.

Exemple :

- $V = \{A, B, C, D, E, F, G, H\}$
- $E = \{\{A, B\}, \{A, D\}, \{B, C\}, \{C, D\}, \{D, E\}, \{G, H\}\}$

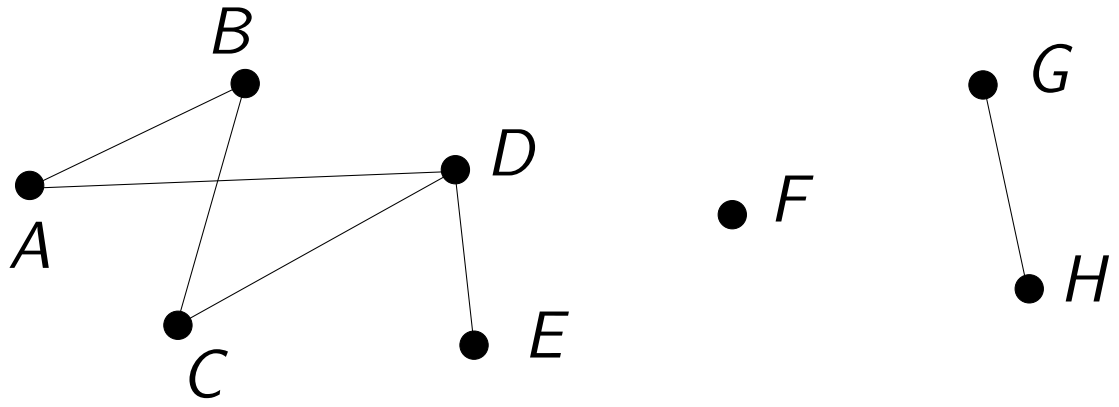


Notation : L'arête $\{A, B\} = \{B, A\}$ pourra être dénotée par A—B ou par B—A.

Définitions : Dans un graphe $G = (V, E)$,

- deux sommets $A, B \in V$ sont *adjacents* s'ils sont reliés par une arête, i.e, si A—$B \in E$;
- une arête A—B est *incidente* aux sommets A et B ;
- le *degré* d'un sommet est le nombre d'arêtes qui lui sont incidentes.

Exemple :



- A et B sont adjacents ;
- l'arête B—C est incidente à B et à C ;
- le degré de A est 2 ;
- le degré de D est 3 ;
- le degré de F est 0 ;
- le degré de G est 1.

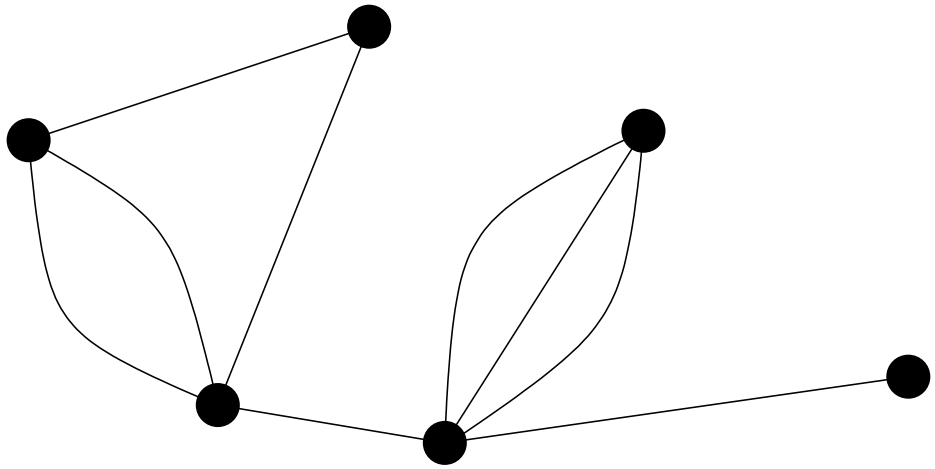
Sous-graphes

Définition : Soit un graphe $G = (V, E)$. Le graphe $G' = (V', E')$ est un *sous-graphe* de G si les conditions suivantes sont réunies :

- $V' \subseteq V$ et $V' \neq \emptyset$;
- $E' \subseteq E$;
- les sommets composant les arêtes de E' doivent appartenir à V'.

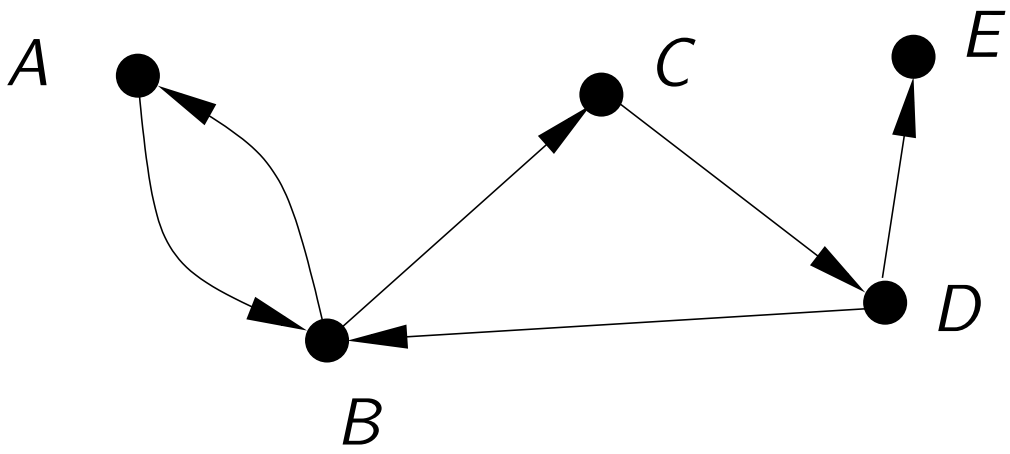
Extensions des graphes

Multigraphes : Une paire de sommets peut être connectée par *plus d'une arête*.



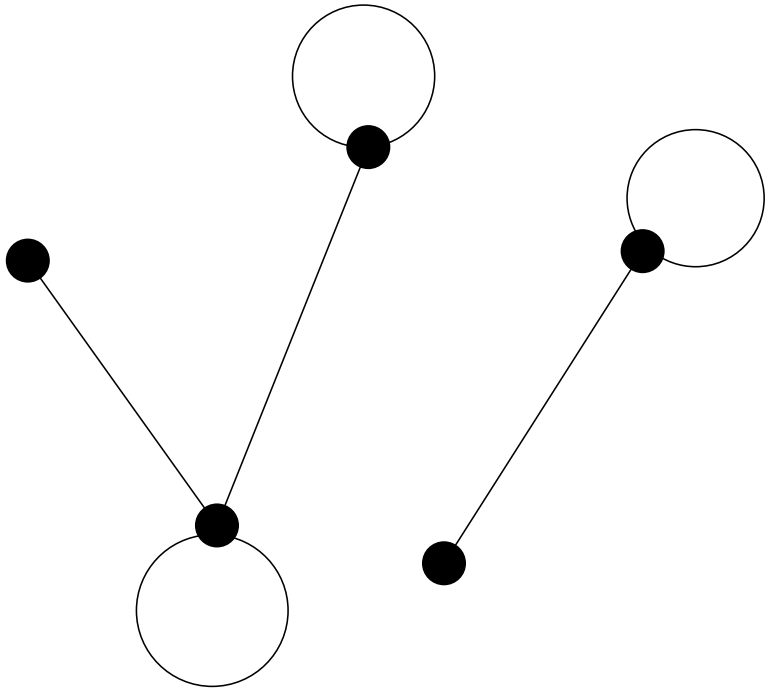
Graphes dirigés :

- Les arêtes sont des paires *ordonnées* de sommets.
- Une arête partant du sommet A et allant au sommet B est dénotée $A \longrightarrow B$.
- Le *degré intérieur* d'un sommet est le nombre d'arêtes arrivant à ce sommet.
- Le *degré extérieur* d'un sommet est le nombre d'arêtes sortant de ce sommet.



Le degré intérieur de D est 1 ; son degré extérieur est 2.

Boucles : On peut autoriser qu'un graphe contienne des boucles, c'est-à-dire qu'une arête ait pour extrémités le même sommet.



Notes :

- Des combinaisons sont possibles.
- Sauf lorsque cela sera spécifié expressément, un graphe sera toujours “simple” :
  - arêtes non dirigées,
  - pas de boucles,
  - au plus une arête entre deux sommets.

Applications

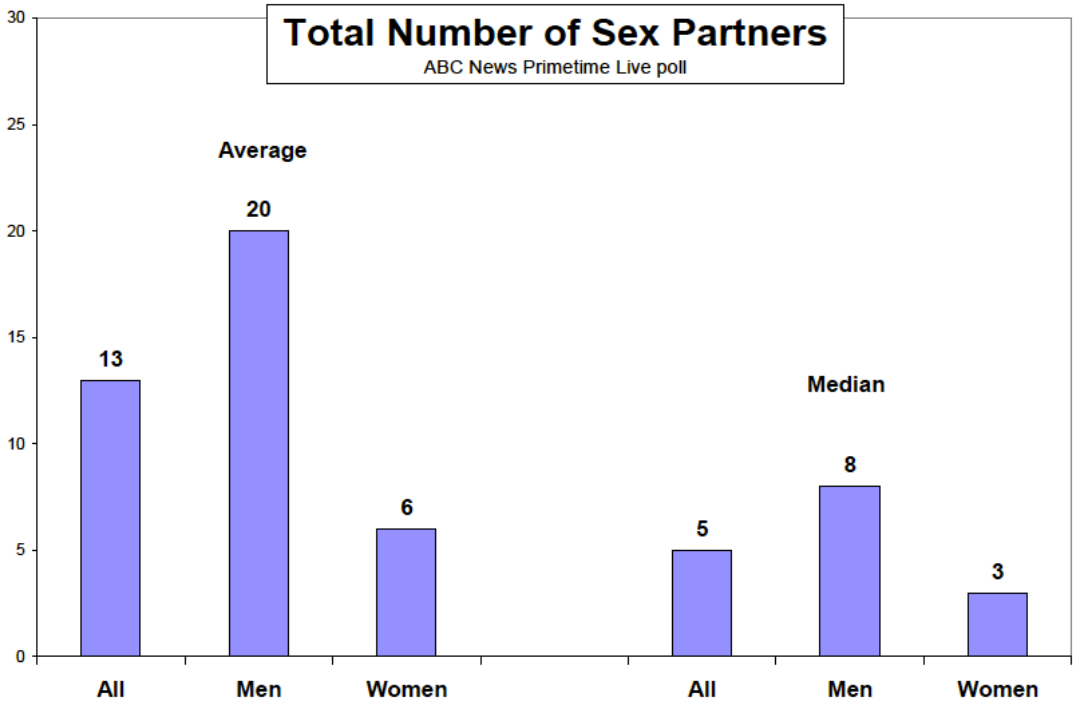
Les graphes peuvent être utilisés pour modéliser une grande variété de problèmes.

Exemples :

- cartes routières,
- connexions aériennes,
- WWW,
- réseaux sociaux,
- structures de données,
- etc.

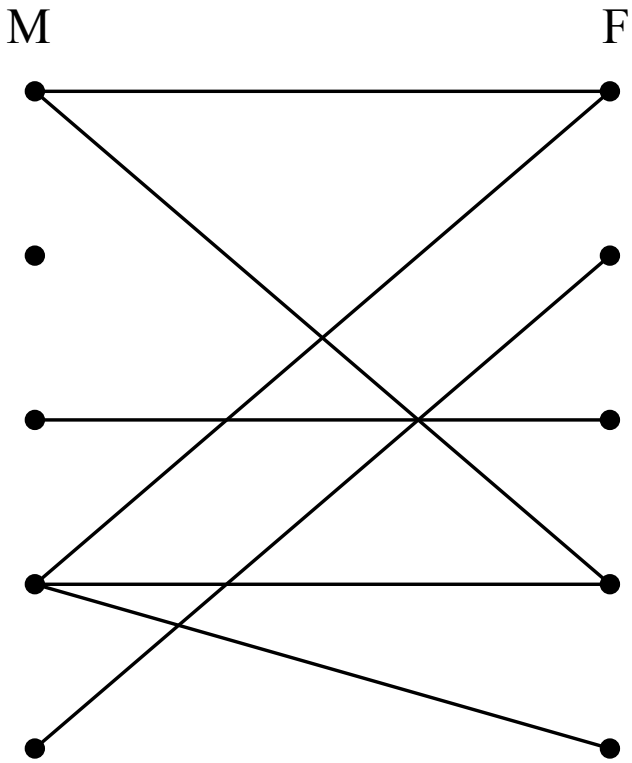
Un étude sur les comportements sexuels aux USA

- Une étude de la chaîne américaine ABC News a mené au résultat suivant :



- Ces résultats vous paraissent-ils sérieux ?

Le graphe des relations



- $G = (V, E)$ où V est divisé en deux sous-ensembles, les hommes M et les femmes F. Il y a une arête entre un homme et une femme s'ils ont eu une relation.
- Le graphe résultant est *biparti* (voir plus loin).

- Toute arête a exactement une extrémité dans M et une extrémité dans F. On a donc :

$$\sum_{x \in M} \deg(x) = \sum_{x \in F} \deg(x) = |E|$$

- En divisant les deux membres par $|M| \cdot |F|$, on obtient :

$$\frac{\sum_{x \in M} \deg(x)}{|M|} \cdot \frac{1}{|F|} = \frac{\sum_{x \in F} \deg(x)}{|F|} \cdot \frac{1}{|M|}$$

- qui donne directement :

$$\text{Avg. deg in } M = \frac{|F|}{|M|} \cdot \text{Avg. deg in } F$$

- Le rapport entre les degrés moyens ne dépend donc que du rapport entre les nombres d'hommes et de femmes dans la population
- D'après l'étude, on aurait :

$$20 = \frac{|F|}{|M|} \cdot 6,$$

c'est-à-dire 3 fois plus de femmes que d'hommes dans la population, ce qui est impossible.

Lemme des “poignées de main”

Lemme : La somme des degrés des sommets d'un graphe est égale à deux fois le nombre d'arêtes :

$$\sum_{x \in V} \deg(x) = 2 \cdot |E|$$

Démonstration : Chaque arête ajoute deux à la somme des degrés, un pour chacun de ses extrémités. □

Conséquences :

- Tout graphe a un nombre pair de sommets de degré impair.
- Exemple : il n'existe pas de graphe avec trois sommets de degrés respectivement 2,2, et 1.

Isomorphisme

Définition : Un *isomorphisme* entre des graphes $G = (V_G, E_G)$ et $H = (V_H, E_H)$ est une bijection $f : V_G \to V_H$ telle que :

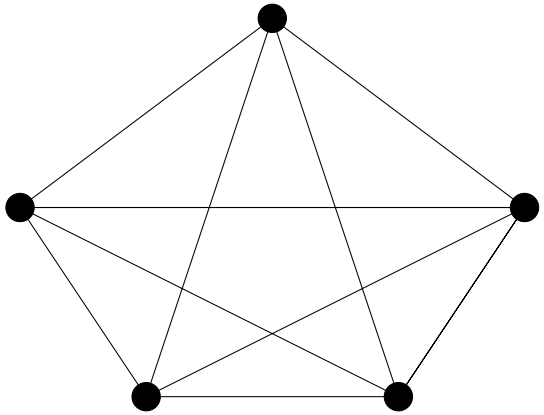
$$u—v \in E_G \text{ si et seulement si } f(u)—f(v) \in E_H$$

Deux graphes sont *isomorphes* quand il y a un isomorphisme entre eux.

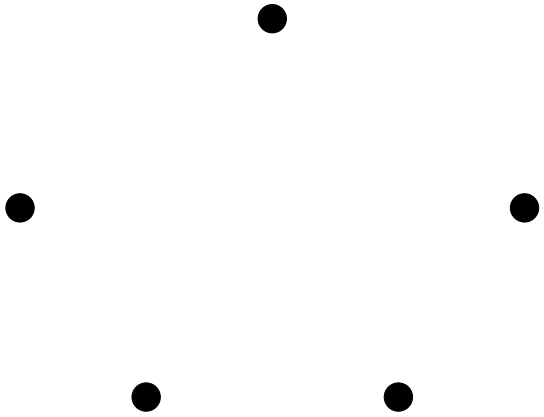
Des graphes isomorphes partagent la plupart de leurs propriétés : nombre de sommets, arêtes, patterns de degrés de sommets, etc.

Quelques graphes particuliers

- K_n, le graphe complet contenant n sommets :

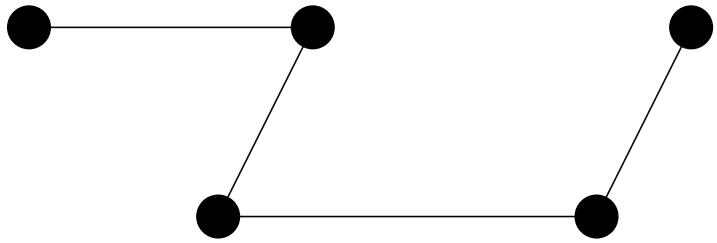


- Le *graphe vide* contenant n sommets :



- Un *chemin* est un graphe $G = (V, E)$ où
  - $V = \{v_1, v_2, \ldots, v_n\}$,
  - $E = \{v_1 — v_2, v_2 — v_3, \ldots, v_{n-1} — v_n\}$,
  - $n \geq 1$,
  - les sommets $v_1, v_2, \ldots, v_n$ sont tous distincts,
  - les sommets v_1 et v_n sont appelés les *extrémités* du chemin.

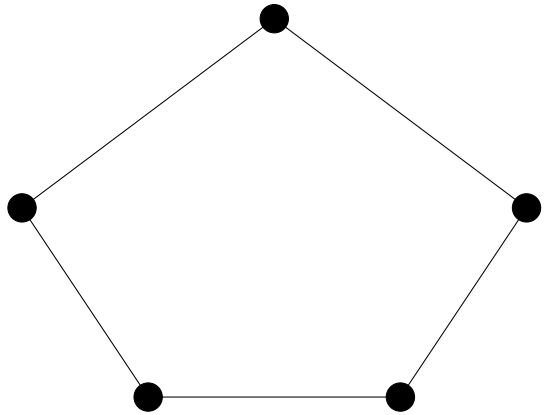
La *longueur* d'un chemin contenant n sommets est $n - 1$.



Soit $G = (V, E)$ un graphe, et $u, v \in V$. On dit qu'il *existe un chemin de u à v dans G* s'il existe un sous-graphe de G qui est un chemin à extrémités u et v.

- Un *cycle* est un graphe $G = (V, E)$ où
  - $V = \{v_1, v_2, \ldots, v_n\}$,
  - $E = \{v_1 — v_2, v_2 — v_3, \ldots, v_{n-1} — v_n, v_n — v_1\}$,
  - $n \geq 3$,
  - les sommets $v_1, v_2, \ldots, v_n$ sont tous distincts.

La *longueur* d'un cycle contenant n sommets est n.



Soit $G = (V, E)$ un graphe. Un cycle dans G est un sous-graphe de G qui est isomorphe à un cycle pour une longueur $n \geq 3$.

Parcours

Définition : Un *parcours* d'un graphe $G = (V, E)$ est une séquence de sommets et d'arêtes de la forme suivante :

$$v_0 \; v_0\text{—}v_1 \; v_1 \; v_1\text{—}v_2 \; v_2 \; \ldots \; v_{n-1} \; v_{n-1}\text{—}v_n \; v_n$$

où $v_i\text{—}v_{i+1} \in E$ pour $i = \{0, 1, \ldots, n-1\}$.

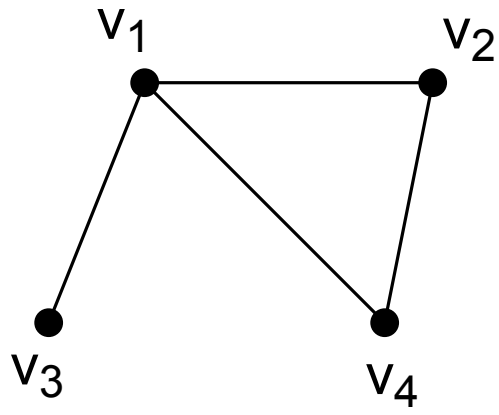
Si $v_0 = v_n$, alors le parcours est dit *fermé*. La longueur du parcours est égale au nombre d'arêtes n.

Remarques :

- Aussi appelé une *promenade*.
- Il existe un parcours entre deux sommets si et seulement si il existe un chemin entre ces sommets.
- Théorème : Le plus court parcours entre deux sommets est un chemin.

Matrices d'adjacence

- Un graphe $G = (V, E)$ avec pour sommets $V = \{v_1, v_2, \ldots, v_n\}$ peut être représenté par une matrice d'adjacence de taille $n \times n$. L'élément (i, j) de cette matrice vaut 1 si v_i—$v_j \in E$, 0 sinon.
- Par exemple :



$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

Théorème : Soit G un graphe dirigé (potentiellement avec des boucles) avec pour sommets $v_1, v_2, \ldots, v_n$ et M sa matrice d'adjacence. $(M^k)_{ij}$ est égal au nombre de parcours de longueur k de v_i à v_j.

Démonstration :

- La démonstration fonctionne par induction sur k.
- Soit $P(k) =$ "$(M^k)_{ij}$ est égal au nombre de chemins de longueur k de v_i à v_j".
- *Cas de base ($k = 1$) :* Par définition de la matrice d'adjacence, $(M^1)_{ij} = M_{i,j} = 1$ s'il y a un chemin de longueur 1 entre v_i et v_j, 0 sinon.
- *Cas inductif :*
  - Supposons $P(k)$ vrai pour un $k \geq 1$.
  - Tout parcours de longueur $k+1$ entre v_i et v_j est constitué d'une chemin de longueur k de v_i à un certain sommet v_m suivi d'une arête v_m—v_j.

- Le nombre de parcours de longueur $k+1$ entre v_i et v_j est donc égal à :

$$(M^k)_{i1}M_{1j} + (M^k)_{i2}M_{2j} + \ldots + (M^k)_{in}M_{nj},$$

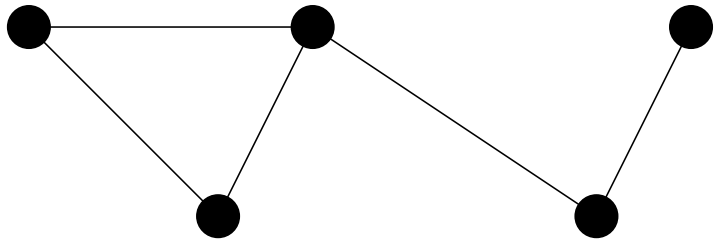
  qui est précisément la valeur de $(M^{k+1})_{ij}$.
- Par induction, $P(k)$ est vrai pour $k \geq 1$. □

Application : La longueur du plus court chemin entre deux sommets v_i et v_j est la plus petite valeur de k tel que $M^k_{ij} \neq 0$.

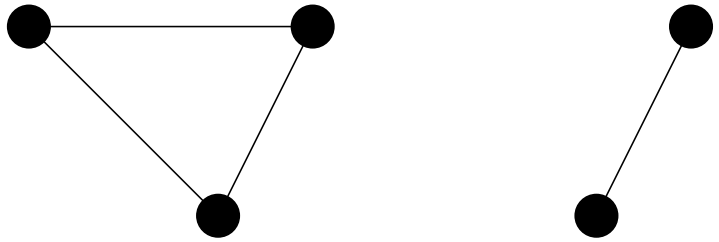
Graphes connexes

Définition : Un graphe $G = (V, E)$ est *connexe* si pour toute paire de sommets $u, v \in V$, il existe un chemin à extrémités u et v dans G.

Exemple de graphe connexe :



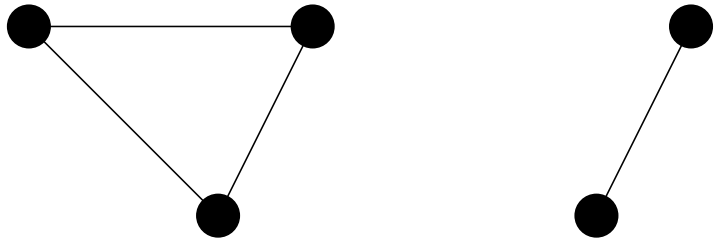
Exemple de graphe non connexe :



Composantes connexes

Définition : Soit $G = (V, E)$ un graphe. Une *composante connexe* de G est un sous-graphe connexe maximal, c'est-à-dire un sous-graphe connexe tel que l'ajout de tout sommet supplémentaire rend le sous-graphe non connexe.

Exemple :



Ce graphe contient 2 composantes connexes.

Théorème : Tout graphe $G = (V, E)$ contient au moins $|V| - |E|$ composantes connexes.

Démonstration :

- La démonstration fonctionne par induction sur le nombre d'arêtes.
- Soit $P(n) =$ "Tout graphe $G = (V, E)$ avec $|E| = n$ contient au moins $|V| - n$ composantes connexes".
- *Cas de base :* Dans un graphe sans arête, tout sommet est une composante connexe. Il y en a donc exactement $|V|$.
- *Cas inductif :*
  - Supposons que, pour un $n \in \mathbb{N}$, tout graphe contenant n arêtes possède au moins $|V| - n$ composantes connexes.
  - Soit $G = (V, E)$ un graphe contenant $n + 1$ arêtes.

- Enlevons une arête arbitraire u—v de G.
- Soit G' le sous-graphe résultant.
- Par hypothèse d'induction, G' possède au moins $|V| - n$ composantes connexes.
- Ajoutons l'arête u—v pour réobtenir le graphe G.
- Si u et v étaient dans la même composante connexe de G', alors G a le même nombre de composantes connexes que G'.
- Sinon, les composantes connexes dans lesquelles se trouvaient u et v dans G' se voient fusionnées, tandis que les autres composantes connexes restent inchangées. G a donc au moins $|V| - n - 1 = |V| - (n+1)$ composantes connexes.

- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}$. □

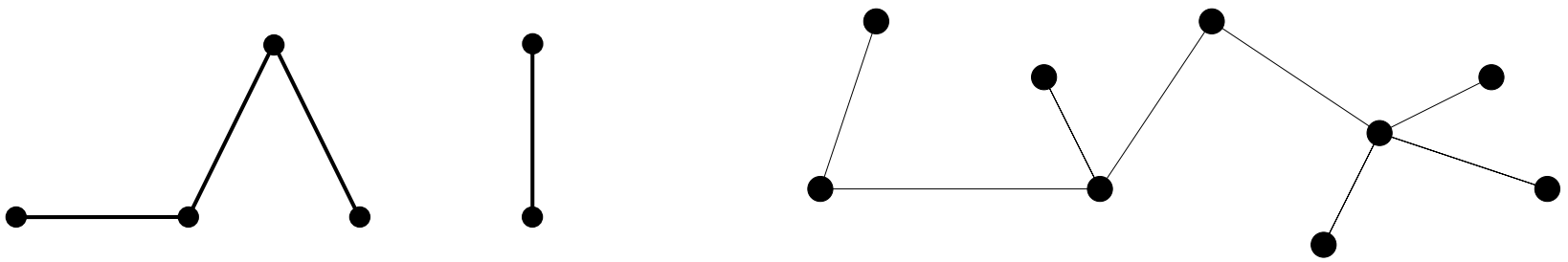
Corollaire : Tout graphe connexe contenant n sommets possède au moins $n - 1$ arêtes.

Arbres et forêts

Définition : Un graphe est *acyclique* si chacun de ses sous-graphes n'est pas un cycle. Un graphe

Définition : Un graphe acyclique est appelé une *forêt*. Un graphe acyclique connexe est appelé un *arbre*.
Toute composante connexe d'une forêt est un arbre.

Exemple :



Définition : Dans un arbre, une *feuille* est un sommet de degré 1. (Dans l'exemple, il y a 5 feuilles.)

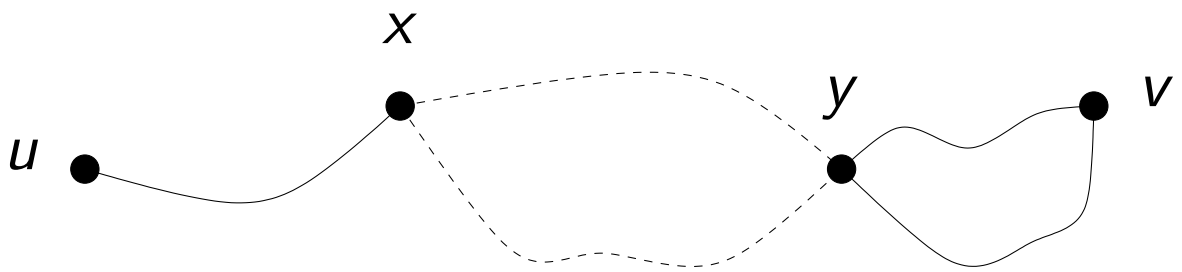
Théorème : Soit $T = (V, E)$ un arbre. Entre chaque paire de sommets, il y a un chemin unique.

Démonstration :

Existence : Le graphe étant connexe, il y a au moins un chemin entre chaque paire de sommets.

Unicité :

- Par l'absurde, supposons qu'il existe deux chemins différents entre les sommets u et v.
- En commencant par u, soit x le premier sommet à partir duquel les chemins divergent, et soit y le sommet suivant qu'ils partagent.



- Il existe deux chemins entre x et y sans arête commune. Ils définissent un cycle.
- C'est une contradiction car les arbres sont acycliques. □

Théorème : Soit $T = (V, E)$ un arbre.

1. Tout sous-graphe connexe de T est un arbre.
2. Ajouter une arête crée un cycle.
3. Retirer une arête rend le graphe non connexe.

Démonstration :

1. Un cycle d'un sous-graphe est cycle du graphe complet. Donc, un sous-graphe d'un graphe acyclique est acyclique. S'il est connexe, c'est un arbre par définition.
2. Une arête supplémentaire u—v entre le chemin unique à extrémités u et v crée un cycle.
3. - Supposons que l'on retire une arête u—v.
   - Le chemin unique entre u et v devait être u—v.
   - Il n'existe donc plus de chemin entre u et v.
   - Par conséquent, le graphe est devenu non connexe. □

Théorème : Soit $T = (V, E)$ un arbre contenant au moins 2 sommets. T contient au moins 2 feuilles.

Démonstration :

- Soit $v_1, \ldots, v_m$ la séquence de sommets d'un plus long chemin dans T.
- T contient au moins 2 sommets et est connexe. Donc, T contient au moins une arête.
- Il ne peut pas y avoir d'arête v_1—v_i, pour $2 < i \leq m$, sinon la séquence $v_1, \ldots, v_i$ formerait un cycle.
- Il ne peut pas y avoir d'arête u—v_1 où u n'est pas dans le chemin, sinon on pourrait allonger ce chemin.
- Seule arête incidente à v_1 : v_1—v_2. v_1 est donc une feuille.
- Un argument symétrique permet de montrer que v_m est une deuxième feuille. □

Théorème : Soit $T = (V, E)$ un arbre. On a $|V| = |E| + 1$.

Démonstration :

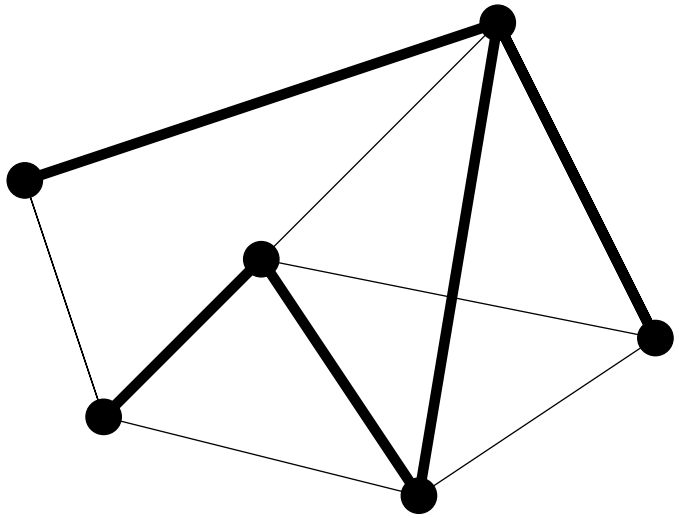
- La démonstration fonctionne par induction sur $|V|$.
- *Cas de base :* Si $|V| = 1$, on a $|E| + 1 = 0 + 1 = 1$.
- *Cas inductif :*
  - Supposons que le théorème soit vrai pour tout arbre contenant n sommets.
  - Soit $T = (V, E)$ un arbre contenant $n + 1$ sommets.
  - Soit v une feuille quelconque (elle existe car T contient au moins 1 arête, donc 2 sommets).
  - Soit $T' = (V', E')$ l'arbre obtenu en retirant v et son arête incidente.
  - On a $|V'| = |E'| + 1$.
  - En réinsérant v et son arête incidente, on obtient $|V| = |E| + 1$. □

Lemme : Un graphe $G = (V, E)$ est un arbre si et seulement si G est une forêt et $|V| = |E| + 1$.

Arbres couvrants

Définition : Soit $G = (V, E)$ un graphe. Un arbre $T = (V', E')$ est un *arbre couvrant* de G si $V' = V$ et $E' \subseteq E$.

Exemple :



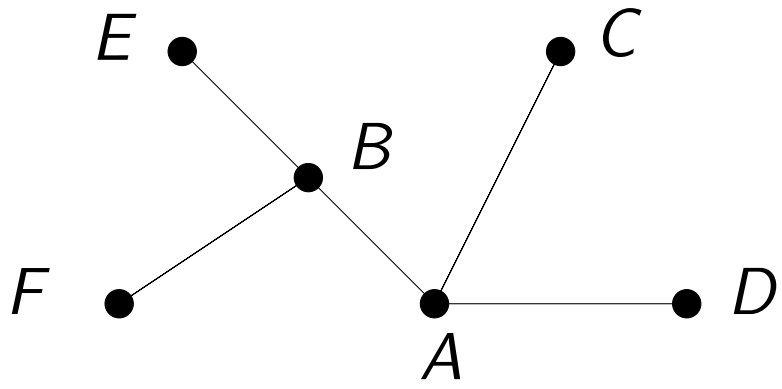
Théorème : Tout graphe connexe $G = (V, E)$ contient un arbre couvrant.

Démonstration :

- Par l'absurde, supposons que tout sous-graphe connexe $T = (V, E')$ de G soit nécessairement cyclique.
- Soit $T = (V, E')$ un de ces sous-graphes qui possède le plus petit nombre possible d'arêtes.
- T admet un cycle : v_0—v_1, v_1—v_2, ..., v_n—v_0.
- Supposons que l'on retire l'arête v_n—v_0. Soit x, y une paire de sommets quelconque.
  - Si x et y étaient connectés par un parcours ne contenant pas v_n—v_0, ils le restent.
  - Sinon, ils restent connectés par un parcours contenant le reste du cycle.
- Contradicition : T avait le plus petit nombre possible d'arêtes.
- Donc, T est acyclique. □

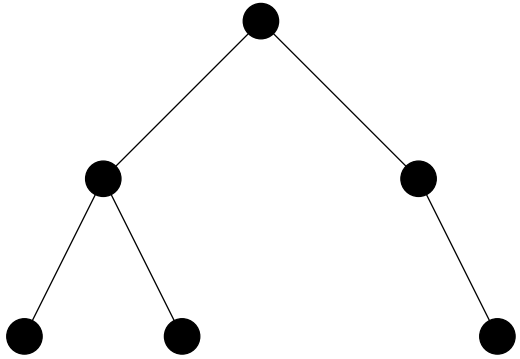
Arbres particuliers

- Arbre avec racine :
  - Un *arbre avec racine* est un arbre dans lequel un sommet est identifié comme étant la *racine*.
  - Soit u—v une arête d'un arbre avec racine telle que u est plus proche de la racine que v. Le sommet u est le *père* de v, et le sommet v est le *fils* de u.
  - Exemple :



Si A est la racine, alors E et F sont les fils de B, et A est le père de B, de C et de D.

- Un *arbre binaire* est un arbre avec racine dans lequel tout sommet a au plus 2 fils.



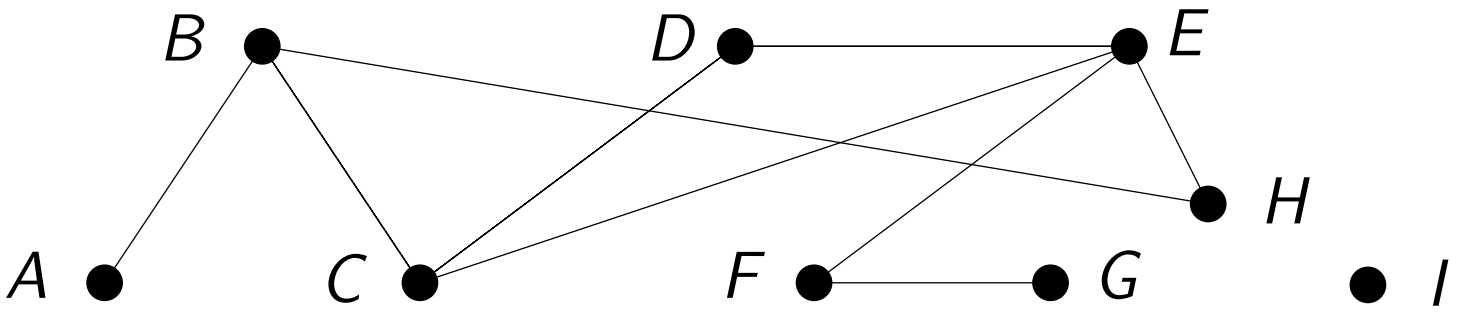
- Un arbre binaire est *ordonné* si les fils d'un sommet sont distingués : on les appelle *fils à gauche* et *fils à droite*.

Distance et diamètre

Définition :

- La *distance* entre deux sommets d'un graphe est la longueur du plus court chemin entre eux.
- Si un tel chemin n'existe pas, la distance entre les deux sommets est dite "infinie".

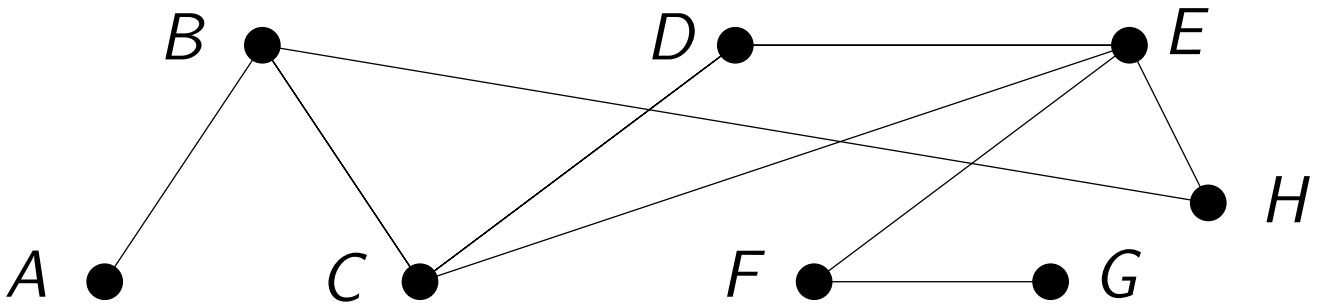
Exemple :



- la distance entre G et C est 3,
- la distance entre A et lui-même est 0,
- la distance entre I et n'importe quel autre sommet est infinie.

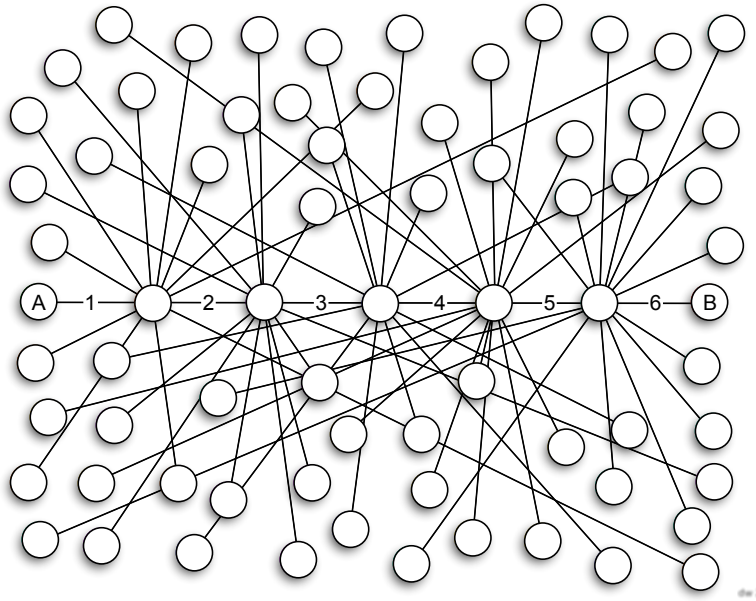
Définition : Le *diamètre* d'un graphe est la distance entre les deux sommets les plus éloignés.

Exemple :



- Les sommets qui sont les plus distants sont A et G.
- Leur distance est de 5.
- Le graphe a donc un diamètre de 5.

Six degrés de séparation



(wikipedia)

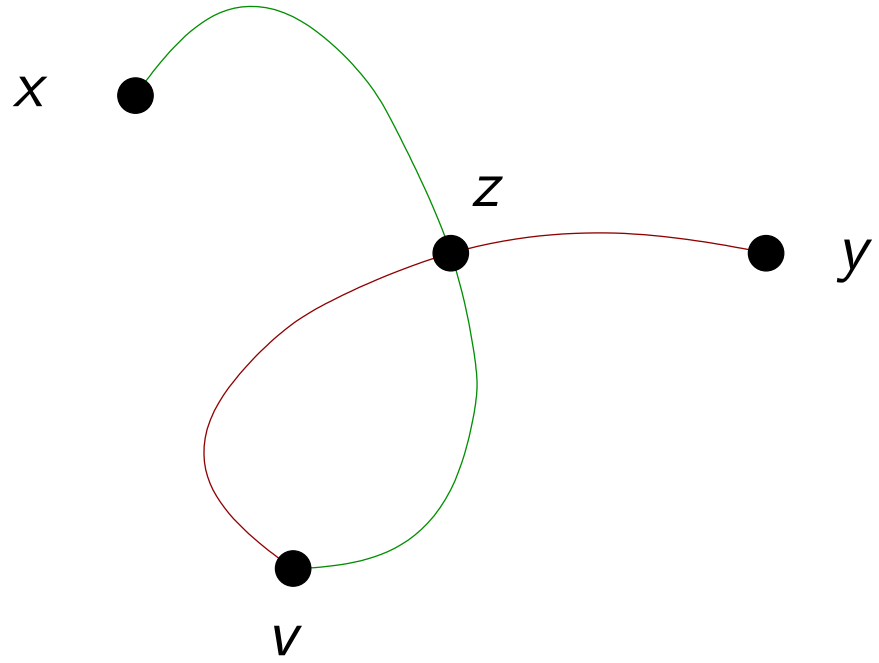
- Théorie selon laquelle deux personnes quelconques sur la planète peuvent être reliées au travers d'une chaîne d'au plus 6 relations.
- Ou de manière équivalente, le diamètre du réseau social global est au plus 6.
- Le distance moyenne a été mesuré à 6.5 (sur base de msn, facebook, etc.).

Théorème : Soit v un sommet arbitraire d'un graphe G. Si tout sommet est distant de v d'une distance au plus égale à d, alors le diamètre de G est borné par $2d$.

Démonstration :

- Soient x et y deux sommets quelconques de G.
- Il existe un chemin π_1 de longueur au plus égale à d entre x et v.
- Il existe un chemin π_2 de longueur au plus égale à d entre v et y.
- Soit z le sommet qui se trouve à la fois sur π_1 et sur π_2, et qui est le plus proche possible de x. (Un tel z existe toujours car, au pire, il pourrait être v.)
- On obtient un chemin entre x et y de longueur au plus égale à $2d$ en joignant le segment de x et z à celui entre z et y. □

Illustration :



Coloriage de graphes

Problème : l'apparitorat de la faculté doit mettre au point l'horaire des examens de la session de juin.

Contraintes :

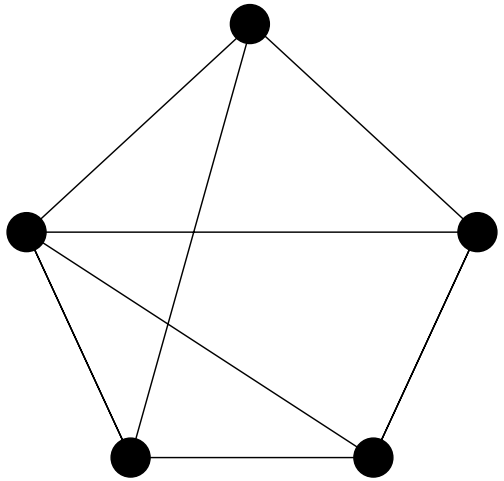
- Un étudiant ne peut pas participer à deux examens en même temps.
- La période d'examens doit être la plus courte possible.

Question : De quelle manière la théorie des graphes peut-elle nous aider à modéliser ce problème ?

Solution : Soit un graphe avec

- un sommet par cours,
- une arête entre deux sommets si au moins un des étudiants suit les deux cours.

Exemple :

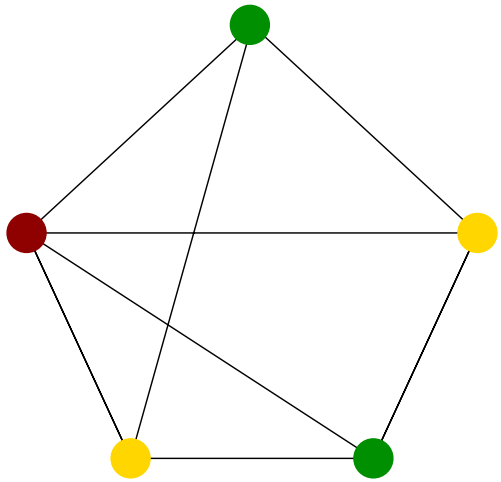


Associons une couleur à chaque plage horaire :

- lundi matin
- lundi après-midi
- mardi matin
- ...

Il est possible d'organiser l'examen sur *n plages horaires* si et seulement si il est possible de *colorier* les sommets du graphe à l'aide de *n couleurs* de telle manière que pour toute paire de sommets adjacents, ces sommets soient coloriés différemment.

Exemple :



Autres applications : allocation de registres, allocation de fréquences de station radio, coloriage de cartes...

k-coloriages

Définition : Un graphe G est *k-coloriable* s'il existe un ensemble C de k couleurs tel que chaque sommet puisse être colorié avec une couleur $c \in C$ sans que deux sommets adjacents ne partagent la même couleur.

Remarque : Tout graphe k-coloriable est nécessairement $(k+1)$-coloriable.

Définition : Le *nombre chromatique* $\chi(G)$ d'un graphe G est le plus petit nombre de couleurs nécessaires pour colorier le graphe G.

Un graphe est k-coloriable ssi $\chi(G) \leq k$.

Théorème : Soit $k \in \mathbb{N}_0$, et soit G un graphe dont chaque sommet est au plus de degré k. Le graphe G est $(k+1)$-coloriable.

Démonstration :

- La démonstration fonctionne par induction sur le nombre n de sommets de G.
- Soit $P(n) =$ "Tout graphe à n sommets de degrés au plus égaux à k est $(k+1)$-coloriable".
- *Cas de base :* $P(1)$ est vrai, car tout graphe à 1 sommet est 1-coloriable.

- *Cas inductif :* Supposons que $P(n)$ soit vrai.
  - Soit G un graphe à $n+1$ sommets, chacun de degré au plus égal à k.
  - Retirons de G un sommet v arbitraire, ainsi que ses arêtes incidentes. Soit G' le graphe résultant.
  - G' est $(k+1)$-coloriable.
  - Ajoutons le sommet v et ses arêtes incidentes.
  - Le degré de v est au plus égal à k, et $k+1$ couleurs sont disponibles.
  - Associons à v une couleur différente de tous ses sommets adjacents.
  - G est donc $(k+1)$-coloriable.
- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}_0$. □

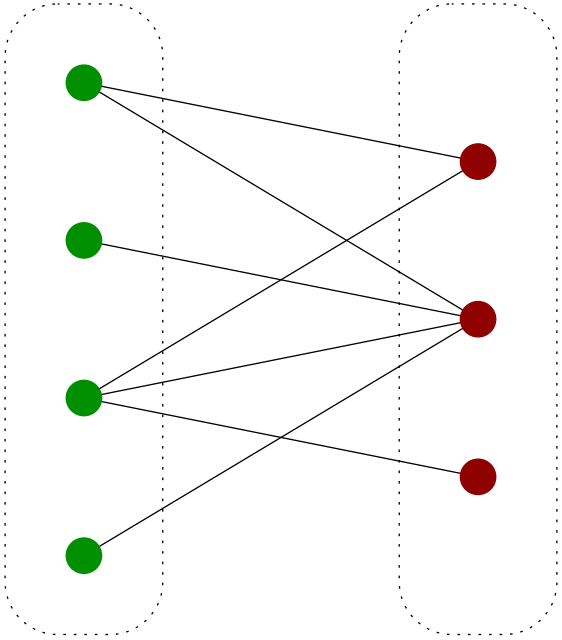
Graphes bipartis

Définition : Un graphe *biparti* est un graphe dont les sommets peuvent être divisés en deux sous-ensembles disjoints $L(G)$ et $R(G)$ tels que toute arête a une extrémité dans $L(G)$ et l'autre extrémité dans $R(G)$.

Lemme : Un graphe G est *biparti* ssi il est 2-coloriable.

Propriété : Soit G un graphe biparti. Si deux sommets u, v de G sont adjacents, alors dans tout 2-coloriage de G, un des deux sommets sera colorié avec une couleur, et l'autre sommet sera colorié avec la couleur restante.

Tout graphe biparti peut donc être représenté d'une façon similaire à la suivante :

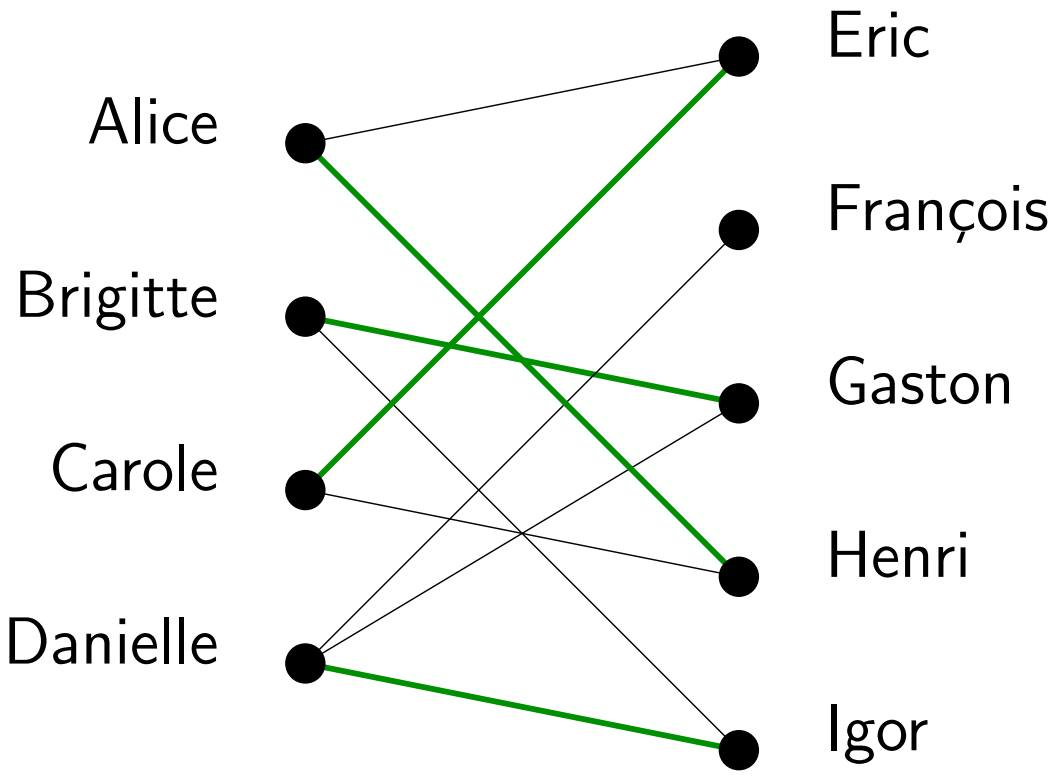


Théorème : Un graphe est biparti si et seulement s'il ne contient aucun cycle de longueur impaire.

Théorème de Hall

Données : Une groupe contient un certain nombre de filles et de garçons. Chaque fille aime certains garçons.

Problème : Sous quelles conditions chaque fille peut-elle est mariée à un garçon qu'elle aime ?



Définition : L'*ensemble des garçons aimés par un ensemble de filles* est l'ensemble des garçons aimés par au moins une de ces filles.

Condition de mariage : *Tout sous-ensemble des filles aime au moins un ensemble de garçons aussi grand.*

Exemple : Il est impossible de trouver une correspondance si ensemble de 4 filles aime un ensemble composé de seulement 3 garçons.

Théorème : Il est possible de trouver une correspondance entre un ensemble F de filles et un ensemble G de garçons si et seulement si la condition de mariage est satisfaite.

Démonstration :

$\boxed{\Rightarrow}$

- Considérons une correspondance possible.
- Soit F' un sous-ensemble quelconque de F.
- Chaque fille $f \in F'$ aime au moins le garçon avec lequel elle est mariée.
- Donc, la condition de mariage est satisfaite.

$\boxed{\Leftarrow}$

- Supposons que la condition de mariage soit satisfaite, et montrons qu'il existe une correspondance.
- La démonstration fonctionne par induction forte sur $|F|$.
- *Cas de base :* Si $|F| = 1$, une correspondance existe.
- *Cas inductif :* Supposons $|F| \geq 2$.
  - - Supposons que tout sous-ensemble propre des filles aime un ensemble de garçons *strictement plus grand*.
    - On peut marier une fille quelconque avec un garçon qu'elle aime.
    - La condition de mariage est satisfaite pour les personnes restantes.
    - On peut trouver une correspondance par induction.

- - Supposons qu'un ensemble $F' \subset F$ aime un ensemble de garçons $G' \subseteq G$ tel que $|G'| = |F'|$.
  - On peut marier les filles de F' avec les garçons de G' par induction.
  - Montrons que la condition de mariage est satisfaite pour les garçons et filles restantes.
  - Soit un sous-ensemble quelconque $F'' \subseteq (F \setminus F')$. Soit G'' l'ensemble des garçons aimés par F''.
  - Il faut montrer que $|F''| \leq |G''|$.
  - Comme $F' \cup F''$ aime $G' \cup G''$, on a $|F' \cup F''| \leq |G' \cup G''|$.
  - Comme $|F'| = |G'|$, on a $|F''| \leq |G''|$. □

Un énoncé formel

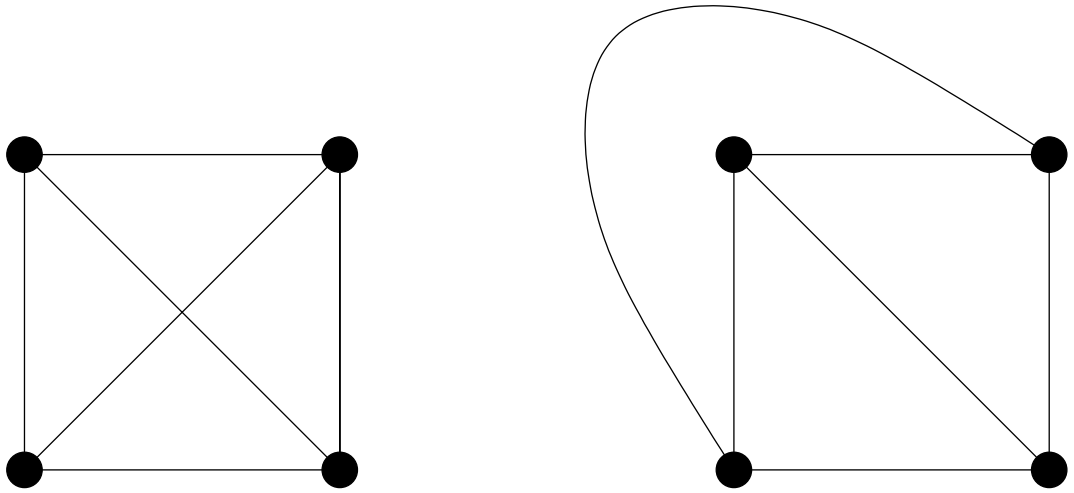
Définition : Soit S un sous-ensemble des sommets d'un graphe. $N(S)$ est défini par le nombre de sommets n'appartenant pas à S, mais adjacents à au moins un sommet de S.

Théorème : Soit $G = (L \cup R, E)$ un graphe biparti tel que toute arête a une extrémité dans L et l'autre extrémité dans R. Il existe une correspondance pour les sommets de L si et seulement si $|S| \leq |N(S)|$ pour tout $S \subseteq L$.

Graphes planaires

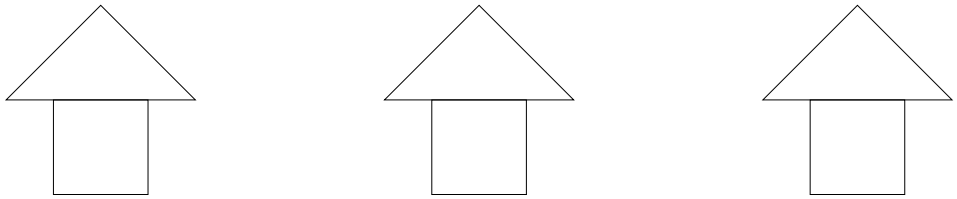
Définition informelle : Un graphe G est *planaire* s'il admet une représentation dans le plan telle que ses arêtes ne se croisent pas. Une telle représentation est appelée une *représentation planaire* de G.

Exemple :



Problème

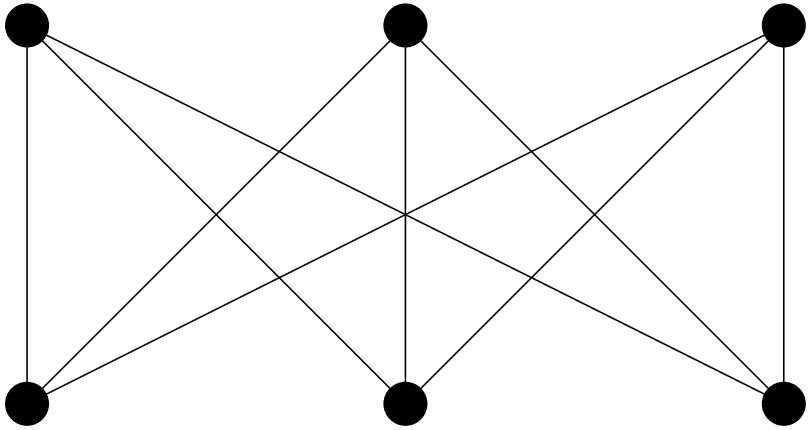
Données : Trois chiens et trois maisons



Chien Chien Chien

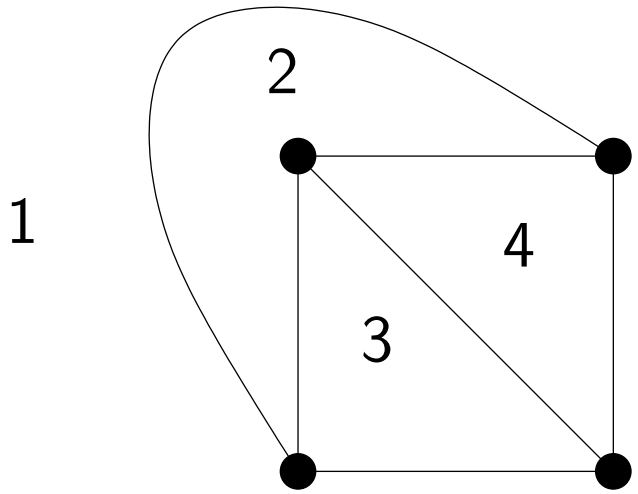
Question : Est-il possible de trouver des chemins de chaque chien vers chaque maison de telle façon qu'il n'y ait pas d'intersection ?

Réponse : C'est possible si et seulement si le graphe suivant ($K_{3,3}$) est planaire :



Formule d'Euler

Une représentation planaire d'un graphe planaire partitionne le plan en *faces* :



Théorème (formule d'Euler) : Pour toute représentation planaire d'un graphe planaire connexe $G = (V, E)$, on a

$$|V| - |E| + f = 2,$$

où f est le nombre de faces de cette représentation.

Démonstration :

- La démonstration fonctionne par induction sur le nombre d'arêtes.
- Soit $P(e) =$ "Pour toute représentation planaire d'un graphe planaire connexe $G = (V, E)$ tel que $|E| = e$, on a $|V| - e + f = 2$, où f est le nombre de faces de cette représentation".
- *Cas de base :* Si $e = 0$, on a nécessairement $|V| = 1$ et $f = 1$. Dès lors, $|V| - e + f = 2$.
- *Cas inductif :*
  - Supposons que $P(e)$ soit vrai, avec $e \in \mathbb{N}$.
  - Soit G un graphe avec $e + 1$ arêtes.
  - Si G est acyclique, alors le graphe est un arbre. Toute représentation planaire contient une seule face, et $(e + 1) + 1$ sommets. On a $(e + 2) - (e + 1) + 1 = 2$, donc $P(e + 1)$ est vrai.

- Sinon, G contient au moins un cycle.
  - Soient un arbre couvrant et une arête u—v dans le cycle, mais pas dans l'arbre.
  - Retirer l'arête u—v fusionne deux faces de la représentation planaire de G. Soit G' le graphe résultant, et soient v et f les nombres de sommets et de faces d'une représentation planaire de G'.
  - G' est connexe (l'arbre couvrant n'a pas été modifié). Donc, $v - e + f = 2$ par l'hypothèse d'induction.
  - En ajoutant l'arête u—v, on réobtient G. Il possède v sommets, $e + 1$ arêtes et $f + 1$ faces. Dès lors, $P(e + 1)$ est vrai.
- Par induction, $P(e)$ est vrai pour tout $e \in \mathbb{N}$. □

$K_{3,3}$ n'est pas planaire

- Les faces d'une représentation planaire d'un graphe sont limitées par des *cycles de sommets*.
- Supposons que $K_{3,3}$ soit planaire, et considérons une représentation planaire de $K_{3,3}$.
- D'après la formule d'Euler, le nombre de faces est égal à $2 - 6 + 9 = 5$.

- Soit N le nombre moyen de sommets délimitant chaque face.
- Toute face d'une représentation planaire de $K_{3,3}$ (si elle existe) doit être délimitée par un cycle d'au moins 4 sommets. On a donc $N \geq 4$.
- Or, on a $N = \frac{2 \cdot 9}{5} = 3,6 < 4$, car chaque arête intervient dans les limites d'exactement 2 faces.
- C'est une contradiction, donc $K_{3,3}$ n'est pas planaire.

Chapitre 5

Sommations et comportements asymptotiques

Introduction

Supposons

- que nous ayons la possibilité de placer de l'argent à un intérêt annuel de 6 %,
- que nous gagnions à la loterie, et
- que nous ne comptons dépenser les gains que dans 20 ans.

Recevoir 1.000.000 euros en une seule fois est plus avantageux que de recevoir 50.000 euros par an pendant 20 ans.

Question : Qu'en est-il si nous pouvons choisir entre recevoir 50.000 euros par an pendant 20 ans, et recevoir 500.000 euros de suite ?

Supposons que nous placions 1 euro aujourd'hui à un taux d'intérêt annuel de p %.

- Dans un an, nous aurons $1 + p$ euros,
- dans deux ans $(1 + p)^2$ euros, et ainsi de suite.

Donc,

- la valeur actuelle d'un euro qui sera payé dans un an n'est que de $\dfrac{1}{1 + p}$ euros,
- la valeur actuelle d'un euro qui sera payé dans deux ans n'est que de $\dfrac{1}{(1 + p)^2}$ euros, et ainsi de suite.

Calculons les valeurs actuelles des paiements de m euros au début de chacune des n prochaines années :

Paiements	Valeurs actuelles (euros)
m euros payés aujourd'hui	m
m euros payés dans un an	$m/(1+p)$
m euros payés dans deux ans	$m/(1+p)^2$
$\vdots$	$\vdots$
m euros payés dans $n-1$ ans	$m/((1+p)^{n-1})$
Valeur actuelle totale	$V = \sum_{k=1}^{n} \frac{m}{(1+p)^{k-1}}$

Solutions analytiques

Définition : Une *solution analytique* est une expression mathématique qui peut être évaluée à l'aide d'un nombre constant d'opérations de base (addition, multiplication, exponentiation, etc.).

Question : Comment trouver une solution analytique pour

$$\begin{aligned} V &= \sum_{k=1}^{n} \frac{m}{(1+p)^{k-1}} \\ &= \sum_{j=0}^{n-1} \frac{m}{(1+p)^{j}} \\ &= m \sum_{j=0}^{n-1} \left(\frac{1}{1+p} \right)^{j} \ ? \end{aligned}$$

Séries géométriques

Théorème : Pour tous $n \geq 0$ et $z \neq 1$, on a

$$\sum_{i=0}^{n} z^i = \frac{1 - z^{n+1}}{1 - z}.$$

Démonstration :

$$\begin{array}{rcccccccccc} S & = & 1 & + & z & + & z^2 & + & \ldots & + & z^n \\ zS & = & & & z & + & z^2 & + & \ldots & + & z^n & + & z^{n+1} \end{array}$$

On a $S - zS = 1 - z^{n+1}$, et donc $S = \dfrac{1 - z^{n+1}}{1 - z}$. □

Retour au problème introductif

On obtient

$$\begin{aligned} V &= m\sum_{j=0}^{n-1}\left(\frac{1}{1+p}\right)^j \\ &= m.\frac{1-\left(\frac{1}{1+p}\right)^n}{1-\left(\frac{1}{1+p}\right)}. \end{aligned}$$

Avec $m = 50.000$, $n = 20$ et $p = 0,06$, on obtient

$$V \approx 607.906 \text{ euros.}$$

Il est donc plus intéressant de recevoir 50.000 euros par an pendant 20 ans.

Sommes infinies

Définition : $\sum_{i=0}^{\infty} z_i = \lim_{n\to\infty} \sum_{i=0}^{n} z_i$.

Théorème : Si $|z| < 1$, alors $\sum_{i=0}^{\infty} z^i = \frac{1}{1-z}$.

Démonstration :

$$\begin{aligned}
\sum_{i=0}^{\infty} z^i &= \lim_{n\to\infty} \sum_{i=0}^{n} z^i \\
&= \lim_{n\to\infty} \frac{1-z^{n+1}}{1-z} \\
&= \frac{1}{1-z}.
\end{aligned}$$

□

Question : A un taux de 6%, est-il plus intéressant de recevoir 50.000 euros par an à vie, ou 1.000.000 euros de suite ?

Réponse : On a

$$\begin{aligned} V &= m\sum_{j=0}^{\infty}\left(\frac{1}{1+p}\right)^j \\ &= m.\frac{1}{1-\left(\frac{1}{1+p}\right)} \\ &= m.\frac{1+p}{p}. \end{aligned}$$

En substituant m et p par 50.000 et 0.06, on obtient

$$V \approx 883.333 \text{ euros.}$$

Il est donc plus intéressant de recevoir 1.000.000 euros de suite.

Variantes des séries géométriques

Théorème : Pour tous $n \geq 0$ et $z \neq 1$, on a

$$\sum_{i=0}^{n} iz^i = \frac{z - (n+1)z^{n+1} + nz^{n+2}}{(1-z)^2}.$$

Démonstration : On a

$$\sum_{i=0}^{n} iz^i = z \cdot \sum_{i=0}^{n} iz^{i-1} = z \cdot \left(\frac{d}{dz} \sum_{i=0}^{n} z^i \right) = z \cdot \left(\frac{d}{dz} \frac{1 - z^{n+1}}{1-z} \right).$$

En développant, on obtient

$$
\begin{aligned}
& z \cdot \left(\frac{d}{dz} \frac{1 - z^{n+1}}{1 - z} \right) \\
= \quad & z \cdot \left(\frac{-(n+1)z^n(1-z) - (-1)(1 - z^{n+1})}{(1-z)^2} \right) \\
= \quad & z \cdot \left(\frac{-(n+1)z^n + (n+1)z^{n+1} + 1 - z^{n+1}}{(1-z)^2} \right) \\
= \quad & z \cdot \left(\frac{1 - (n+1)z^n + nz^{n+1}}{(1-z)^2} \right) \\
= \quad & \frac{z - (n+1)z^{n+1} + nz^{n+2}}{(1-z)^2}.
\end{aligned}
$$

□

Corollaire : Si $|z| < 1$, alors $\sum_{i=0}^{\infty} iz^i = \frac{z}{(1-z)^2}$.

Démonstration : On a

$$\begin{aligned}\sum_{i=0}^{\infty} iz^i &= \lim_{n\to\infty} \sum_{i=0}^{n} iz^i \\ &= \lim_{n\to\infty} \frac{z-(n+1)z^{n+1}+nz^{n+2}}{(1-z)^2} \\ &= \frac{z}{(1-z)^2}.\end{aligned}$$

□

Autre variante : En intégrant les deux côtés de $\sum_{i=0}^{\infty} z^i = \frac{1}{1-z}$ (de 0 à x), on peut obtenir :

$$\sum_{j=1}^{\infty} \frac{x^j}{j} = -\ln(1-x).$$

Somme de puissances

Théorème : Pour tout $n \in \mathbb{N}$, on a

$$\sum_{i=1}^{n} i^2 = \frac{(2n+1)(n+1)n}{6}.$$

Démonstration : Par induction sur n. □

Comment trouver l'expression analytique ?

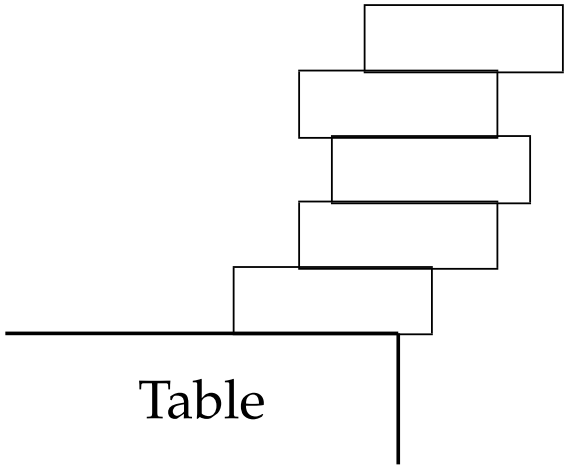
- Supposer que la somme est un polynôme de degré 3 (car somme∼intégration)

$$\sum_{i=1}^{n} i^2 = an^3 + bn^2 + cn + d$$

- Identifier les constantes a, b, c, d à partir de quelques valeurs de la somme
- Prouver sa validité par induction

Empilage de blocs

De combien au maximum peut dépasser une série de n blocs identiques empilés au bord d'une table ?



Soient deux objets de masses respectives m_1 et m_2 et dont les centres de masse sont aux positions x_1 et x_2. Le centre de masse du système constitué des deux objets se trouve à la position :

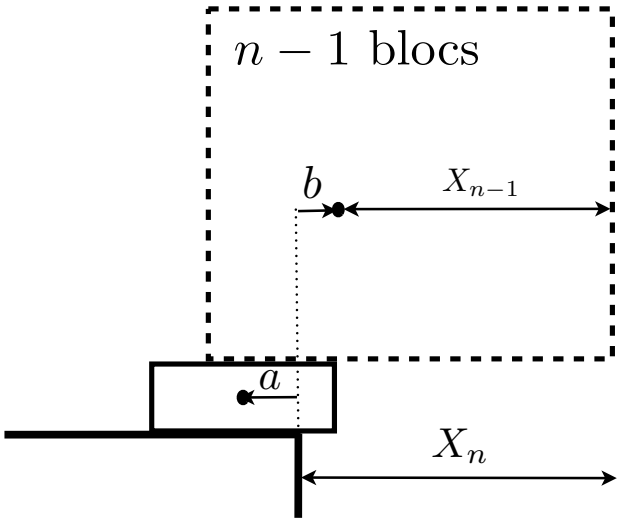
$$\frac{x_1 m_1 + x_2 m_2}{m_1 + m_2}$$

Théorème : Le plus grand dépassement possible d'une pile de n blocs ($n \geq 1$) est :

$$X_n = \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \ldots + \frac{1}{2n}.$$

Démonstration :

- La démonstration fonctionne par induction sur n le nombre de blocs
- Soit $P(n)$ = "le plus grand dépassement possible d'une pile de n blocs ($n \geq 1$) est $1/2 + 1/4 + \ldots + 1/(2n)$".
- *Cas de base ($n = 1$) :* Avec un seul bloc, le dépassement maximum est $X_1 = 1/2$ et donc $P(1)$ est vrai.
- *Cas inductif :*
  - Supposons $P(n-1)$ vrai pour un $n \geq 2$ pour démontrer que $P(n)$ est vrai.
  - Une pile de n blocs peut être vue comme une pile de $n-1$ blocs posée sur un bloc.



- Pour avoir un dépassement maximal, on a nécessairement que :
  1. les $n-1$ blocs supérieurs ont un dépassement maximal noté X_{n-1},
  2. Le centre de masse des n blocs se trouve juste au dessus du bord de la table,
  3. Le centre de masse des $n-1$ blocs supérieurs se trouve juste au dessus du bord droit du bloc inférieur

  (sinon, on pourrait obtenir un dépassement supérieur en changeant la disposition du système)

- Soient a la position du centre de masse du bloc inférieur et b la position du centre de masse des $n-1$ blocs, relatives au bord de la table.
- Par 2, on a $a.1 + b.(n-1) = 0$. Par 3, on a $b = a + 1/2$. En combinant les deux, on obtient $b = 1/(2n)$.
- Finalement :

$$X_n \;=\; X_{n-1} + b = X_{n-1} + \frac{1}{2n} = \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \ldots + \frac{1}{2n},$$

en exploitant le fait que $P(n)$ est vrai.

- Par induction, $P(n-1)$ est vrai pour tout $n \geq 1$. □

Exemple : Avec 4 blocs, on a

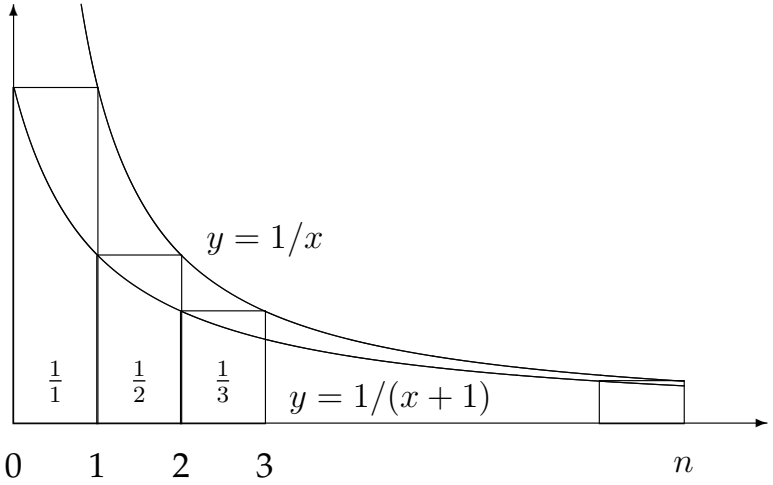
$$X_4 = \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \frac{1}{8} = 25/24 > 1.$$

Il est donc possible de placer un bloc entier en dehors de la table.

Série harmonique

Définition : $H_n = \frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{n}$ est une *série harmonique*. H_n est le n-ème nombre harmonique.

La série harmonique n'a pas de solution analytique. Des bornes inférieures et supérieures peuvent cependant être déterminées par intégration.



$$\begin{aligned}
\int_0^n \frac{1}{x+1}\,dx &\leq H_n \leq 1 + \int_1^n \frac{1}{x}\,dx \\
[\ln(x+1)]_0^n &\leq H_n \leq 1 + [\ln x]_1^n \\
\ln(n+1) &\leq H_n \leq 1 + \ln(n)
\end{aligned}$$

$$\Rightarrow H_n \sim \ln n$$

Définition : Soient deux fonctions $f, g : \mathbb{R} \to \mathbb{R}$. On écrit $f(x) \sim g(x)$ ssi $\lim_{x\to\infty} f(x)/g(x) = 1$ (f et g sont *asymptotiquement équivalents*).

Remarque sur les produits

Les mêmes techniques peuvent être utilisées pour calculer des produits en utilisant le logarithme :

$$\prod f(n) = \exp\left(\ln\left(\prod f(n)\right)\right) = exp\left(\sum \ln f(n)\right).$$

Permet de borner $n! = 1 \cdot 2 \cdot 3 \ldots (n-1) \cdot n$:

$$\frac{n^n}{e^n} \leq n! \leq \frac{(n+1)^{(n+1)}}{e^n}$$

Stirling's formula :

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

Notation asymptotique

Définition : Soient $f : \mathbb{R} \to \mathbb{R}$ et $g : \mathbb{R} \to \mathbb{R}$ deux fonctions. On écrit $f(x) = O(g(x))$ s'il existe des constantes x_0 et $c > 0$ telles que $|f(x)| \leq c.g(x)$ pour tout $x \geq x_0$.

Propriété : On a $5x + 100 = O(x)$.

Démonstration : On doit trouver des constantes x_0 et $c > 0$ telles que $|5x + 100| \leq cx$ pour tout $x \geq x_0$. Soient $c = 10$ et $x_0 = 20$. On a

$$|5x + 100| \leq 5x + 5x = 10x$$

pour tout $x \geq 20$. □

Propriété : On a $x = O(x^2)$.

Démonstration : On doit trouver des constantes x_0 et $c > 0$ telles que $|x| \leq c \cdot x^2$ pour tout $x \geq x_0$. Soient $c = 1$ et $x_0 = 1$. On a

$$|x| \leq 1 \cdot x^2$$

pour tout $x \geq 1$. □

Propriété : On a $x^2 \neq O(x)$.

Démonstration : Par l'absurde, supposons qu'il existe des constantes x_0 et $c > 0$ telles que

$$|x^2| \leq c \cdot x$$

pour tout $x \geq x_0$. On doit donc avoir

$$x \leq c$$

pour tout $x \geq x_0$, ce qui est impossible à satisfaire pour $x = \max(x_0, c + 1)$. □

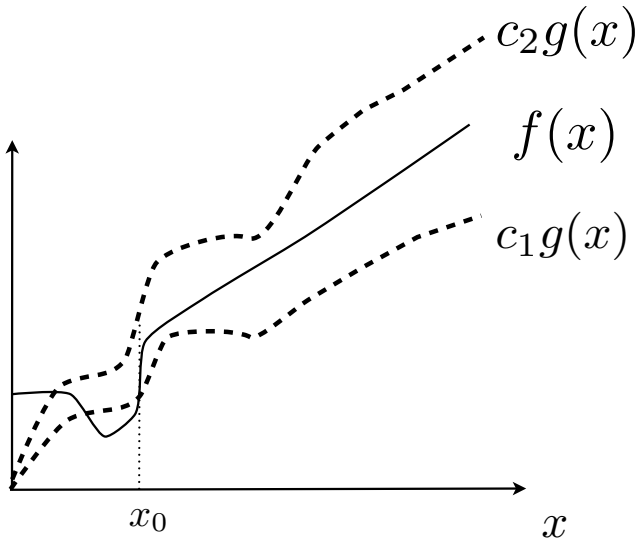
Notations Ω, Θ

Soient $f : \mathbb{R} \to \mathbb{R}$ et $g : \mathbb{R} \to \mathbb{R}$ deux fonctions :

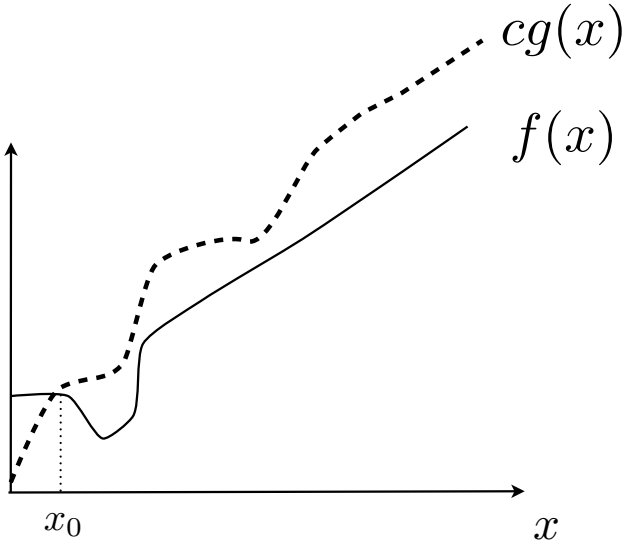
- $f(x) = \Omega(g(x))$ s'il existe des constantes x_0 et $c > 0$ telles que $f(x) \geq c.g(x) \geq 0$ pour tout $x \geq x_0$.
  (*borne inférieure*)
- $f(x) = \Theta(g(x))$ s'il existe des constantes x_0, c_1 et $c_2 > 0$ telles que $0 \leq c_1 g(x) \leq f(x) \leq c_2 g(x)$ pour tout $x \geq x_0$.
  (*équivalence asymptotiquement à un facteur près*)

Propriétés :

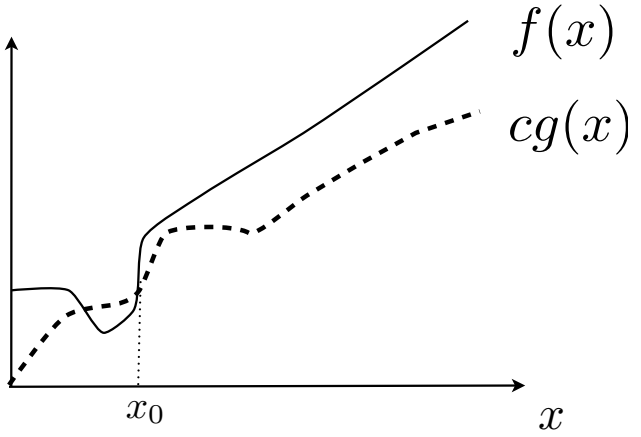
- $f(x) = \Omega(g(x)) \Leftrightarrow g(x) = O(f(x))$
- $f(x) = \Theta(g(x)) \Leftrightarrow f(x) = O(g(x))$ et $f(x) = \Omega(g(x))$
- $f(x) = \Theta(g(x)) \Leftrightarrow f(x) = O(g(x))$ et $g(x) = \Omega(f(x))$



$f(x) = \Theta(g(x))$



$f(x) = O(g(x))$



$f(x) = \Omega(g(x))$

Remarques

- Dans beaucoup de textes, on retrouve la notation O alors que Θ serait plus approprié.
- "$O(g) = f$" n'a pas de sens
  (Sinon $2n = O(n) \Rightarrow 1 = 2$)
- Parfois, on écrit $f \in O(g)$ à la place de $f = O(g)$ où $O(g)$ désigne alors l'ensemble des fonctions f telles que $f = O(g)$.
- Une équation du type :

$$2n^2 + 3n + 1 = 2n^2 + \Theta(n)$$

signifie qu'il existe une fonction $f(n) = \Theta(n)$ telle que :

$$2n^2 + 3n + 1 = 2n^2 + f(n).$$

Chapitre 6

Récurrences

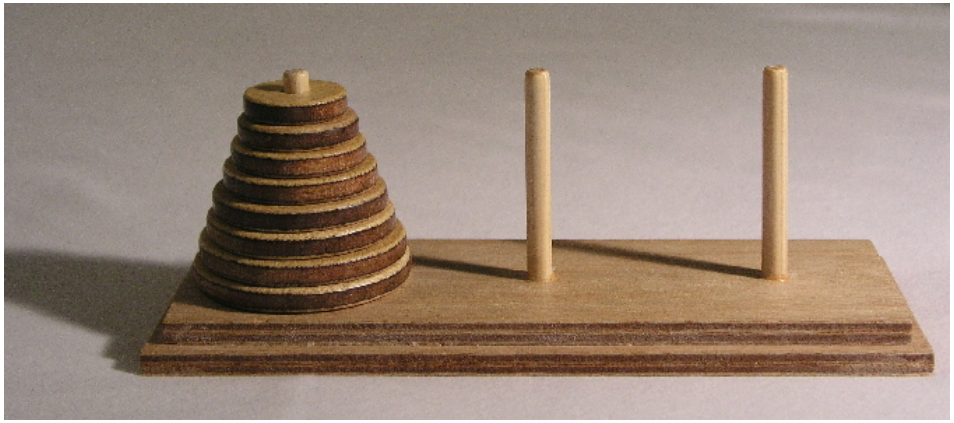
Introduction

Rappel : La notation asymptotique vue dans le chapitre 5 permet d'approximer la complexité des algorithmes.

But de ce chapitre : Étudier des méthodes permettant de résoudre des *équations récurrentes.*

Motivation : La complexité des *algorithmes récursifs* est souvent calculable à partir d'équations récurrentes.

Tours de Hanoï



Source : `http ://fr.wikipedia.org/wiki/Tours_de_Hanoï`

But : Déplacer la tour complète de la première tige vers une des deux autres tiges.

Contraintes :

- On ne peut déplacer qu'un seul disque à la fois.
- Un disque ne peut jamais être déposé sur un disque de diamètre inférieur.

Solution récursive :

- Cas de base : Déplacer une tour d'un seul disque est immédiat.
- Cas récursif : Pour déplacer une tour de $n+1$ disques de la première vers la troisième tige en connaissant une solution pour le déplacement d'une tour de n disques :
  1. Par récursion, déplacer n disques vers la deuxième tige ;
  2. Déplacer le disque restant vers la troisième tige ;
  3. Par récursion, déplacer les n disques de la deuxième tige vers la troisième tige.

Notation : Soit T_n le nombre minimum d'étapes nécessaires au déplacement d'une tour de n disques d'une tige vers une autre.

Propriété (borne supérieure) : On a $T_n \leq 2T_{n-1} + 1$.

Remarques :

- Pour déplacer une tour, il faut obligatoirement déplacer le disque du bas.
- Accéder au disque du bas nécessite de déplacer tous les autres disques vers une tige libre (au moins T_{n-1} étapes).
- Ensuite, il faut remettre en place le reste de la tour (au moins T_{n-1} étapes).

On a donc la propriété suivante :
Propriété (borne inférieure) : On a $T_n \geq 2T_{n-1} + 1$.

Récurrence : On sait à présent que $T_n = 2T_{n-1} + 1$.

Question : Comment calculer *efficacement* T_n, pour de grands n ?

Solution : Trouver une solution analytique pour T_n.

Méthode “Deviner-et-Vérifier”

Principes :

1. Calculer les quelques premières valeurs de T_n ;
2. Deviner une solution analytique ;
3. Démontrer qu'elle est correcte (par exemple par induction).

Application :

n	1	2	3	4	5	6	$\cdots$
T_n	1	3	7	15	31	63	$\cdots$
- On devine $T_n = 2^n - 1$
- On peut le démontrer par induction (exercice).

Méthode “Plug-and-Chug” (force brute)

1. “Plug” (appliquer l’équation récurrente) et “Chug” (simplifier)

$$\begin{aligned} T_n &= 1 + 2T_{n-1} \\ &= 1 + 2(1 + 2T_{n-2}) \\ &= 1 + 2 + 4T_{n-2} \\ &= 1 + 2 + 4(1 + 2T_{n-3}) \\ &= 1 + 2 + 4 + 8T_{n-3} \\ &= \dots \end{aligned}$$

Remarque : Il faut simplifier *avec modération*.

2. Identifier et vérifier un modèle
   - Identification :

$$T_n = 1 + 2 + 4 + \cdots + 2^{i-1} + 2^i T_{n-i}$$

   - Vérification en développant une étape supplémentaire :

$$\begin{aligned} T_n &= 1 + 2 + 4 + \cdots + 2^{i-1} + 2^i(1 + 2T_{n-(i+1)}) \\ &= 1 + 2 + 4 + \cdots + 2^{i-1} + 2^i + 2^{i+1} T_{n-(i+1)} \end{aligned}$$

3. Exprimer le $n^{\text{ème}}$ terme en fonction des termes précédents
   En posant $i = n - 1$, on obtient

$$\begin{aligned} T_n &= 1 + 2 + 4 + \cdots + 2^{n-2} + 2^{n-1} T_1 \\ &= 1 + 2 + 4 + \cdots + 2^{n-2} + 2^{n-1} \end{aligned}$$

4. Trouver une solution analytique pour le $n^{\text{ème}}$ terme

$$
\begin{aligned}
T_n &= 1 + 2 + 4 + \cdots + 2^{n-2} + 2^{n-1} \\
&= \sum_{i=0}^{n-1} 2^i \\
&= \frac{1 - 2^n}{1 - 2} \\
&= 2^n - 1
\end{aligned}
$$

Tri par fusion

Algorithme : Pour trier une liste de n éléments,

1. Diviser la liste en deux ;
2. Trier récursivement les deux sous-listes ;
3. Fusionner les deux listes triées.

Complexité : Soit T_n le nombre *maximum* de comparaisons à effectuer pour trier une liste de n éléments.

- On a $T_1 = 0$.
- Si $n > 1$, alors :
  - au pire $2T_{n/2}$ comparaisons pour trier les deux sous-listes ;
  - au pire $n - 1$ comparaisons pour fusionner deux sous-listes triées.

  Donc, $T_n = 2T_{n/2} + n - 1$.

Exercice : Trouver une solution analytique pour T_n.
(réponse : $T_n = n \log n - n + 1 \approx n \log n$).

Remarque

- On a supposé n puissance de 2 pour simplifier les développements
- La vraie récurrence est du type :
  - $T(1) = 1$
  - $T(n) = T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + n - 1$ (Pour $n > 1$)
- Généralement, on peut ignorer les problèmes d'arrondis car ils n'affectent pas la complexité

Comparaison

- Tours de Hanoï :
  - $T_1 = 1$
  - $T_n = 2T_{n-1} + 1$
  - Solution analytique : $T_n = 2^n - 1$

- Tri par fusion :
  - $T_1 = 0$
  - $T_n = 2T_{n/2} + n - 1$
  - Solution analytique : $T_n \approx n \log n$

Générer des petits sous-problèmes mène en général à des solutions plus rapides que celles pour lesquelles on tente en priorité de réduire le travail additionnel à faire à chaque appel récursif.

Un algorithme rapide

Soit un algorithme pour lequel, à chaque étape, les données du problème sont divisées en deux, et une seule étape additionnelle est nécessaire pour regrouper les résultats.

La complexité de cet algorithme est décrite par la récurrence suivante :

- $S_1 = 0$
- $S_n = 2S_{n/2} + 1$ (avec $n \geq 2$).

A l'aide de la méthode "Deviner-et-Vérifier", on obtient

n	S_n
1	0
2	$2S(1)+1=1$
4	$2S(2)+1=3$
8	$2S(4)+1=7$
16	$2S(8)+1=15$

On devine donc la solution $S_n = n-1$.

La vérification est immédiate :

Théorème : Supposons

- $S_1 = 0$
- $S_n = 2S_{n/2} + 1$ (avec $n \geq 2$).

Si n est une puissance de 2, alors $S_n = n - 1$.

Démonstration : (par induction forte)

- Soit $P(n) =$ "Si n est une puissance de 2, alors $S_n = n - 1$".
- *Cas de base :* $P(1)$ est vrai car $S_1 = 1 - 1 = 0$.
- *Cas inductif :* Supposons $P(1), P(2), \ldots, P(n-1)$.
  - Si n n'est pas une puissance de 2, alors $P(n)$ est trivialement vrai.
  - Sinon, $S_n = 2S_{n/2} + 1 = 2(\frac{n}{2} - 1) + 1 = n - 1$. □

Attention aux pièges de l'induction

Théorème : Si n est une puissance de 2, alors $S_n \leq n$
(vrai puisque on vient de démontrer $S_n = n - 1$)

Essai de démonstration :

- Par induction forte avec $P(n) =$ "Si n est une puissance de 2, alors $S_n \leq n$"
- *Cas de base :* $P(1)$ est vrai car $S_1 = 0 \leq 1$.
- *Cas inductif :* Supposons $P(1), P(2), \ldots, P(n-1)$.
  - Si n n'est pas une puissance de 2, alors $P(n)$ est trivialement vrai.
  - Sinon, $S_n = 2S_{n/2} + 1 \leq 2(n/2) + 1 = n + 1 \not\leq n$

□

Exercice : quid de $S_n \leq 2n$ ou $S_n \leq n - 2$?

Variation du nombre de sous-problèmes

Supposons :

- $T_1 = 1$;
- $T_n = aT_{n/2} + n$.

Solution (qui peut être obtenue par la méthode "Plug-and-Chug") :

$$T_n \approx \begin{cases} \dfrac{2n}{2-a} & \text{pour } 0 \leq a < 2; \\ n \log n & \text{pour } a = 2; \\ \dfrac{an^{\log a}}{a-2} & \text{pour } a > 2. \end{cases}$$

Observation : La solution dépend fortement de la valeur de a.

Une première généralisation

Théorème (Master theorem) : Soient deux constantes $a \geq 1$ et $b > 1$ et une fonction $f(n) = O(n^d)$ avec $d \geq 0$. La complexité asymptotique de la récurrence suivante :

$$T(n) = aT(n/b) + f(n)$$

est :

$$T(n) = \begin{cases} O(n^d) & \text{pour } d > \log_b a \\ O(n^d \log n) & \text{pour } d = \log_b a; \\ O(n^{\log_b a}) & \text{pour } d < \log_b a. \end{cases}$$

(Introduction to algorithms, Cormen et al.)

Exemple d'application

- Soit la récurrence suivante :

$$T(n) = 7T(n/2) + O(n^2).$$

(Méthode de Strassen pour la multiplication de matrice)

- $T(n)$ satisfait aux conditions du théorème avec $a = 7$, $b = 2$, et $d = 2$.
- $\log_b a = \log_2 7 = 2.807... \Rightarrow d = 2 < \log_b a = 2.807...$
- Par le troisième cas du théorème, on a :

$$T(n) = O(n^{\log_b a}) = O(n^{2.807...}).$$

Une seconde généralisation

Forme générale d'une récurrence "Diviser pour régner" :

$$T(x) = \begin{cases} \text{est défini} & \text{pour } 0 \leq x \leq x_0 \\ \displaystyle\sum_{i=1}^{k} a_i T(b_i x) + g(x) & \text{pour } x > x_0 \end{cases}$$

avec

- $a_1, a_2, \ldots, a_k > 0$,
- $b_1, b_2, \ldots, b_k \in [0, 1[$,
- x_0 suffisamment grand,
- $|g'(x)| = O(x^c)$ pour un $c \in \mathbb{N}$.

Théorème (Akra-Bazzi) :

$$T(x) = \Theta\left(x^p\left(1 + \int_1^x \frac{g(u)}{u^{p+1}}\,\mathrm{d}u\right)\right)$$

où

- p satisfait l'équation $\sum_{i=1}^{k} a_i b_i^p = 1$

Exemple d'application

- Soit la récurrence "diviser pour régner" suivante :

$$T(x) = 2T(x/2) + 8/9\,T(3x/4) + x^2$$

- On a bien $|g'(x)| = |2x| = O(x)$
- Trouvons p satisfaisant :

$$2(\frac{1}{2})^p + \frac{8}{9}(\frac{3}{4})^p = 1$$

$\Rightarrow p = 2$

- Par application du théorème, on obtient :

$$\begin{aligned} T(x) &= \Theta\left(x^2\left(1 + \int_1^x \frac{u^2}{u^3}du\right)\right) \\ &= \Theta(x^2(1 + \log x)) \\ &= \Theta(x^2 \log x) \end{aligned}$$

Changement de variables

- Considérons la récurrence suivante :

$$T(n) = 2T(\sqrt{n}) + \log n$$

- Posons $m = \log n$. On a :

$$T(2^m) = 2T(2^{m/2}) + m.$$

- Soit $S(m) = T(2^m)$. On a :

$$S(m) = 2S(m/2) + m \Rightarrow S(m) = O(m \log m).$$

- Finalement :

$$T(n) = T(2^m) = S(m) = O(m \log m) = O(\log n \log \log n).$$

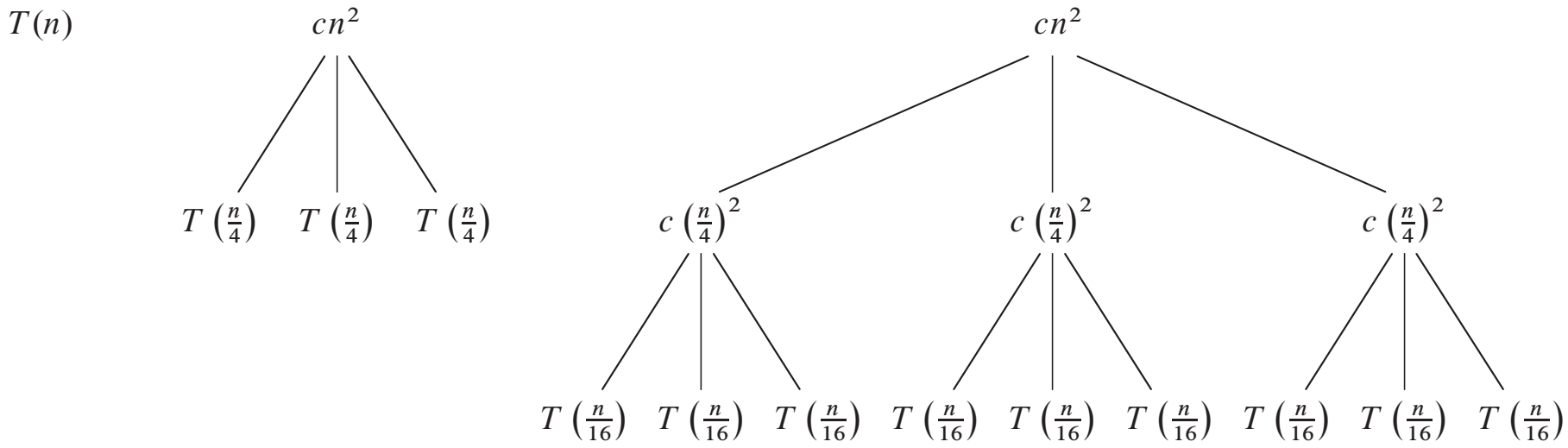
Arbres de récursion

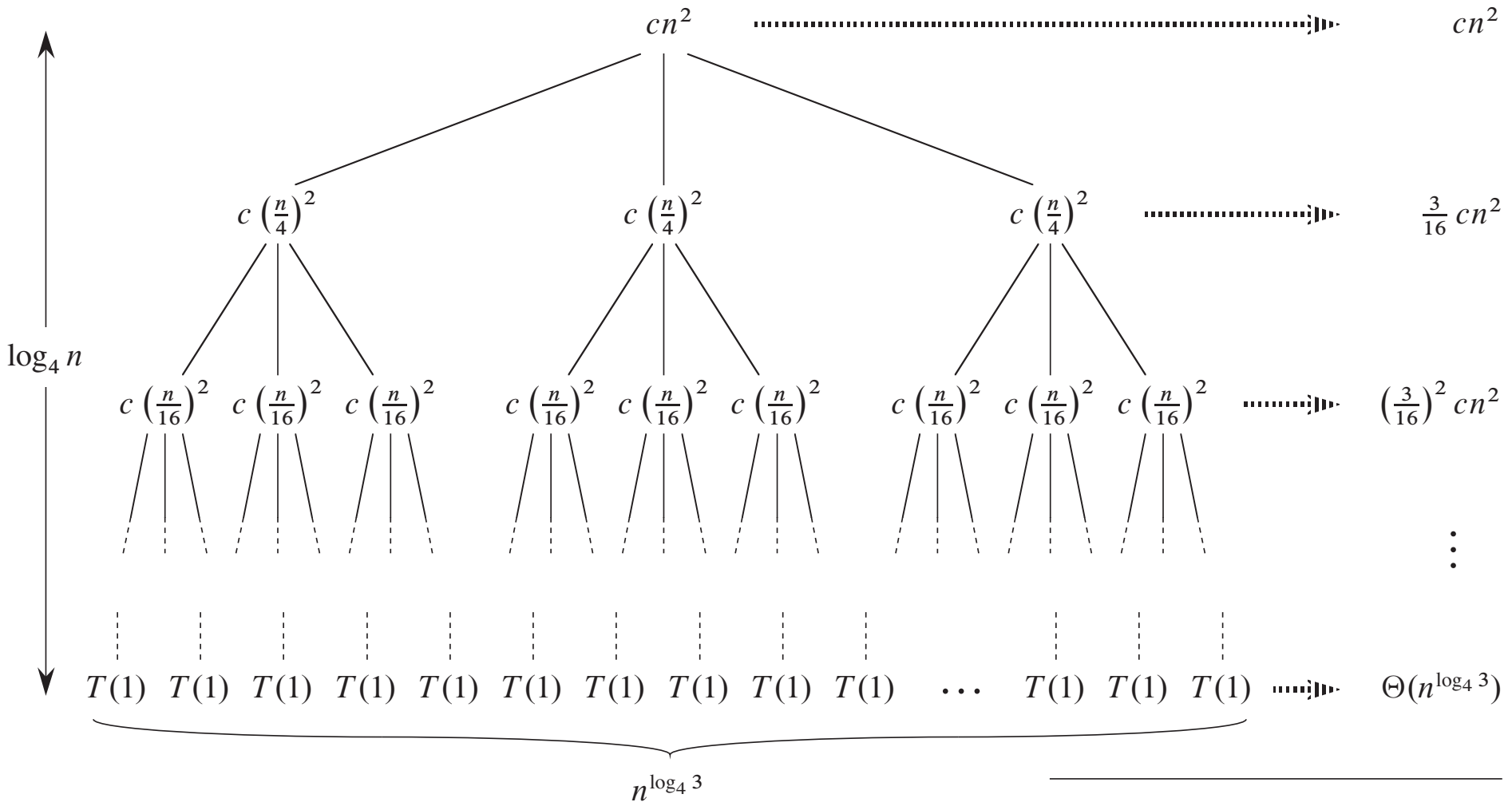
Approche alternative graphique pour *deviner* une solution analytique à une récurrence.

Illustration sur la récurrence suivante :

- $T(1) = a$
- $T(n) = 3T(n/4) + cn^2$ (Pour $n > 1$)

(Introduction to algorithms, Cormen et al.)


$T(n)$
cn^2
$T\left(\frac{n}{4}\right)$ $T\left(\frac{n}{4}\right)$ $T\left(\frac{n}{4}\right)$
cn^2
$c\left(\frac{n}{4}\right)^2$ $c\left(\frac{n}{4}\right)^2$ $c\left(\frac{n}{4}\right)^2$
$T\left(\frac{n}{16}\right)$ $T\left(\frac{n}{16}\right)$ $T\left(\frac{n}{16}\right)$ $T\left(\frac{n}{16}\right)$ $T\left(\frac{n}{16}\right)$ $T\left(\frac{n}{16}\right)$ $T\left(\frac{n}{16}\right)$ $T\left(\frac{n}{16}\right)$ $T\left(\frac{n}{16}\right)$


cn^2
cn^2
$c\left(\frac{n}{4}\right)^2$
$c\left(\frac{n}{4}\right)^2$
$c\left(\frac{n}{4}\right)^2$
$\frac{3}{16}cn^2$
$\log_4 n$
$c\left(\frac{n}{16}\right)^2$
$c\left(\frac{n}{16}\right)^2$
$c\left(\frac{n}{16}\right)^2$
$c\left(\frac{n}{16}\right)^2$
$c\left(\frac{n}{16}\right)^2$
$c\left(\frac{n}{16}\right)^2$
$c\left(\frac{n}{16}\right)^2$
$c\left(\frac{n}{16}\right)^2$
$c\left(\frac{n}{16}\right)^2$
$\left(\frac{3}{16}\right)^2 cn^2$
$T(1)$ $T(1)$ $T(1)$ $T(1)$ $T(1)$ $T(1)$ $T(1)$ $T(1)$ $T(1)$ $T(1)$ $\cdots$ $T(1)$ $T(1)$ $T(1)$
$\Theta(n^{\log_4 3})$
$n^{\log_4 3}$

- Le coût total est la somme du coût de chaque niveau de l'arbre :

$$\begin{aligned} T(n) &= cn^2 + \frac{3}{16}cn^2 + \ldots + \left(\frac{3}{16}\right)^{\log_4 n-1} cn^2 + an^{\log_4 3} \\ &= \sum_{i=0}^{\log_4 n-1} \left(\frac{3}{16}\right)^i cn^2 + an^{\log_4 3} \\ &< \sum_{i=0}^{\infty} \left(\frac{3}{16}\right)^i cn^2 + an^{\log_4 3} \\ &= \frac{1}{1-(3/16)} cn^2 + an^{\log_4 3} \\ &= O(n^2) \end{aligned}$$

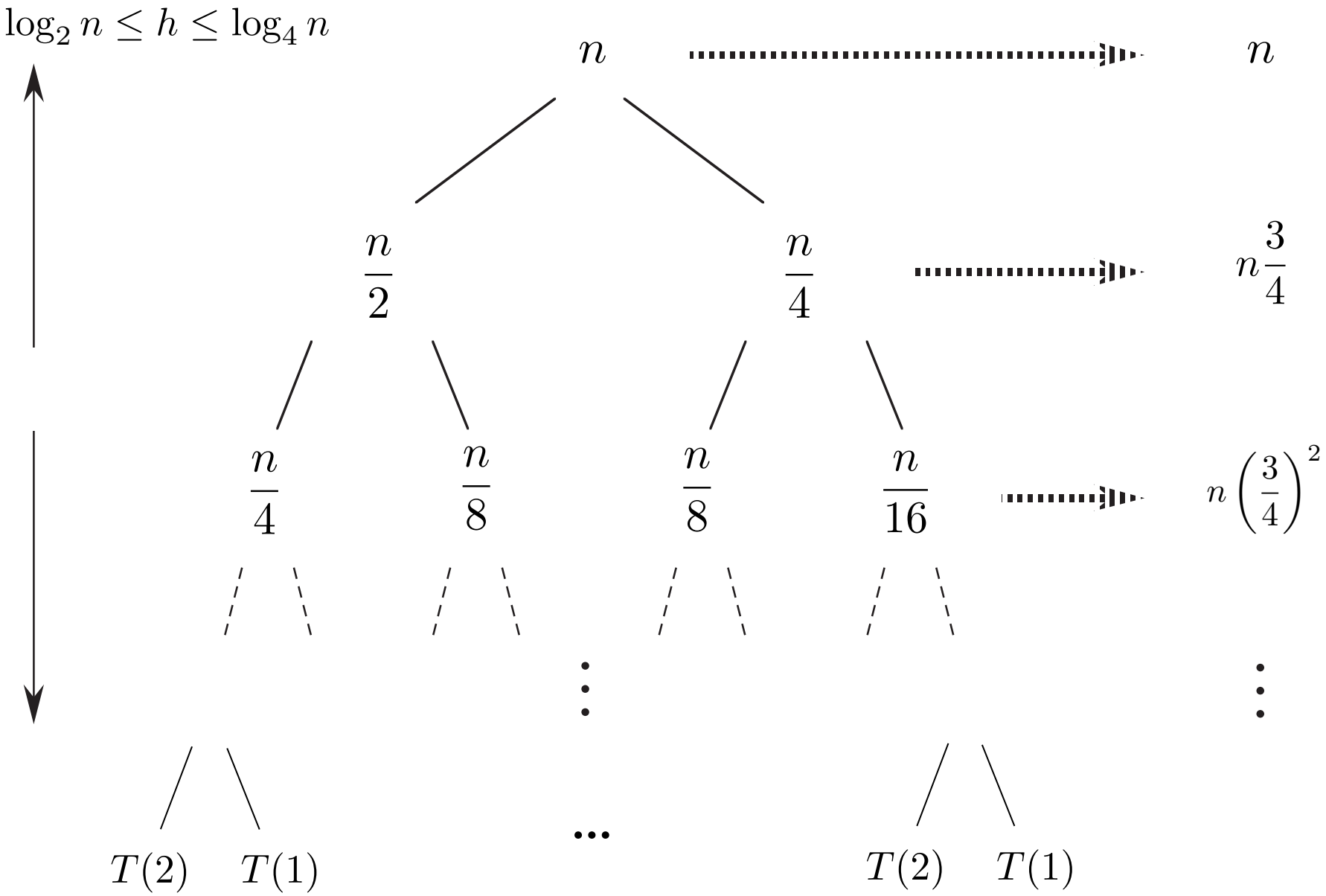
(à vérifier par induction)

- Comme le coût de la racine est cn^2, on a aussi $T(n) = \Omega(n^2)$ et donc $T(n) = \Theta(n^2)$.

Autre exemple :

- $T(1) = 1$
- $T(2) = 2$
- $T(n) = T(n/2) + T(n/4) + n$ (pour $n > 2$)

(On suppose que n est toujours une puissance de 2)


$\log_2 n \leq h \leq \log_4 n$
n
n
$\frac{n}{2}$
$\frac{n}{4}$
$n\frac{3}{4}$
$\frac{n}{4}$
$\frac{n}{8}$
$\frac{n}{8}$
$\frac{n}{16}$
$n\left(\frac{3}{4}\right)^2$
$T(2)$
$T(1)$
$T(2)$
$T(1)$

- On déduit de l'arbre que

$$T(n) \leq \sum_{i=0}^{\infty} n \left(\frac{3}{4}\right)^i = n \frac{1}{1-\frac{3}{4}} = O(n)$$

- Vérification par induction forte qu'il existe un c tel que pour tout $n \geq n_0$, on a $T(n) \leq cn$

$$\begin{aligned} T(n) &= T(n/2) + T(n/4) + n \\ &\leq cn/2 + cn/4 + n \\ &= (c3/4 + 1)n \\ &\leq cn \end{aligned}$$

  $\Rightarrow$ ok pour tout $c > 4$

- Puisqu'on a aussi $T(n) = \Omega(n)$, on en déduit $T(n) = \Theta(n)$.

Induction et notation asymptotique

Théorème faux : Soit la récurrence :

- $T(1) = 1$,
- $T(n) = 2T(n/2) + n$ (pour $n > 1$).

On a $T(n) = O(n)$.

(la solution correcte est $T(n) = \Theta(n \log(n))$)

Démonstration : (par induction forte)

- Soit $P(n) =$ "$T(n) = O(n)$".
- *Cas de base :* $P(1)$ est vrai car $T(1) = 1 = O(1)$.
- *Cas inductif :* Pour $n \geq 2$, supposons $P(1), P(2), \ldots, P(n-1)$. On a :

$$\begin{aligned} T(n) &= 2T(n/2) + n \\ &= 2O(n/2) + n \\ &= O(n) \end{aligned}$$

Où est l'erreur ?

Récurrences linéaires

Définition : Une *récurrence linéaire homogène* est une récurrence de la forme

$$f(n) = a_1 f(n-1) + a_2 f(n-2) + \cdots + a_d f(n-d)$$

où $a_1, a_2, \ldots, a_d \in \mathbb{R}$ sont des constantes. La valeur $d \in \mathbb{N}_0$ est appelée l'*ordre* de la récurrence.

Définition : Une *récurrence linéaire* (générale) est une récurrence de la forme

$$f(n) = a_1 f(n-1) + a_2 f(n-2) + \cdots + a_d f(n-d) + g(n),$$

où g est une fonction ne dépendant pas de f.

Suite de ce chapitre : Étude d'une méthode permettant de *résoudre* les récurrences linéaires, c'est-à-dire de trouver des solutions analytiques équivalentes.

Théorème : Si $f_1(n)$ et $f_2(n)$ sont solutions d'une récurrence linéaire homogène (sans tenir compte des conditions initiales), alors toute combinaison linéaire $cf_1(n) + df_2(n)$ de $f_1(n)$ et $f_2(n)$ est également une solution pour tout $c, d \in \mathbb{R}$.

Démonstration : On a $f_1(n) = \sum_{i=1}^{d} a_i f_1(n-i)$ et

$f_2(n) = \sum_{i=1}^{d} a_i f_2(n-i)$. Dès lors,

$$\begin{aligned} cf_1(n) + df_2(n) &= c \cdot \left(\sum_{i=1}^{d} a_i f_1(n-i) \right) + d \cdot \left(\sum_{i=1}^{d} a_i f_2(n-i) \right) \\ &= \sum_{i=1}^{d} a_i (cf_1(n-i) + df_2(n-i)). \end{aligned}$$

□

Exemple de résolution d'une récurrence

Supposons l'existence d'une nouvelle discipline scientifique, et des contraintes suivantes :

- N places de professeurs enseignant cette discipline sont disponibles dans le monde.
- Chaque professeur
  - est nommé à vie ;
  - est supposé immortel ;
  - forme chaque année exactement un étudiant qui deviendra professeur l'année suivante (exception : lors de leur première année d'enseignement, les professeurs sont trop occupés pour former un étudiant).
- Année 0 : il n'y a aucun professeur.
- Année 1 : le premier professeur (autodidacte) est formé.

Question : Quand les N places de professeurs seront-elles occupées ?

Etape 1 : Trouver une récurrence

Année (n)	Nombre de professeurs ($f(n)$)
0	0
1	1 (1 nouveau)
2	1 (1 ancien qui forme un étudiant)
3	2 (1 nouveau, 1 ancien)
4	3 (1 nouveau, 2 anciens)
5	5 (2 nouveaux, 3 anciens)
6	8 (3 nouveaux, 5 anciens)
$\vdots$	$\vdots$

Pour $n \geq 2$, on obtient $f(n) = f(n-1) + f(n-2)$.
Remarque : Il s'agit d'une récurrence linéaire homogène.

Etape 2 : Résoudre la récurrence

- Une solution analytique pour une récurrence linéaire a souvent une forme exponentielle.
- On devine $f(n) = cx^n$ (c et x sont des paramètres à trouver).
-

$$
\begin{aligned}
& f(n) = f(n-1) + f(n-2) \\
\Rightarrow \quad & cx^n = cx^{n-1} + cx^{n-2} \\
\Rightarrow \quad & x^2 = x + 1 \\
\Rightarrow \quad & x = \frac{1 \pm \sqrt{5}}{2}
\end{aligned}
$$

- Les fonctions $c\left(\frac{1+\sqrt{5}}{2}\right)^n$ et $c\left(\frac{1-\sqrt{5}}{2}\right)^n$ sont des solutions de la récurrence (sans tenir compte des conditions initiales).
- Il en est de même pour toute combinaison linéaire de ces deux fonctions.
- On a donc $f(n) = c_1\left(\frac{1+\sqrt{5}}{2}\right)^n + c_2\left(\frac{1-\sqrt{5}}{2}\right)^n$.

- $f(0) = c_1 \left(\frac{1+\sqrt{5}}{2}\right)^0 + c_2 \left(\frac{1-\sqrt{5}}{2}\right)^0 = c_1 + c_2 = 0.$
- $f(1) = c_1 \left(\frac{1+\sqrt{5}}{2}\right)^1 + c_2 \left(\frac{1-\sqrt{5}}{2}\right)^1 = 1.$
- On obtient $c_1 = \frac{1}{\sqrt{5}}$ et $c_2 = \frac{-1}{\sqrt{5}}$.
- Finalement,

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

Réponse à la question : Les N places de professeurs seront occupées lorsque $f(n)$ deviendra supérieur ou égal à N.

Comme $\left|\frac{1-\sqrt{5}}{2}\right| \approx 0,618 < 1$, cela se produira lorsque

$$f(n) \approx \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n \geq N.$$

Ce nombre d'années n grandit donc logarithmiquement en fonction de N.

Résolution des récurrences linéaires

Soit une récurrence de la forme

$$f(n) = a_1 f(n-1) + a_2 f(n-2) + \cdots + a_d f(n-d) + g(n)$$

et les conditions initiales $f(0) = b_0$, $f(1) = b_1$, etc.

Etape 1 : Trouver les racines de l'*équation caractéristique*

Définition : L'équation caractéristique est

$$x^d = a_1 x^{d-1} + a_2 x^{d-2} + \cdots + a_{d-1} x + a_d.$$

Remarque : Le terme $g(n)$ n'est pas pris en compte dans l'équation caractéristique.

Etape 2 : Trouver une *solution homogène*, sans tenir compte des conditions initiales

Il suffit d'additionner les termes suivants :

- Une racine non répétée r de l'équation caractéristique génère le terme

$$c_r r^n,$$

où c_r est une constante à déterminer plus tard.

- Une racine r avec multiplicité k de l'équation caractéristique génère les termes

$$c_{r_1} r^n, c_{r_2} n r^n, c_{r_3} n^2 r^n, \ldots, c_{r_k} n^{k-1} r^n,$$

où $c_{r_1}, c_{r_2}, \ldots, c_{r_k}$ sont des constantes à déterminer plus tard.

Etape 3 : Trouver une *solution particulière*, sans tenir compte des conditions initiales.

Une technique simple consiste à *deviner et vérifier* en essayant des solutions *ressemblant* à $g(n)$.

Exemples :

- Si $g(n)$ est un polynôme, essayer avec un polynôme de même degré, ensuite avec un polynôme de degré immédiatement supérieur, et ainsi de suite.
  Exemple : Si $g(n) = n$, essayer d'abord $f(n) = bn + c$, ensuite, $f(n) = an^2 + bn + c$, ...
- Si $g(n) = 3^n$, essayer d'abord $f(n) = c3^n$, ensuite $f(n) = bn3^n + c3^n$, $f(n) = an^2 3^n + bn3^n + c3^n$, ...

Remarque : On doit attribuer aux constantes $a, b, c, \ldots$ des valeurs satisfaisant l'équation récurrente.

Etape 4 : Former une *solution générale*, sans tenir compte des conditions initiales

Il suffit d'additionner la solution homogène et la solution particulière

Etape 5 : Déterminer les valeurs des constantes introduites à l'étape 2

- Pour chaque condition initiale, appliquer la solution générale à cette condition. On obtient une équation en fonction des constantes à déterminer.
- Résoudre le système formé par ces équations.

Exemple

On demande de résoudre la récurrence suivante :

- $f(1) = 1$
- $f(n) = 4f(n-1) + 3^n$

Etape 1 : Trouver les racines de l'équation caractéristique

- L'équation caractéristique est $x = 4$.
- Sa seule racine est 4.

Etape 2 : Trouver une solution homogène, sans tenir compte des conditions initiales

La solution homogène est $f(n) = c4^n$.

Etape 3 : Trouver une solution particulière, sans tenir compte des conditions initiales.

- On devine que la solution est de la forme $d3^n$, où d est une constante.
- En substituant, on obtient

$$\begin{aligned} d3^n &= 4d3^{n-1} + 3^n \\ 3d &= 4d + 3 \\ d &= -3 \end{aligned}$$

- On vérifie que $-3 \cdot 3^n = -3^{n+1}$ est bien une solution particulière.

Etape 4 : Former une solution générale, sans tenir compte des conditions initiales

On obtient la solution générale

$$f(n) = c4^n - 3^{n+1}.$$

Etape 5 : Déterminer les valeurs des constantes introduites à l'étape 2

$$\begin{aligned} f(1) = 1 &\Rightarrow c4^1 - 3^{1+1} = 1 \\ &\Rightarrow c = \frac{5}{2}. \end{aligned}$$

Conclusion : $f(n) = \frac{5}{2}4^n - 3^{n+1}$.

Changement de variables

Un changement de variables permet parfois de transformer une récurrence “diviser pour régner” en une récurrence linéaire.

Soit la récurrence du transparent 241 :

$$T(n) = 7T(n/2) + O(n^2)$$

En posant : $n = 2^m$ et $S(m) = T(2^m)$, on obtient :

$$S(m) = T(2^m) = 7T(2^{m-1}) + O((2^m)^2) = 7S(m-1) + O(4^m)$$

Résumé

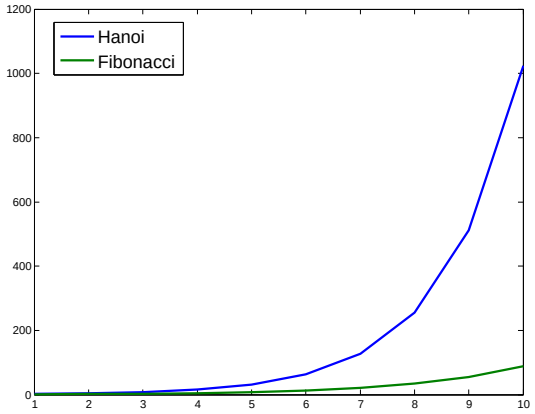
- Outils de résolution d'équations récurrentes :
  - Méthodes génériques : "Deviner-et-Vérifier", "Plug-and-Chug", arbres de récursion
  - Récurrences "Diviser pour régner" : théorème "Master", théorème d'Akra-Bazzi
  - Récurrences "linéaires"

  Les deux dernières sont les plus systématiques.
- Le plus dur reste de traduire un problème réel en une équation récurrente.
- Exemple : Soit un type de plante qui vit éternellement, mais qui peut seulement se reproduire la première année. A quelle vitesse la population croît-elle ?

Comparaison

	Récurrence	Solution
Tours de Hanoï	$T_n = 2T_{n-1} + 1$	$T_n \sim 2^n$
Tours de Hanoï 2	$T_n = 2T_{n-1} + n$	$T_n \sim 2 \cdot 2^n$
Algo rapide	$T_n = 2T_{n/2} + 1$	$T_n \sim n$
Tri par fusion	$T_n = 2T_{n/2} + n - 1$	$T_n \sim n \log n$
Fibonacci	$T_n = T_{n-1} + T_{n-2}$	$T_n \sim (1.618\ldots)^{n+1}/\sqrt{5}$

- Récurrences “Diviser pour régner” généralement polynomiales
- Récurrences linéaires généralement exponentielles



Chapitre 7

Techniques de dénombrement

Introduction

Objectifs de ce chapitre : Etudier des techniques de *dénombrement d'ensembles*.

Exemples d'applications pratiques :

- Déterminer le temps et l'espace requis pour résoudre un problème algorithmique donné ?
- Les techniques de dénombrement sont à la base de la théorie des probabilités (second semestre)
- A l'origine de deux techniques de démonstration importantes : le principe des tiroirs et les démonstrations combinatoires.

- Dans la séquence de 90 nombres à 25 chiffres ci-dessous, est-il possible de trouver deux sous-ensembles de nombres partageant la même somme ?

2048013538550296444803 8	3171004832173501394113017	5763257331083479647409398	8247331000042995311646021
4894459918669156762409 92	3208234421597368647019265	5800949123548989122628663	8496243997123475922766310
1082662032430379651370981	3437254656355157864869113	6042900801199280218026001	8518399140676002660747477
1178480894769706178994993	3574883393058653923711365	6116171789137737896701405	8543691283470191452333763
1253127351683239693851327	3644909946040480189969149	6144868973001582369723512	8675309258374137092461352
1301505129234077811069011	3790044132737084094417246	6247314593851169234746152	8694321112363996867296665
1311567111143866433882194	3870332127437971355322815	6814428944266874963488274	8772321203608477245851154
1470029452721203587686214	4080505804577801451363100	6870852945543886849147881	8791422161722582546341091
1578271047286257499433886	4167283461025702348124920	6914955508120950093732397	9062628024592126283973285
1638243921852176243192354	4235996831123777788211249	6949632451365987152423541	9137845566925526349897794
1763580219131985963102365	4670939445749439042111220	7128211143613619828415650	9153762966803189291934419
1826227795601842231029694	4815379351865384279613427	7173920083651862307925394	9270880194077636406984249
1843971862675102037201420	4837052948212922604442190	7215654874211755676220587	9324301480722103490379204
2396951193722134526177237	5106389423855018550671530	7256932847164391040233050	9436090832146695147140581
2781394568268599801096354	5142368192004769218069910	7332822657075235431620317	9475308159734538249013238
2796605196713610405408019	5181234096130144084041856	7426441829541573444964139	9492376623917486974923202
2931016394761975263190347	5198267398125617994391348	7632198126531809327186321	9511972558779880288252979
2933458058294405155197296	5317592940316231219758372	7712154432211912882310511	9602413424619187112552264
3075514410490975920315348	5384358126771794128356947	7858918664240262356610010	9631217114906129219461111
3111474985252793452860017	5439211712248901995423441	7898156786763212963178679	9908189853102753335981319
3145621587936120118438701	5610379826092838192760458	8147591017037573337848616	9913237476341764299813987
3148901255628881103198549	5632317555465228677676044	8149436716871371161932035	
3157693105325111284321993	5692168374637019617423712	8176063831682536571306791	

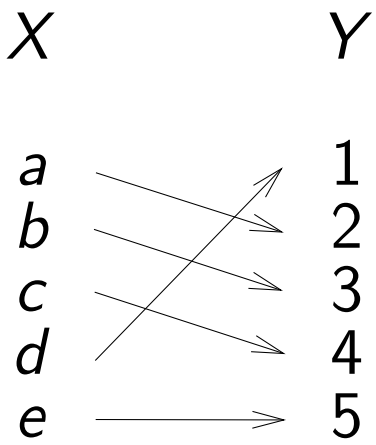
Bijections

Définition : Une fonction $f : X \longrightarrow Y$ est une *bijection* si et seulement si les deux conditions suivantes sont satisfaites :

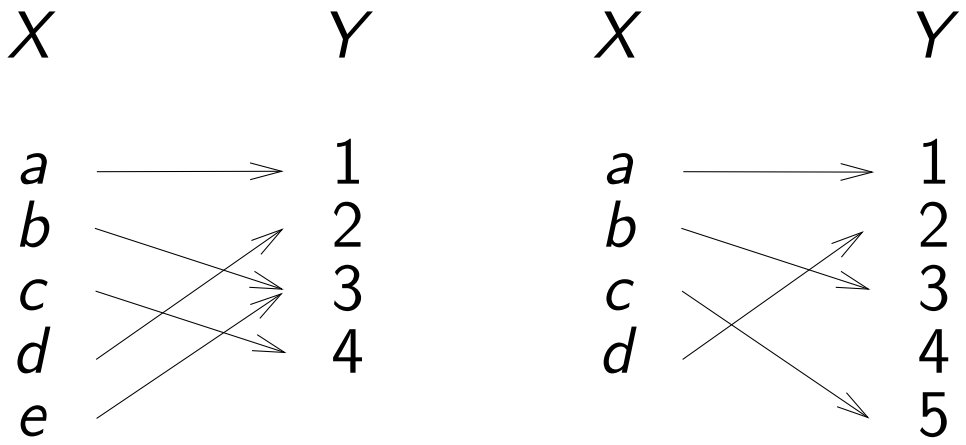
- $(\forall y \in Y)(\exists x \in X) \;\; (f(x) = y)$
- $(\forall x_1, x_2 \in X) \;\; [(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2)]$.

Exemples :

- La fonction représentée ci-dessous est une bijection.



- Les fonctions représentées ci-dessous ne sont pas des bijections.



Propriété : S'il existe une bijection $f : A \longrightarrow B$, alors $|A| = |B|$.

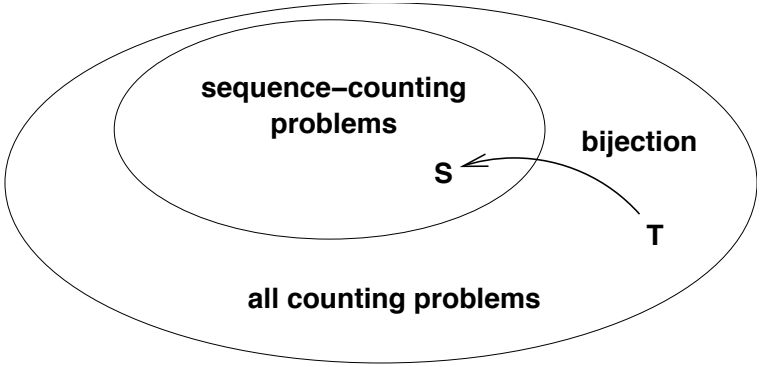
Application : Soient

- $A =$ l'ensemble des possibilités pour sélectionner 12 objets lorsqu'il en existe 5 sortes différentes ;
- $B =$ l'ensemble des séquences de 16 bits comportant exactement quatre "1".

On peut représenter biunivoquement les manières de sélectionner 12 objets parmi 5 sortes disponibles par les séquence de 16 bits comportant exactement quatre "1" :

$$\underbrace{00}_{\text{Sorte A}}\ 1\ \underbrace{\ }_{\text{Sorte B}}\ 1\ \underbrace{000000}_{\text{Sorte C}}\ 1\ \underbrace{00}_{\text{Sorte D}}\ 1\ \underbrace{00}_{\text{Sorte E}}$$

On a donc $|A| = |B|$.



Stratégie générale pour le dénombrement :

- Apprendre à compter certains types d'objets
- Utiliser la règle de bijection pour compter tout le reste

Dans ce cours, on va apprendre à dénombrer les *séquences*.

Une séquence est une collection ordonnée d'éléments (appelés composants ou termes).

Exemple : (a,b,c) et (c,b,a) sont deux séquences différentes

Produits cartésiens

Définition (rappel) : Si $P_1, P_2, \ldots, P_n$ sont des ensembles, alors le *produit cartésien*

$$P_1 \times P_2 \times \cdots \times P_n$$

est l'ensemble de toutes les séquences $(p_1, p_2, \ldots, p_n)$ avec $p_1 \in P_1$, $p_2 \in P_2$, $\ldots$, $p_n \in P_n$.

Propriété : Si $P_1, P_2, \ldots, P_n$ sont des ensembles, alors

$$|P_1 \times P_2 \times \cdots \times P_n| = |P_1| \cdot |P_2| \cdots |P_n|.$$

Application : sous-ensembles

Soit $X = \{x_1, x_2, \ldots, x_n\}$ un ensemble comportant n éléments.

Question : Combien existe-t-il de sous-ensembles de X ?

Exemple : L'ensemble $X = \{x_1, x_2, x_3\}$ admet 8 sous-ensembles :
$\{\}, \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}, \{x_1, x_2, x_3\}$.

Réponse : Bijection entre l'ensemble des sous-ensembles de X et les séquences de n bits :

$$S \mapsto (b_1, b_2, \ldots, b_n),$$

- $S \subseteq X$,
- $b_i = 1$ si et seulement si $x_i \in S$.

sous-ensemble :	$\{$		x_2,	x_3,		x_5,		x_7,		x_{10}	$\}$
séquence :	$($	0	1	1	0	1	0	1	0	0	1	$)$

Comme l'ensemble des séquences de n bits est $\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\} = \{0,1\}^n$, il en existe 2^n.

L'ensemble X admet donc 2^n sous-ensembles.

Unions disjointes

Propriété : Si $A_1, A_2, \ldots, A_n$ sont des ensembles disjoints, alors

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Remarque : Si les ensembles $A_1, A_2, \ldots, A_n$ ne sont pas nécessairement disjoints, alors le calcul de $|A_1 \cup A_2 \cup \cdots \cup A_n|$ est plus compliqué, et sera étudié plus tard.

Application : mots de passe

Considérons un programme dans lequel un mot de passe est dit valide si

- il contient entre 6 et 8 caractères,
- son premier caractère est une lettre (majuscule ou minuscule), et
- les autres caractères sont soit des lettres, soit des chiffres.

Question : Combien existe-t-il de mots de passe valides ?

Réponse : Définissons F et S par

- $F = \{a, b, \ldots, z, A, B, \ldots, Z\}$,
- $S = \{a, b, \ldots, z, A, B, \ldots, Z, 0, 1, \ldots, 9\}$.

L'ensemble des mots de passe valides est

$$(F \times S^5) \cup (F \times S^6) \cup (F \times S^7).$$

Comme $(F \times S^5)$, $(F \times S^6)$ et $(F \times S^7)$ sont disjoints, on a

$$\begin{aligned} & |(F \times S^5) \cup (F \times S^6) \cup (F \times S^7)| \\ = \; & |(F \times S^5)| + |(F \times S^6)| + |(F \times S^7)| \\ = \; & 52 \cdot 62^5 + 52 \cdot 62^6 + 52 \cdot 62^7 \\ \approx \; & 1,8 \cdot 10^{14} \text{ mots de passe valides.} \end{aligned}$$

Principe des tiroirs (Pigeonhole principle)

Principe des tiroirs : Si $|X| > |Y|$, alors, pour toute fonction $f : X \to Y$, il existe deux éléments distincts de X qui sont associés au même élément de Y.

Source : `http ://en.wikipedia.org/wiki/Pigeonhole_principle`

Exemples

- Si n chaussettes occupent m tiroirs, et si $n > m$, alors au moins un tiroir doit contenir strictement plus d'une chaussette. *(version française du "pigeonhole principe")*
- Un tiroir dans une chambre sombre contient des chaussettes rouges, des chaussettes vertes et des chaussettes bleues. Combien faut-il en retirer du tiroir pour être sûr d'avoir deux chaussettes de la même couleur ?
- S'il y a n personnes qui se serrent la main ($n > 1$), il y a toujours deux personnes qui saluent le même nombre de personnes.
- Tout algorithme de compression sans perte ne fonctionnera pas pour certaines entrées (le taux de compression sera inférieur à 1).

Principe des tiroirs généralisé : Si $|X| > k \cdot |Y|$, alors toute fonction $f : X \to Y$ fait correspondre au moins $k + 1$ éléments distincts de X vers le même élément de Y.

Exemple : Démontrons qu'au moins 5 liégeois ont exactement le même nombre de cheveux

- Environ 900.000 personnes habitant la province de Liège ne sont pas chauves. Soit A cet ensemble.
- Le nombre de cheveux sur une personne est au plus de 200.000. Soit $B = \{1, 2, \ldots, 200.000\}$.
- On a $|A| > 4 \cdot |B|$.
- Dès lors, au moins 5 liégeois ont exactement le même nombre de cheveux.

Application : sous-ensembles partageant la même somme

- Dans la séquence de 90 nombres à 25 chiffres ci-dessous, est-il possible de trouver deux sous-ensembles de nombres partageant la même somme ?

20480135385502964448038	31710048321735013941130 17	57632573310834796474093 98	82473310000429953116460 21
48944599186691567624099 2	32082344215973686470192 65	58009491235489891226286 63	84962439971234759227663 10
10826620324303796513709 81	34372546563551578648691 13	60429008011992802180260 01	85183991406760026607474 77
11784808947697061789949 93	35748833930586539237113 65	61161717891377378967014 05	85436912834701914523337 63
12531273516832396938513 27	36449099460404801899691 49	61448689730015823697235 12	86753092583741370924613 52
13015051292340778110690 11	37900441327370840944172 46	62473145938511692347461 52	86943211123639968672966 65
13115671111438664338821 94	38703321274379713553228 15	68144289442668749634882 74	87723212036084772458511 54
14700294527212035876862 14	40805058045778014513631 00	68708529455438868491478 81	87914221617225825463410 91
15782710472862574994338 86	41672834610257023481249 20	69149555081209500937323 97	90626280245921262839732 85
16382439218521762431923 54	42359968311237777882112 49	69496324513659871524235 41	91378455669255263498977 94
17635802191319859631023 65	46709394457494390421112 20	71282111436136198284156 50	91537629668031892919344 19
18262277956018422310296 94	48153793518653842796134 27	71739200836518623079253 94	92708801940776364069842 49
18439718626751020372014 20	48370529482129226044421 90	72156548742117556762205 87	93243014807221034903792 04
23969511937221345261772 37	51063894238550185506715 30	72569328471643910402330 50	94360908321466951471405 81
27813945682685998010963 54	51423681920047692180699 10	73328226570752354316203 17	94753081597345382490132 38
27966051967136104054080 19	51812340961301440840418 56	74264418295415734449641 39	94923766239174869749232 02
29310163947619752631903 47	51982673981256179943913 48	76321981265318093271863 21	95119725587798802882529 79
29334580582944051551972 96	53175929403162312197583 72	77121544322119128823105 11	96024134246191871125522 64
30755144104909759203153 48	53843581267717941283569 47	78589186642402623566100 10	96312171149061292194611 11
31114749852527934528600 17	54392117122489019954234 41	78981567867632129631786 79	99081898531027533359813 19
31456215879361201184387 01	56103798260928381927604 58	81475910170375733378486 16	99132374763417642998139 87
31489012556288811031985 49	56323175554652286776760 44	81494367168713711619320 35	
31576931053251112843219 93	56921683746370196174237 12	81760638316825365713067 91	

- Considérons un ensemble S de 90 nombres à 25 chiffres.
- Soit A l'ensemble des sous-ensembles de S.
- Soit B l'ensemble des sommes potentielles.
- Il y a $|A| = 2^{90}$ sous-ensembles possibles. On a $2^{90} \geq 1,237 \cdot 10^{27}$.
- La somme de tout sous-ensemble vaut au maximum $90 \cdot 10^{25}$. Les sommes potentielles sont donc $B = \{0, 1, \ldots, 90 \cdot 10^{25}\}$. Il y en a $90 \cdot 10^{25} + 1 \leq 0,901 \cdot 10^{27}$.
- On a $|A| > |B|$.
- Par le principe des tiroirs, deux sous-ensembles partagent la même somme.

Produits cartésiens généralisés

Propriété : Soit S un ensemble de séquences, chacune de longueur k. S'il y a

- n_1 possibilités pour les premiers éléments,
- n_2 possibilités pour les deuxièmes éléments quand le premier élément est fixé,
- n_3 possibilités pour les troisièmes éléments quand le premier et le deuxième élément sont fixés, etc.,

alors

$$|S| = n_1 \cdot n_2 \cdot n_3 \ldots n_k.$$

Application : permutations

Définition : Une *permutation* d'un ensemble S est une séquence qui contient chaque élément de S exactement une fois.

Exemple : Les permutations de l'ensemble $\{a, b, c\}$ sont

$$(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a).$$

Question : Considérons un ensemble de n éléments. Combien de permutations de cet ensemble existe-t-il ?

Réponse :

- Il y a n choix possibles pour le premier élément.
- Pour chacun d'entre-eux, il y a $n-1$ choix possibles pour le deuxième élément.
- Une fois que les deux premiers éléments sont fixés, il y a $n-2$ possibilités pour le troisième élément, etc.
- Il y a donc

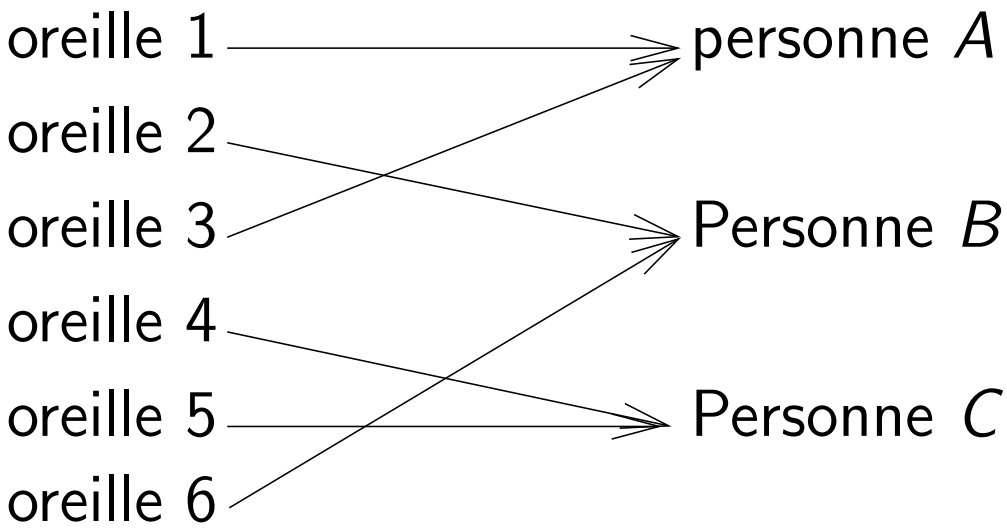
$$n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1 = n!$$

permutations possibles pour un ensemble à n éléments.

Règle de division

Définition : Soit $f : X \to Y$ une fonction. Cette fonction est une *fonction k-vers-1* si et seulement si elle fait correspondre exactement k éléments de X vers chaque élément de Y.

Exemple de fonction 2-vers-1 :

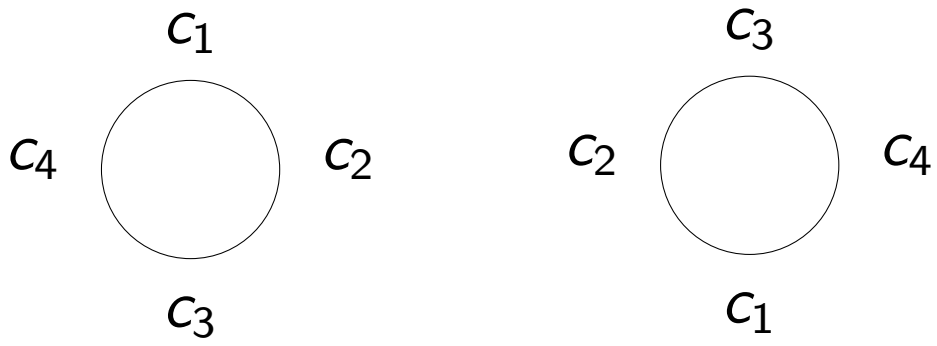


Propriété : Si $f : X \to Y$ est une fonction k-vers-1, alors $|X| = k \cdot |Y|$.

Application : permutations cycliques

Question : De combien de manières peut-on disposer n personnes autour d'une table ronde ?

Remarque : Les deux dispositions suivantes sont équivalentes :



Réponse :

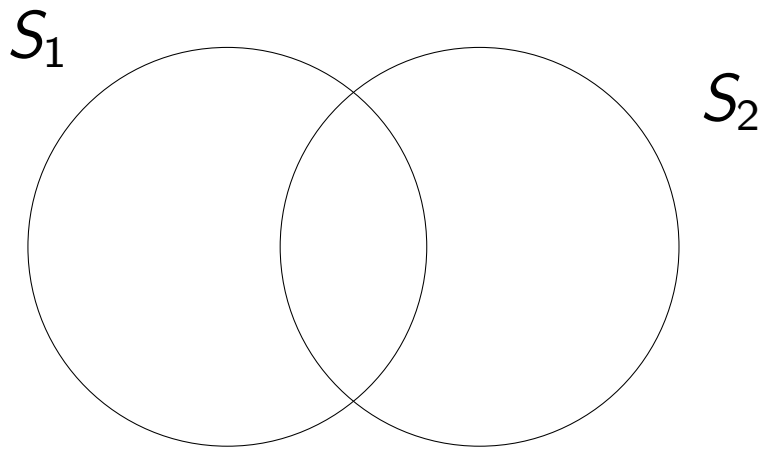
- Soit A l'ensemble des *permutations* des n personnes.
- Soit B l'ensemble des *dispositions* possibles.
- Soit $f : A \longrightarrow B$ la fonction qui fait correspondre les permutations aux dispositions correspondantes.
- Cette fonction est une fonction n-vers-1.
- Par la règle de division, on obtient

$$\begin{aligned} |B| &= \frac{|A|}{n} \\ &= \frac{n!}{n} \\ &= (n-1)! \end{aligned}$$

Union de deux ensembles

Propriété : Soit S_1 et S_2 deux ensembles non nécessairement disjoints. On a

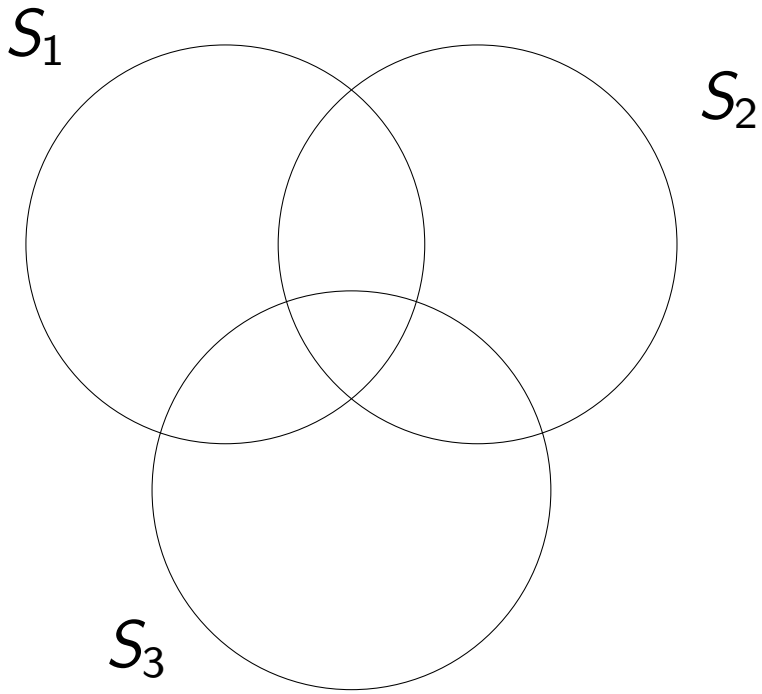
$$|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|.$$



Union de trois ensembles

Propriété : Soient S_1, S_2 et S_3 trois ensembles non nécessairement disjoints. On a

$$\begin{aligned} |S_1 \cup S_2 \cup S_3| &= |S_1| + |S_2| + |S_3| \\ &\quad -|S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| \\ &\quad +|S_1 \cap S_2 \cap S_3|. \end{aligned}$$



Application

Considérons les permutations de l'ensemble $\{0, 1, 2, \ldots, 9\}$ dans lesquelles au moins une des conditions suivantes est satisfaite :

- 4 précède directement 2,
- 0 précède directement 4, ou
- 6 précède directement 0.

Question : Combien existe-t-il de telles permutations ?

Réponse :

- Soient P_{42}, P_{60} et P_{04} l'ensemble des permutations dans lesquelles 42, 60 et 04 apparaissent respectivement.
- Il existe une bijection entre P_{42} et l'ensemble des permutations de $\{42, 0, 1, 3, 5, 6, 7, 8, 9\}$. On a donc $|P_{42}| = 9!$.
- Idem pour $P_{60} = P_{04} = 9!$.
- Il existe une bijection entre $P_{42} \cap P_{60}$ et l'ensemble des permutations de $\{42, 60, 1, 3, 5, 7, 8, 9\}$. On a donc $|P_{42} \cap P_{60}| = 8!$.
- Il existe une bijection entre $P_{60} \cap P_{04}$ et l'ensemble des permutations de $\{604, 1, 2, 3, 5, 7, 8, 9\}$. On a donc $|P_{60} \cap P_{04}| = 8!$.
- On a aussi $|P_{42} \cap P_{04}| = 8!$ et $|P_{60} \cap P_{04} \cap P_{42}| = 7!$.
- On obtient $|P_{42} \cup P_{04} \cup P_{60}| = 9! + 9! + 9! - 8! - 8! - 8! + 7!$.

Union de n ensembles

Propriété (Principe d'inclusion-exclusion) : Soient $S_1, S_2, \ldots, S_n$ des ensembles non nécessairement disjoints. On a

$$
\begin{aligned}
& |S_1 \cup S_2 \cup \cdots \cup S_n| \\
= \quad & \text{la somme des tailles des ensembles individuels} \\
- \quad & \text{la somme des tailles des intersections de 2 ensembles} \\
+ \quad & \text{la somme des tailles des intersections de 3 ensembles} \\
- \quad & \text{la somme des tailles des intersections de 4 ensembles} \\
+ \quad & \ldots
\end{aligned}
$$

Plus formellement :

$$\left|\bigcup_{i=1}^{n} S_i\right| = \sum_{\emptyset \neq I \subseteq \{1,\ldots,n\}} (-1)^{|I|+1} \left|\bigcap_{i \in I} S_i\right|$$

Calcul de la fonction indicatrice d'Euler

Rappel : La fonction indicatrice d'Euler $\phi(n)$ désigne le nombre d'entiers de $\{0, 1, 2, \ldots, n-1\}$ premiers avec n.

On peut calculer $\phi(n)$ par le principe d'inclusion-exclusion.

- Soit S l'ensemble des entiers non négatifs plus petits que n qui *ne* sont *pas* premiers avec n. On a $\phi(n) = n - |S|$.
- Supposons la factorisation suivante de n :

$$n = p_1^{e_1} \ldots p_m^{e_m},$$

où p_i sont des nombres premiers distincts.

- Soit C_a l'ensemble des entiers positifs plus petit que n et divisible par a, on a :

$$S = \bigcup_{i=1}^{m} C_{p_i}$$

- Les tailles des intersections entre C_{p_i} sont faciles à calculer.
- Par exemple, $C_{p_i} \cap C_{p_j} \cap C_{p_k}$ est l'ensemble des entiers ($< n$) divisibles par p_i,p_j et p_k. Comme p_i, p_j et p_k sont des premiers distincts, $C_{p_i} \cap C_{p_j} \cap C_{p_k}$ est l'ensemble des entiers ($< n$) divisibles par $p_i \cdot p_j \cdot p_k$:

$$|C_{p_i} \cap C_{p_j} \cap C_{p_k}| = \frac{n}{p_i p_j p_k}.$$

- En appliquant le principe d'inclusion-exclusion, on obtient :

$$\begin{aligned} |S| &= \left| \bigcup_{i=1}^{m} C_{p_i} \right| \\ &= \sum_{i=1}^{m} |C_{pi}| - \sum_{1 \le i < j \le m} |C_{p_i} \cap C_{p_j}| \\ &\quad + \sum_{1 \le i < j < k \le m} |C_{p_i} \cap C_{p_j} \cap C_{p_k}| - \ldots + (-1)^{m-1} \left| \bigcap_{i=1}^{m} C_{p_i} \right| \end{aligned}$$

$$|S| = n\left(\sum_{i=1}^{m}\frac{1}{p_i} - \sum_{1\le i<j\le m}\frac{1}{p_i p_j} + \sum_{1\le i<j<k\le m}\frac{1}{p_i p_j p_k} - \ldots + (-1)^{m-1}\frac{1}{p_1 p_2 \ldots p_m}\right)$$

- Finalement, on a

$$\begin{aligned}\phi(n) &= n - |S| \\ &= n\left(1 - \sum_{i=1}^{m}\frac{1}{p_i} + \sum_{1\le i<j\le m}\frac{1}{p_i p_j} - \ldots + (-1)^m\frac{1}{p_1 p_2 \ldots p_m}\right) \\ &= n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right).\end{aligned}$$

- En remplaçant n par sa factorisation :

$$\begin{aligned}\phi(n) &= \prod_{i=1}^{m} p_i^{e_i}\left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^{m}(p_i^{e_i} - p_i^{e_i-1}).\end{aligned}$$

Combinaisons

Combien de sous-ensembles de taille k peut-on tirer dans un ensemble de n éléments distincts ?

Exemples :

- De combien de manière puis-je choisir 5 livres dans ma collection de 100 livres ?
- Combien ai-je de chance de gagner le gros lot au lotto en choisissant mes 6 numéros complètement au hasard ?

On note ce nombre C_n^k (ou bien $\binom{n}{k}$ en notation anglo-saxone).

Propriété : Le nombre de sous-ensembles de taille k d'un ensemble à n éléments est

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

Dérivation de C_n^k

Par la règle des produits cartésiens généralisés, le nombre de séquences construites à partir de k éléments distincts tirés d'un ensemble de taille n est :

$$n \cdot (n-1) \cdot (n-2) \ldots (n-k+1) = \frac{n!}{(n-k)!}$$

Il existe une fonction $k!$-vers-1 de chaque séquence vers l'ensemble des éléments qu'elle contient :

$$(x_1, x_2, x_3) \longrightarrow \{x_1, x_2, x_3\}$$

Par la règle de division, on obtient :

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

Dérivation alternative

- Le nombre de permutations de n éléments est $n!$.
- Soit la fonction f qui fait correspondre chaque permutation à l'ensemble de ses k premiers éléments.
- Toutes les permutations avec les mêmes k premiers éléments (en ordre quelconque) et les mêmes $n-k$ derniers éléments (en ordre quelconque) sont envoyés par f sur le même ensemble de k éléments.
- f est donc une fonction $n!(n-k)!$-vers-1
- Par la règle de division : $C_n^k = \frac{n!}{n!(n-k)!}$.

Séquences de bits

Combien de séquences de n bits contiennent exactement k "1" ?

Il existe une bijection entre ces séquences et les sous-ensembles de k éléments choisis parmi n.

Exemple : $k = 5$, $n = 10$

sous-ensemble :	$\{$		x_2,	x_3,		x_5,		x_7,		x_{10}	$\}$
séquence :	(	0	1	1	0	1	0	1	0	0	1)

Corollaire : Le nombre de séquences de n bits avec exactement k "1" est C_n^k.

Application

On a montré (slide 280) qu'il existait une bijection entre :

- A=L'ensemble des manières de sélectionner 12 objets lorsqu'il en existe 5 sortes différentes ;
- B=L'ensemble des séquences de 16 bits comportant exactement quatre "1".

$$\underbrace{00}_{\text{Sorte A}}\ 1\ \underbrace{\ }_{\text{Sorte B}}\ 1\ \underbrace{000000}_{\text{Sorte C}}\ 1\ \underbrace{00}_{\text{Sorte D}}\ 1\ \underbrace{00}_{\text{Sorte E}}$$

On a donc $|A| = |B| = C_{16}^4$.

Combinaisons avec répétitions

On peut généraliser pour conclure qu'il existe une bijection entre :

- A=L'ensemble des manières de sélectionner k éléments avec répétition parmi n (*combinaisons avec répétition*) ;
- B=L'ensemble des séquences de $n+k-1$ bits comportant exactement $n-1$ "1".

On a donc $|A| = |B| = C_{n+k-1}^{n-1} = C_{n+k-1}^{k}$.

Propriété : Le nombre de combinaisons avec répétitions de k éléments choisis parmi n est :

$$C_{n+k-1}^{k} = \frac{(n+k-1)!}{k!(n-1)!}.$$

Séquences de sous-ensembles

C_n^k est aussi le nombre de manière de diviser un ensemble de n éléments en deux sous-ensembles l'un de taille k, l'autre de taille $n - k$.

Combien y a-t'il de partitions possibles d'un ensemble de n éléments en m sous-ensembles de tailles respectives k_1, k_2, $\ldots$, k_n ?

Propriété : Le nombre de sous-ensembles de taille k d'un ensemble à n éléments est

$$\frac{n!}{k_1!k_2!\ldots k_m!}.$$

On note ces nombres $\binom{n}{k_1,k_2,\ldots,k_m}$ et on les appelle les coefficients multinomiaux.

Dérivation

- Soit un ensemble A de n éléments.
- On peut faire correspondre une permutation $(a_1, a_2, \ldots, a_n)$ de A à une séquence $(A_1, A_2, \ldots, A_m)$ de m sous-ensembles de tailles respectives $k_1, k_2, \ldots, k_m$ en prenant les k_1 premiers éléments comme sous-ensemble A_1, les k_2 éléments suivants comme sous-ensemble A_2,..., et les k_m derniers éléments comme sous-ensemble A_m.
- Toute permutation qui ne modifie pas la répartition des éléments dans les m blocs est envoyée vers la même partition.
- La correspondance est donc $k_1!k_2!\ldots k_m!$-vers-1.
- Par la règle de division, on obtient :

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1!k_2!\ldots k_m!}.$$

Application : séquences avec répétitions

De combien de façons distinctes peut-on arranger les lettres du mot *BOOKKEEPER* ?

Réponse :

- Il y a un B, deux O, deux K, trois E, un P et un R dans *BOOKKEEPER*.
- Il existe une bijection entre les arrangements de *BOOKKEEPER* et les partitions de $\{1, 2, \ldots, 10\}$ en 6 sous-ensembles de tailles respectives $1, 2, 2, 3, 1, 1$.
- Exemple :
  $$BOOKKEEPER \to (\underbrace{\{1\}}_{B}, \underbrace{\{2,3\}}_{O}, \underbrace{\{4,5\}}_{K}, \underbrace{\{6,7,9\}}_{E}, \underbrace{\{8\}}_{P}, \underbrace{\{10\}}_{R})$$
- Le nombre d'arrangements est :
  $$\frac{10!}{1!2!2!3!1!1!} = 151200$$

Règle du bookkepper

Propriété : Le nombre de séquences contenant n_1 copies de l_1, n_2 copies de l_2, ..., et n_k copies de l_k est

$$\frac{(n_1 + n_2 + \ldots + n_k)!}{n_1! n_2! \ldots n_k!},$$

pour autant que $l_1, l_2, \ldots, l_k$ soient distincts.

Binôme de Newton

Question : Quel est le coefficient de $a^{n-k}b^k$ dans le développement de $(a+b)^n$?

Exemple :

$$\begin{aligned}(a+b)^4 &= aaaa + aaab + aaba + aabb \\ &\quad + abaa + abab + abba + abbb \\ &\quad + baaa + baab + baba + babb \\ &\quad + bbaa + bbab + bbba + bbbb\end{aligned}$$

Observation : Il y a un terme pour chaque séquence, de longueur n, composée de a et de b.

Réponse : Le nombre de termes contenant k copies de b et $n-k$ copies de a est donc

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

Théorème : Pour tous $n \in \mathbb{N}$ et $a, b \in \mathbb{R}$, on a

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

Formule du multinôme de Newton

Théorème : Pour tous $n \in \mathbb{N}$, on a

$$(z_1+z_2+\ldots+z_m)^n = \sum_{k_1,\ldots,k_m \in \mathbb{N} | k_1+\ldots+k_m=n} \binom{n}{k_1, k_2, \ldots, k_m} z_1^{k_1} z_2^{k_2} \ldots z_m^{k_m}$$

Exemple : $\binom{10}{1,2,2,3,1,1}$ est le coefficient de $bo^2k^2e^3pr$ dans le développement de $(b+o+k+e+p+r)^{10}$.

Mains de poker

- Dans un jeu de cartes, il y a 52 cartes.
- Chaque carte a une couleur et une valeur.
- Couleurs possibles : $\spadesuit, \heartsuit, \clubsuit, \diamondsuit$.
- Valeurs possibles : 2,3,4,5,6,7,8,9,V,D,R,A.
- Une main est un ensemble de 5 cartes parmi les 52 disponibles.
- Nombre total de mains : $C_{52}^5 = 2.598.960$.

- Un carré est une main contenant 4 cartes de la même valeur.
- Exemple : $\{8\spadesuit, 8\diamondsuit, D\heartsuit, 8\heartsuit, 8\clubsuit\}$.
- Un carré est caractérisé par
  - La valeur des 4 cartes ;
  - La valeur de la carte supplémentaire ;
  - La couleur de la carte supplémentaire.
- L'ensemble des carrés peut être mis en bijection avec l'ensemble des séquences composées de deux valeurs distinctes suivies d'une couleur.
- Exemple : $(8, D, \heartsuit) \leftrightarrow \{8\spadesuit, 8\diamondsuit, D\heartsuit, 8\heartsuit, 8\clubsuit\}$.
- Il y a donc $13 \cdot 12 \cdot 4 = 624$ mains contenant un carré (une sur 4165).

- Une main pleine est une main contenant 3 cartes d'une valeur et deux cartes d'une autre valeur.
- Exemple : $\{2\spadesuit, 2\clubsuit, 2\diamondsuit, V\clubsuit, V\diamondsuit\}$.
- Une main pleine est caractérisée par
  - La valeur du brelan (3 cartes d'une même valeur) ;
  - Les couleurs du brelan ;
  - La valeur de la paire ;
  - Les couleurs de la paire.
- Il y a donc

$$13 \cdot \underbrace{C_4^3}_{4} \cdot 12 \cdot \underbrace{C_4^2}_{6} = 3.744$$

mains pleines différentes.

- Une double paire est une main contenant 2 cartes d'une valeur et deux cartes d'une autre valeur.
- Exemple : $\{3\diamondsuit, 3\spadesuit, D\diamondsuit, D\heartsuit, A\clubsuit\}$.
- Une double paire est caractérisée par
  - Les valeurs des deux paires ;
  - Les couleurs de la première paire ;
  - Les couleurs de la deuxième paire ;
  - La valeur de la carte supplémentaire ;
  - La couleur de la carte supplémentaire.
- Il y a donc

$$\underbrace{C_{13}^2}_{78} \cdot \underbrace{C_4^2}_{6} \cdot \underbrace{C_4^2}_{6} \cdot 11 \cdot \underbrace{C_4^1}_{4} = 123.552$$

doubles paires différentes.

- Combien de mains contiennent au moins une carte de chaque couleur ?
- Exemple : $\{7\diamondsuit, R\clubsuit, 3\diamondsuit, A\heartsuit, 2\spadesuit\}$.
- Une telle main est décrite par
  - Les valeurs du $\diamondsuit$, du $\clubsuit$, du $\heartsuit$ et du $\spadesuit$;
  - La couleur de la carte supplémentaire ;
  - La valeur de la carte supplémentaire.
- Remarque :

$$\begin{matrix}(7, R, A, 2, \diamondsuit, 3) \\ (3, R, A, 2, \diamondsuit, 7)\end{matrix} \rightarrow \{7\diamondsuit, R\clubsuit, A\heartsuit, 2\spadesuit, 3\diamondsuit\}$$

- Il s'agit d'une correspondance 2-vers-1.
- Le nombre de possibilités est donc de $\dfrac{13^4 \cdot 4 \cdot 12}{2}$.

Démonstrations combinatoires

Définition : Une *démonstration combinatoire* est un argument qui établit une propriété algébrique en utilisant des techniques de dénombrement.

Théorème : $C_n^k = C_n^{n-k}$.

Démonstration algébrique :

- $C_n^k = \dfrac{n!}{k!(n-k)!}$
- $C_n^{n-k} = \dfrac{n!}{(n-k)!(n-(n-k))!} = \dfrac{n!}{k!(n-k)!}$ □

Démonstration combinatoire : *Sélectionner k objets parmi n est équivalent à déterminer les $n-k$ objets qui ne seront pas choisis.* □

Question : Un concours est organisé, et, parmi un ensemble de n personnes (dont une personne A), k personnes doivent être sélectionnées pour y participer. Combien de sélections possibles existe-t-il ?

Réponse 1 :

- Si A est sélectionné, il reste $k-1$ personnes à sélectionner parmi les $n-1$ restantes : C_{n-1}^{k-1} possibilités.
- Si A n'est pas sélectionné, il reste k personnes à sélectionner parmi les $n-1$ restantes : C_{n-1}^{k} possibilités.
- Les deux ensembles d'équipes sont disjoints.
- On a donc $C_{n-1}^{k-1} + C_{n-1}^{k}$ possibilités.

Réponse 2 :

- Il y a k personnes à sélectionner parmi n.
- Le nombre de sélections possibles vaut donc C_n^k.

Conclusion (Formule de Pascal) :

$$C_{n-1}^{k-1} + C_{n-1}^{k} = C_n^k.$$

Une démonstration plus formelle

- Soit S l'ensemble de tous les sous-ensembles de taille k des entiers $\{1, \ldots, n\}$.
- On sait déjà que $|S| = C_n^k$.
- Soient les deux ensembles suivants :

$$\begin{aligned} A &= \{(1, X) | X \subseteq \{2, \ldots, n\} \wedge |X| = k - 1\} \\ B &= \{(0, Y) | Y \subseteq \{2, \ldots, n\} \wedge |Y| = k\} \end{aligned}$$

- A et B sont clairement disjoints (le premier élément de la paire est différent) et donc :

$$|A \cup B| = |A| + |B|,$$

avec

$$\begin{aligned} |A| &= C_{n-1}^{k-1} \\ |B| &= C_{n-1}^{k} \end{aligned}$$

- Soit la fonction $f : (A \cup B) \to S$:

$$f(c) = \begin{cases} X \cup \{1\} & \text{si } c = (1, X), \\ Y & \text{si } c = (0, Y). \end{cases}$$

- f est une bijection de $A \cup B$ vers S.
- On a donc $|S| = |A| + |B|$, ce qui prouve le théorème. □

Un modèle pour les démonstrations combinatoires

1. Définir un ensemble S ;
2. Démontrer que $|S| = n$ en le dénombrant d'une manière ;
3. Démontrer que $|S| = m$ en le dénombrant d'une autre manière ;
4. Conclure que $|S| = n = m$.

Application

Théorème :

$$\sum_{r=0}^{n} C_n^r C_{2n}^{n-r} = C_{3n}^n.$$

Démonstration (combinatoire) :

- Soit S l'ensemble des mains à n cartes qui peuvent être obtenues en mélangeant
  - un jeu de n cartes rouges (numérotées $1, 2, \ldots, n$)
  - avec un jeu de $2n$ cartes noires (numérotées $1, 2, \ldots, 2n$).
- D'une part, on a

$$|S| = C_{3n}^n.$$

- D'autre part :
  - Le nombre de mains contenant exactement r cartes rouges est
$$C_n^r C_{2n}^{n-r}.$$
  - Le nombre de cartes rouges est compris entre 0 et n.
  - Le nombre total de mains à n cartes vaut donc :
$$|S| = \sum_{r=0}^{n} C_n^r C_{2n}^{n-r}.$$

□

Remarque : Pour démontrer une égalité de manière combinatoire, il est souvent plus facile de définir l'ensemble S sur base du membre ayant la forme la plus simple, comme dans l'exemple précédent.

Un tour de magie

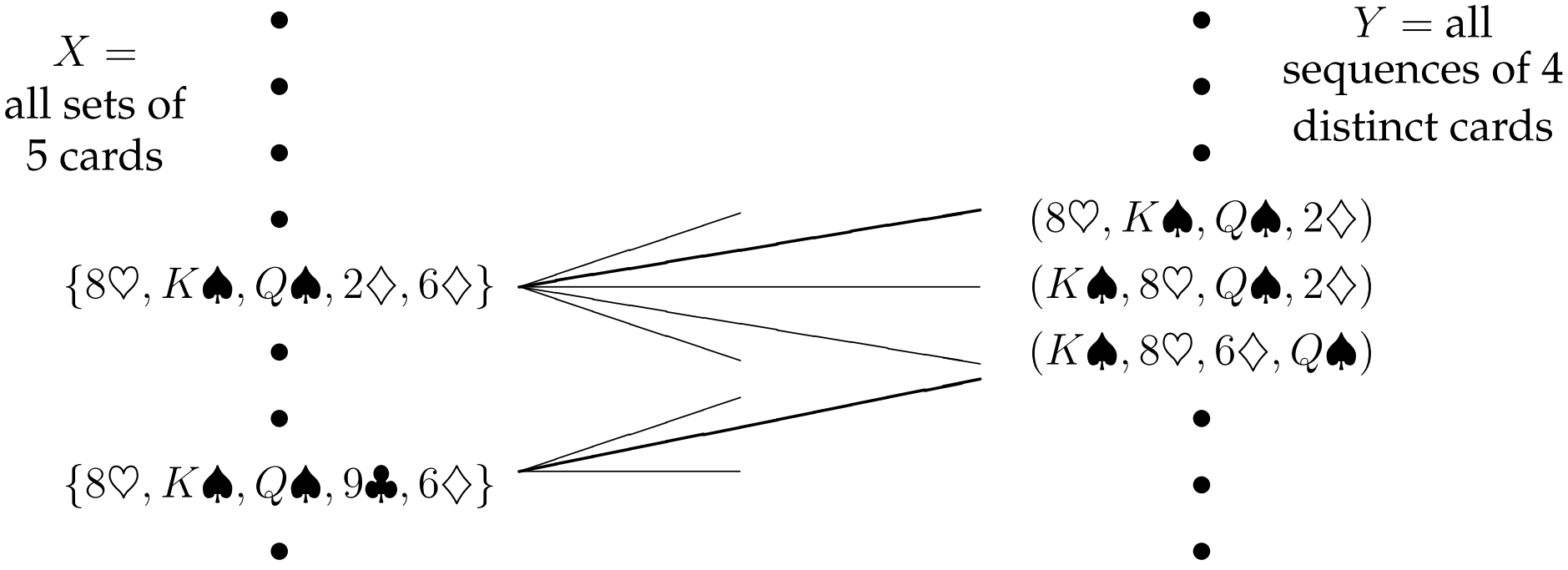
- Un magicien envoie son assistant dans le public avec un jeu de carte
- 5 personnes choisissent une carte dans le jeu
- L'assistant révèle 4 de ces 5 cartes
- Le magicien annonce la carte restante

Première idée

- L'assistant et le magicien conviennent d'un ordre sur les cartes
- Exemple :
  $1\heartsuit < \ldots < R\heartsuit < 1\clubsuit < \ldots < 1\diamondsuit < \ldots < 1\spadesuit < \ldots$
- L'assistant pourrait coder la carte manquante par l'ordre dans lequel les 4 cartes sont présentées.
- Exemple : $(1,2,3,4) \rightarrow 1\heartsuit$, $(1,2,4,3) \rightarrow 2\heartsuit$, etc.
- Problème : il n'y a que $4! = 24$ ordres possibles alors qu'il faut pouvoir coder 48 cartes

Le secret

- L'assistant peut choisir la carte qui va rester cachée et l'ordre dans lequel les 4 cartes seront dévoilées.
- Soit X tous les ensembles de 5 cartes (*non ordonnées*) et Y tous les séquences de 4 cartes distinctes (*ordonnées*)
- Définissons un graphe biparti entre X et Y : $x \in X$ est connecté à $y \in Y$ si les 4 cartes de la séquence y sont dans l'ensemble x.
- Pour que le codage de la cinquième carte soit possible à partir d'une séquence de 4 cartes, il faut qu'une correspondance existe dans le graphe biparti entre X et Y (c'est-à-dire une association de chaque $x \in X$ avec un élément distinct de Y).


$X =$
all sets of
5 cards
$\{8\heartsuit, K\spadesuit, Q\spadesuit, 2\diamondsuit, 6\diamondsuit\}$
$\{8\heartsuit, K\spadesuit, Q\spadesuit, 9\clubsuit, 6\diamondsuit\}$
$Y =$ all
sequences of 4
distinct cards
$(8\heartsuit, K\spadesuit, Q\spadesuit, 2\diamondsuit)$
$(K\spadesuit, 8\heartsuit, Q\spadesuit, 2\diamondsuit)$
$(K\spadesuit, 8\heartsuit, 6\diamondsuit, Q\spadesuit)$

- On doit montrer que la condition du théorème de Hall est vérifiée.

- Théorème de Hall (rappel) : Soit $G = (L \cup R, E)$ un graphe biparti tel que toute arête a une extrémité dans L et l'autre extrémité dans R. Il existe une correspondance pour les sommets de L si et seulement si $|S| \leq |N(S)|$ pour tout $S \subseteq L$
  ($N(S)$ est l'ensemble des sommets n'appartenant pas à S, mais adjacents à au moins un sommet de S).

- Définition : Un graphe biparti G est de *degré contraint* si $\deg(l) \geq \deg(r)$ pour tout $l \in L(G)$ et $r \in R(G)$

Théorème : Soit G un graphe biparti de degré contraint. Il existe une correspondance pour les sommets de L.

Démonstration :

- Montrons que G satisfait la condition de Hall.
- Vu la contrainte de degré, il existe d tel que $\deg(l) \geq d \geq \deg(r)$ pour tout $l \in L$ and $r \in R$.
- Soit $S \subseteq L$ un sous-ensemble de L.
- Tout sommet de $N(S)$ est incident à au plus d arêtes :

$$d|N(S)| \geq \text{“Nb arêtes incidentes à S”}.$$

- Tout sommet de S est l'extrémité d'au moins d arêtes :

$$\text{“Nb arêtes incidentes à S”} \geq d|S|.$$

- En combinant, on a $d|N(S)| \geq d|S|$ et donc $|N(S)| \geq |S|$. □

- Dans le graphe biparti qui nous intéresse, chaque nœud de gauche est de degré $120 (= 5 \cdot 4!)$ et chaque noeud de droite est de degré 48.
- Le graphe est donc de degré contraint et donc, par le théorème précédent, il existe une correspondance pour les sommets de gauche
- En s'accordant sur cette correspondance, le magicien et l'assistant peuvent réaliser leur tour.

- Problème : Il y a $C_{52}^5 \approx 2600000$ correspondances à mémoriser. Impossible sans un truc supplémentaire.

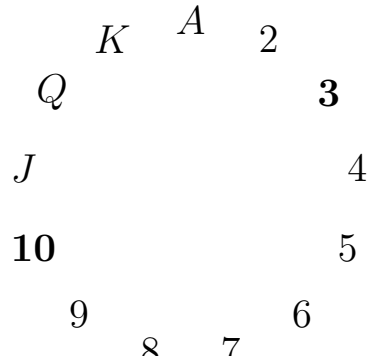
Le vrai truc

Un exemple de codage facile à retenir :

Exemple : Supposons que les 5 cartes soient :

$$10\heartsuit \quad 9\diamondsuit \quad 3\heartsuit \quad D\spadesuit \quad V\diamondsuit$$

- L'assistant choisit 2 cartes de la même couleur (c'est toujours possible par le principe des tiroirs).
  Ex : $10\heartsuit$ et $3\heartsuit$.
- L'assistant détermine le rang de ces deux cartes sur le cycle ci-dessous. Une des deux cartes est toujours à 6 sauts ou moins de l'autre dans le sens anti-horlogique.
  Ex :10 est à 6 sauts de 3.



- Cette carte est la première carte révélée, l'autre est la carte secrète.

  Ex : Le 10♡ est révélé, le 3♡ est la carte que le magicien doit retrouver.
- L'assistant et le magicien s'accorde sur un ordre entre les cartes et l'assistant code le nombre de saut selon le schéma suivant :

$$\begin{aligned}
(\text{petite carte}, \text{moyenne carte}, \text{grande carte}) &= 1\\
(\text{petite carte}, \text{grande carte}, \text{moyenne carte}) &= 2\\
(\text{moyenne carte}, \text{petite carte}, \text{grande carte}) &= 3\\
(\text{moyenne carte}, \text{grande carte}, \text{petite carte}) &= 4\\
(\text{grande carte}, \text{petite carte}, \text{moyenne carte}) &= 5\\
(\text{grande carte}, \text{moyenne carte}, \text{petite carte}) &= 6
\end{aligned}$$

Ex : Soit l'ordre $1\clubsuit < \ldots < R\clubsuit < 1\diamondsuit < \ldots < 1\heartsuit < \ldots < 1\spadesuit \ldots$, l'assistant révèle la séquence suivante :

$$10\heartsuit \quad D\spadesuit \quad V\diamondsuit \quad 9\diamondsuit$$

Avec 4 cartes ?

Le tour est-il possible avec 4 cartes ? Non.

- On aurait dans ce cas $|X| = C_{52}^4 = 270725$ (par la règle du sous-ensemble) et $|Y| = 52 \cdot 51 \cdot 50 = 132600$ (par le produit cartésien généralisé). Par conséquent, $|X| > 2|Y|$.
- Par le principe des tiroirs généralisés, toute correspondance $f : X \to Y$ enverra au moins 3 éléments distincts de X vers le même élément de Y.
- Il n'est donc pas possible de coder de manière non ambigüe une carte cachée avec 3 cartes.

Un problème de dénombrement plus complexe

De combien de manière peut-on remplir un panier avec n fruits avec les contraintes suivantes ?

- Le nombre de pommes doit être pair
- Le nombre de bananes doit être un multiple de 5
- Le panier ne peut pas contenir plus que 4 oranges
- Le panier ne peut pas contenir plus qu'une poire

Chapitre 8

Fonctions génératrices

Introduction

Les fonctions génératrices forment un lien entre l'analyse mathématique des fonctions à valeurs réelles, et les problèmes portant sur les *séquences*.

Motivation : Utiliser les fonctions génératrices pour résoudre des récurrences linéaire et des problèmes de dénombrement d'ensembles.

Notation : Dans ce chapitre, on dénotera les *séquences* en utilisant les symboles $\langle \ldots \rangle$.

Définition

Définition : La *fonction génératrice ordinaire* correspondant à la séquence infinie $\langle g_0, g_1, g_2, g_3, \ldots \rangle$ est la *série formelle*

$$G(x) = g_0 + g_1 x + g_2 x^2 + g_3 x^3 + \cdots = \sum_{n=0}^{\infty} g_n x^n.$$

Notation :

$$\langle g_0, g_1, g_2, g_3, \ldots \rangle \longleftrightarrow g_0 + g_1 x + g_2 x^2 + g_3 x^3 + \cdots$$

Remarque : Les fonctions génératrices ne seront que très rarement évaluées. Dans ce chapitre, les questions de convergence n'ont donc en général pas d'importance.

Exemples :

- $\langle 0, 0, 0, 0, \ldots \rangle \longleftrightarrow 0 + 0x + 0x^2 + 0x^3 + \cdots = 0$
- $\langle 1, 0, 0, 0, \ldots \rangle \longleftrightarrow 1 + 0x + 0x^2 + 0x^3 + \cdots = 1$
- $\langle 3, 2, 1, 0, \ldots \rangle \longleftrightarrow 3 + 2x + 1x^2 + 0x^3 + \cdots = 3 + 2x + x^2$

Rappel : $1 + z + z^2 + z^3 + \cdots = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}$.

On a donc :

- $\langle 1, 1, 1, 1, \ldots \rangle \longleftrightarrow \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$
- $\langle 1, -1, 1, -1, \ldots \rangle \longleftrightarrow \left(\sum_{n=0}^{\infty} x^{2n}\right) - \left(\sum_{n=0}^{\infty} x^{2n+1}\right) = \left(\sum_{n=0}^{\infty} x^{2n}\right) - x\left(\sum_{n=0}^{\infty} x^{2n}\right) = \frac{1-x}{1-x^2} = \frac{1}{1+x}$
- $\langle 1, a, a^2, a^3, \ldots \rangle \longleftrightarrow \sum_{n=0}^{\infty} (ax)^n = \frac{1}{1-ax}$
- $\langle 1, 0, 1, 0, 1, 0, \ldots \rangle \longleftrightarrow \sum_{n=0}^{\infty} x^{2n} = \frac{1}{1-x^2}$

Multiplication par une constante

Propriété : Si $\langle f_0, f_1, f_2, \ldots \rangle \longleftrightarrow F(x)$, alors

$$\langle cf_0, cf_1, cf_2, \ldots \rangle \longleftrightarrow c \cdot F(x).$$

Démonstration :

$$\begin{aligned} \langle cf_0, cf_1, cf_2, \ldots \rangle &\longleftrightarrow \sum_{n=0}^{\infty} cf_n x^n \\ &= c \sum_{n=0}^{\infty} f_n x^n = c \cdot F(x) \end{aligned}$$

□

Addition

Propriété : Si

$$\langle f_0, f_1, f_2, \ldots \rangle \longleftrightarrow F(x) \quad \text{et} \quad \langle g_0, g_1, g_2, \ldots \rangle \longleftrightarrow G(x),$$

alors $\langle f_0 + g_0, f_1 + g_1, f_2 + g_2, \ldots \rangle \longleftrightarrow F(x) + G(x)$.

Démonstration :

$$\begin{aligned} \langle f_0 + g_0, f_1 + g_1, f_2 + g_2, \ldots \rangle \quad &\longleftrightarrow \quad \sum_{n=0}^{\infty} (f_n + g_n) x^n \\ &= \quad \left(\sum_{n=0}^{\infty} f_n x^n \right) + \left(\sum_{n=0}^{\infty} g_n x^n \right) \\ &= \quad F(x) + G(x) \end{aligned}$$

□

Exemples

- Multiplication par une constante :

$$\langle 1,0,1,0,1,0,\ldots\rangle \longleftrightarrow 1+x^2+x^4+x^6+\ldots = \frac{1}{1-x^2}$$

En multipliant la fonction génératrice par 2 :

$$\langle 2,0,2,0,2,0,\ldots\rangle \longleftrightarrow 2+2x^2+2x^4+2x^6+\ldots = \frac{2}{1-x^2}$$

- Addition :

$$\begin{array}{rccccccccc}
 & \langle & 1, & 1, & 1, & 1, & 1, & 1, & \ldots & \rangle & \longleftrightarrow & \frac{1}{1-x} \\
+ & \langle & 1, & -1, & 1, & -1, & 1, & -1, & \ldots & \rangle & \longleftrightarrow & \frac{1}{1+x} \\
\hline
 & \langle & 2, & 0, & 2, & 0, & 2, & 0, & \ldots & \rangle & \longleftrightarrow & \frac{1}{1-x}+\frac{1}{1+x} \\
 & & & & & & & & & & & = \frac{2}{1-x^2}
\end{array}$$

Décalage vers la droite

Propriété : Si $\langle f_0, f_1, f_2, \ldots \rangle \longleftrightarrow F(x)$, alors

$$\langle \underbrace{0, 0, \ldots, 0}_{k \text{ zéros}}, f_0, f_1, f_2, \ldots \rangle \longleftrightarrow x^k \cdot F(x).$$

Démonstration :

$$\langle \overbrace{0, 0, \ldots, 0}^{k \text{ zéros}}, f_0, f_1, f_2, \ldots \rangle \quad \longleftrightarrow \quad \sum_{n=0}^{\infty} f_n x^{n+k}$$

$$= \quad x^k \sum_{n=0}^{\infty} f_n x^n \quad = \quad x^k F(x)$$

□

Dérivation

Propriété : Si $\langle f_0, f_1, f_2, \ldots \rangle \longleftrightarrow F(x)$, alors

$$\langle f_1, 2f_2, 3f_3, \ldots \rangle \longleftrightarrow F'(x).$$

Démonstration :

$$\begin{aligned} \langle f_1, 2f_2, 3f_3, \ldots \rangle &\longleftrightarrow \sum_{n=1}^{\infty} n f_n x^{n-1} \\ &= \frac{d}{dx} \sum_{n=0}^{\infty} f_n x^n \\ &= \frac{d}{dx} F(x) \end{aligned}$$

□

(Dérivation = multiplication par l'index et décalage vers la gauche)

Application

Exercice : Trouver une fonction génératrice pour la séquence $\langle 0, 1, 4, 9, 16, \ldots \rangle$.

Réponse : Soit $F(x) = \dfrac{1}{1-x}$. On a successivement

- $\langle 1, 1, 1, 1, \ldots \rangle \longleftrightarrow F(x)$
- $\langle 1, 2, 3, 4, \ldots \rangle \longleftrightarrow F'(x)$
- $\langle 0, 1, 2, 3, \ldots \rangle \longleftrightarrow x \cdot F'(x)$
- $\langle 1, 4, 9, 16, \ldots \rangle \longleftrightarrow (x \cdot F'(x))'$
- $\langle 0, 1, 4, 9, 16, \ldots \rangle \longleftrightarrow x \cdot (x \cdot F'(x))'$.

En développant, on obtient $\langle 0, 1, 4, 9, 16, \ldots \rangle \longleftrightarrow \dfrac{x \cdot (1+x)}{(1-x)^3}$.

Produit

Propriété :

Si $\langle a_0, a_1, a_2, \ldots \rangle \longleftrightarrow A(x)$ et $\langle b_0, b_1, b_2, \ldots \rangle \longleftrightarrow B(x)$, alors

$$\langle c_0, c_1, c_2, \ldots \rangle \longleftrightarrow A(x) \cdot B(x),$$

où

$$c_n = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_n b_0.$$

Démonstration : Soient $A(x) = \sum_{n=0}^{\infty} a_n x^n$ et $B(x) = \sum_{n=0}^{\infty} b_n x^n$,

on a

$$C(x) = A(x) \cdot B(x) = \sum_{n=0}^{\infty} c_n x^n.$$

Coefficients c_n :

	b_0x^0	b_1x^1	b_2x^2	b_3x^3	$\cdots$
a_0x^0	$a_0b_0x^0$	$a_0b_1x^1$	$a_0b_2x^2$	$a_0b_3x^3$	$\cdots$
a_1x^1	$a_1b_0x^1$	$a_1b_1x^2$	$a_1b_2x^3$	$\cdots$	
a_2x^2	$a_2b_0x^2$	$a_2b_1x^3$	$\cdots$		
a_3x^3	$a_3b_0x^3$	$\cdots$			
$\vdots$	$\cdots$				

($\langle c_0, c_1, c_2, \ldots \rangle$ est appelée la *convolution* des séquences $\langle a_0, a_1, a_2, \ldots \rangle$ et $\langle b_0, b_1, b_2, \ldots \rangle$)

Sommation

Propriété : Si $\langle a_0, a_1, a_2, \ldots \rangle \longleftrightarrow A(x)$, alors

$$\langle s_0, s_1, s_2, \ldots \rangle \longleftrightarrow \frac{A(x)}{1-x} \text{ où } s_n = \sum_{i=0}^{n} a_i \text{ pour } n \geq 0.$$

Démonstration : On a :

$$\langle 1, 1, 1, \ldots \rangle \longleftrightarrow \frac{1}{1-x}.$$

Par la règle du produit, le $n$ième terme de $A(x)/(1-x)$ est donné par :

$$a_0 \cdot 1 + a_1 \cdot 1 + a_2 \cdot 1 + \ldots + a_n \cdot 1 = \sum_{i=0}^{n} a_i.$$

Exemple : somme des carrés

Supposons qu'on veuille calculer $s_n = \sum_{i=0}^{n} i^2$ (voir chapitre 5).

On sait que (slide 354) :

$$\langle 0, 1, 4, 9, 16, \ldots \rangle \longleftrightarrow \frac{x \cdot (1+x)}{(1-x)^3}$$

Par la propriété précédente :

$$\langle s_0, s_1, s_2, s_3, \ldots \rangle \longleftrightarrow \frac{x \cdot (1+x)}{(1-x)^4}$$

s_n est donc le coefficient de x^n dans $\frac{x \cdot (1+x)}{(1-x)^4}$.

Extraction des coefficients

Propriété (séries de Taylor) : Si $F(x)$ est la fonction génératrice pour la séquence

$$\langle f_0, f_1, f_2, \ldots \rangle,$$

alors

$$f_0 = F(0), \quad f_n = \frac{F^{(n)}(0)}{n!} \text{ pour } n \geq 1$$

Démonstration :
Directe en dérivant $F(x) = f_0 + f_1 x + f_2 x^2 + \ldots$. □

Exemple :

$$F(x) = \frac{1}{1-x} \quad \Rightarrow \quad \frac{F^{(n)}(x)}{n!} = \frac{n!}{n!(1-x)^{n+1}}$$

$$\Rightarrow \quad \frac{F^{(n)}(0)}{n!} = \frac{n!}{n!(1-0)^{n+1}} = 1$$

Exemple : somme des carrés

- Calculons le $n$ième terme de

$$F(x) = \frac{x(1+x)}{(1-x)^4} = \frac{x}{(1-x)^4} + \frac{x^2}{(1-x)^4}.$$

- Par les propriétés d'addition et de décalage vers la droite, le coefficient de x^n dans $F(x)$ est donc le coefficient de x^{n-1} dans $\frac{1}{(1-x)^4}$ et le coefficient de x^{n-2} dans $\frac{1}{(1-x)^4}$.
- Soit $G(x) = 1/(1-x)^4$,

$$G^{(n)}(x) = \frac{(n+3)!}{6(1-x)^{n+4}} \Rightarrow \frac{G^{(n)}(0)}{n!} = \frac{(n+3)(n+2)(n+1)}{6}$$

- Finalement :

$$\sum_{i=0}^{n} i^2 = \frac{(n+2)(n+1)n}{6} + \frac{(n+1)n(n-1)}{6} = \frac{(2n+1)(n+1)n}{6}$$

Résolution de récurrence

Principe général :

- Trouver une fonction génératrice pour la récurrence
- Extraire une formulation analytique du $n$ième coefficient

Illustration sur la séquence de Fibonacci :

$$\begin{aligned} f_0 &= 0 \\ f_1 &= 1 \\ f_n &= f_{n-1} + f_{n-2} \quad (\text{pour } n \geq 2) \end{aligned}$$

Première étape : trouver $F(x)$ tel que

$$\langle 0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots \rangle \longleftrightarrow F(x)$$

Par définition de $F(x)$:

$$F(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4.$$

Par définition des nombres de Fibonacci :

$$\langle f_0, f_1, f_2, f_3, f_4, \ldots \rangle = \langle 0, 1, f_1 + f_0, f_2 + f_1, f_3 + f_2, \ldots \rangle$$

Trouvons une fonction génératrice pour le membre de droite (par la règle d'addition) :

$$\begin{array}{cccccccc}
 & \langle\ 0, & 1, & 0, & 0, & 0, & \ldots\rangle & \longleftrightarrow\ x \\
 & \langle\ 0, & f_0, & f_1, & f_2, & f_3, & \ldots\rangle & \longleftrightarrow\ xF(x) \\
+ & \langle\ 0, & 0, & f_0, & f_1, & f_2, & \ldots\rangle & \longleftrightarrow\ x^2F(x) \\
\hline
 & \langle\ 0, & \underbrace{1 + f_0}_{1}, & f_1 + f_0, & f_2 + f_1, & f_3 + f_2, & \ldots\rangle & \longleftrightarrow\ x + xF(x) + x^2F(x)
\end{array}$$

On a donc :

$$F(x) = x + xF(x) + x^2F(x),$$

qui donne :

$$F(x) = \frac{x}{1 - x - x^2}$$

Deuxième étape : trouver une formulation analytique pour le coefficient de x^n dans la série de puissance de $\frac{x}{1-x-x^2}$.

Extraction des coefficients

Calculons la décomposition en fractions partielles de $F(x)$:

- Factorisons le dénominateur :

$$(1 - x - x^2) = (1 - \alpha_1 x)(1 - \alpha_2 x),$$

où $\alpha_1 = (1 + \sqrt{5})/2$ et $\alpha_2 = (1 - \sqrt{5})/2$.

- Trouvons A_1 et A_2 tels que :

$$\frac{x}{1 - x - x^2} = \frac{A_1}{1 - \alpha_1 x} + \frac{A_2}{1 - \alpha_2 x}.$$

En prenant quelques valeurs de x, on obtient :

$$A_1 = \frac{1}{\alpha_1 - \alpha_2} = \frac{1}{\sqrt{5}}, \quad A_2 = \frac{-1}{\alpha_1 - \alpha_2} = -\frac{1}{\sqrt{5}}.$$

En substituant :

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

Puisque

$$\frac{1}{1-\alpha x} = 1 + \alpha x + \alpha^2 x^2 + \ldots,$$

on obtient

$$F(x) = \frac{1}{\sqrt{5}}\left((1 + \alpha_1 x + \alpha_1^2 x^2 + \ldots) - (1 + \alpha_2 x + \alpha_2^2 x^2 + \ldots)\right)$$

Par identification :

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

Dénombrement à l'aide de fonctions génératrices

Rappel (Binôme de Newton) : $(a+b)^k = \sum_{n=0}^{k} C_k^n a^{k-n} b^n$.

Cas particulier : $(1+x)^k = \sum_{n=0}^{k} C_k^n x^n$.

Conclusion : $\langle C_k^0, C_k^1, C_k^2, \ldots, C_k^k, 0, 0, 0, \ldots \rangle \longleftrightarrow (1+x)^k$.

Autrement dit, le coefficient de x^n dans le développement de $(1+x)^k$ est le nombre de façons de choisir n élements distincts dans un ensemble de k éléments.

Exemples :

- Le coefficient de x^2 est C_k^2.
- Le coefficient de x^{k+1} est 0.

Convolution

Principe de convolution (version intuitive) : *La fonction génératrice pour le choix d'éléments dans une union d'ensembles disjoints est le produit des fonctions génératrices pour le choix dans chacun de ces ensembles.*

Exemple 1 :

- La fonction génératrice pour le choix d'éléments (sans répétition) dans le singleton $\{a_1\}$ est $1 + x$.
- Il en est de même pour $\{a_2\}$.
- Par le principe de convolution, la fonction génératrice pour le choix d'éléments (sans répétition) dans $\{a_1, a_2\}$ est

$$(1 + x) \cdot (1 + x) = (1 + x)^2 = 1 + 2x + x^2.$$

Exemple 2 : La fonction génératrice pour le choix d'éléments (sans répétition) dans l'ensemble $\{a_1, a_2, \ldots, a_k\}$ est

$$\underbrace{(1+x)\cdot(1+x)\cdots(1+x)}_{k \text{ fois}} = (1+x)^k,$$

ce qui confirme le résultat du transparent 318.

Propriété (Convolution) : Soient

- $A(x)$ la fonction génératrice pour le choix d'éléments dans un ensemble $\mathcal{A}$, et
- $B(x)$ la fonction génératrice pour le choix d'éléments dans un ensemble $\mathcal{B}$.

Si $\mathcal{A}$ et $\mathcal{B}$ sont disjoints, alors la fonction génératrice pour le choix d'éléments dans l'union $\mathcal{A} \cup \mathcal{B}$ est $A(x) \cdot B(x)$.

Remarque : Ce qu'on appelle "*choix*" dans le théorème n'est pas bien précisé. La propriété de convolution reste valide pour *beaucoup* d'interprétations de ce choix.

Exemples :

- on peut ou non autoriser les répétitions,
- on peut autoriser les répétitions arbitraires, ou les limiter,
- etc.

Seules restrictions :

- l'ordre dans lequel les éléments sont sélectionnés ne doit pas avoir d'importance ;
- les restrictions sur le choix d'éléments dans les ensembles $\mathcal{A}$ et $\mathcal{B}$ doivent être d'application pour le choix d'éléments dans l'ensemble $\mathcal{A} \cup \mathcal{B}$.

Démonstration de la propriété de convolution :

- Soient $A(x) = \sum_{n=0}^{\infty} a_n x^n$, $B(x) = \sum_{n=0}^{\infty} b_n x^n$ et
  $C(x) = A(x) \cdot B(x) = \sum_{n=0}^{\infty} c_n x^n$.
- Par la règle du produit, on a
  $c_n = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_n b_0$.
- Choisir n éléments de $\mathcal{A} \cup \mathcal{B}$ revient à choisir j élements de $\mathcal{A}$ (a_j manières de les choisir) et $n - j$ éléments de $\mathcal{B}$ (b_{n-j} manières de les choisir). Comme $j \in \{0, 1, \ldots, n\}$, on obtient

$$a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_n b_0.$$

Choix avec répétition

Question : De combien de façons peut-on choisir n éléments (avec répétition) lorsque l'on a k sortes d'éléments disponibles ?

Réponse :

- S'il n'y a qu'une seule sorte d'éléments :
  - une seule façon de choisir 0 élément,
  - une seule façon de choisir 1 élément,
  - une seule façon de choisir 2 elements,
  - etc.

La fonction génératrice est donc

$$\langle 1, 1, 1, 1, \ldots \rangle \longleftrightarrow 1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}.$$

- Si on a k sortes d'éléments, on obtient, par la propriété de convolution, la fonction génératrice suivante :

$$\underbrace{\frac{1}{1-x} \cdot \frac{1}{1-x} \cdots \frac{1}{1-x}}_{k \text{ fois}} = \frac{1}{(1-x)^k}$$

- Le nombre cherché est donc le coefficient de x^n dans le développement en série de $\dfrac{1}{(1-x)^k}$.

- Soit $g(x) = \dfrac{1}{(1-x)^k} = (1-x)^{-k}$.
- On obtient
  - $g'(x) = k(1-x)^{-k-1}$
  - $g''(x) = k(k+1)(1-x)^{-k-2}$
  - $g'''(x) = k(k+1)(k+2)(1-x)^{-k-3}$
  - $\ldots$
  - $g^{(n)}(x) = k(k+1)\cdots(k+n-1)(1-x)^{-k-n}$
- Le coefficient cherché est donc

$$\begin{aligned} \frac{g^{(n)}(0)}{n!} &= \frac{k(k+1)\cdots(k+n-1)}{n!} \\ &= \frac{(k+n-1)!}{(k-1)!n!} \\ &= C_{k+n-1}^{n}. \end{aligned}$$

Un problème de dénombrement “impossible”

Problème : De combien de manières peut-on composer un panier avec n fruits (pommes, bananes, oranges et fraises) en respectant les contraintes suivantes ?

- Le nombre de pommes doit être pair ;
- Le nombre de bananes doit être un multiple de 5 ;
- Il y a au plus 4 oranges ;
- Il y a au plus 1 fraise.

Exemple : Il existe 7 façons de composer un panier de 6 fruits :

Pommes	6	4	4	2	2	0	0
Bananes	0	0	0	0	0	5	5
Oranges	0	2	1	4	3	1	0
Fraises	0	0	1	0	1	0	1

Réponse :

- Fonction génératrice pour le choix des pommes :

$$P(x) = 1 + x^2 + x^4 + x^6 + \cdots = \sum_{n=0}^{\infty} x^{2n} = \frac{1}{1-x^2}.$$

- Fonction génératrice pour le choix des bananes :

$$B(x) = 1 + x^5 + x^{10} + x^{15} + \cdots = \sum_{n=0}^{\infty} x^{5n} = \frac{1}{1-x^5}.$$

- Fonction génératice pour le choix des oranges :

$$O(x) = 1 + x + x^2 + x^3 + x^4 = \frac{1-x^5}{1-x}.$$

- Fonction génératrice pour le choix des fraises :

$$F(x) = 1 + x.$$

- Par la propriété de convolution, la fonction génératrice pour la composition d'un panier de fruits est

$$\begin{aligned} & P(x)B(x)O(x)F(x) \\ = & \frac{1}{(1-x^2)} \frac{1}{(1-x^5)} \frac{(1-x^5)}{1-x}(1+x) \\ = & \frac{1}{(1-x)^2} \\ = & 1 + 2x + 3x^2 + 4x^3 + \cdots \end{aligned}$$

- Le coefficient de x^n est toujours $n+1$.
- Il y a donc $n+1$ façons de composer un panier de n fruits.