

Chapitre 1

Introduction, notions préliminaires

Quelles sont les limites ultimes de l'informatique ?

Si on dispose de ressources suffisantes, peut-on résoudre n'importe quel problème ?

Par exemple, un vérificateur de programmes qui déterminerait si un programme contient un bogue ?

Un compilateur optimisant ?

Déterminer si un polynôme à plusieurs variables possède des solutions entières ?

Déterminer si le plan peut être pavé avec un ensemble donné de tuiles ?

Qu'est-ce que *calculer* ?

Certaines machines sont-elles intrinsèquement plus puissantes que d'autres ?

Est-ce que tous les langages de programmation se valent ?

L'ordinateur quantique est-il vraiment plus puissant que l'ordinateur classique ?

Existe-t-il une hiérarchie parmi les modèles calculatoires ?

Un *puzzle* est un problème difficile à résoudre, mais dont la solution est facile à vérifier. Les puzzles existent-ils ?

Est-ce que tous les problèmes dont la solution est facile à vérifier sont des problèmes faciles à résoudre ?

Il existe un *super-puzzle* ! Le résoudre vous donnera la gloire et 1M \$ US, de même qu'une solution à tous les puzzles !

Deux personnes se connaissant à peine et qui discutent sur un réseau téléphonique non sécurisé peuvent-elles en arriver à échanger des informations privées sans craindre qu'un espion n'obtienne aussi ces informations ?

- par contradiction
- par récurrence
- par récurrence généralisée
- par récurrence structurelle
- par inclusion mutuelle
- principe du pigeonnier

Preuve par contradiction

On prouve un énoncé en démontrant que sa négation mène à une contradiction.

Exemple de preuve par contradiction

Exemple 1.1

$\sqrt{2}$ est irrationnel.

Démonstration :

Supposons au contraire que $\exists a, b \in \mathbb{N}$ tels que $\sqrt{2} = \frac{a}{b}$ où $\text{pgcd}(a, b) = 1$.

$$\sqrt{2} = \frac{a}{b} \quad \Rightarrow \quad 2 = \frac{a^2}{b^2} \quad \Rightarrow \quad 2b^2 = a^2,$$

donc $a = 2k$, car a^2 est pair implique que a est pair.

D'où :

$$2b^2 = (2k)^2 \quad \Rightarrow \quad 2b^2 = 4k^2 \quad \Rightarrow \quad b^2 = 2k^2,$$

et donc $b = 2l$, car b^2 est pair implique que b est pair.

On a alors que 2 divise a et b ...

Contradiction ! car le pgcd de a et b n'est pas 1.

On conclut que $\sqrt{2} \neq \frac{a}{b}$, quels que soient $a, b \in \mathbb{N}$. □

Soit P un prédicat sur les entiers naturels, c'est-à-dire P est une fonction $\mathbb{N} \rightarrow \{\langle \text{VRAI} \rangle, \langle \text{FAUX} \rangle\}$.

Si

- $P(n_0)$ est vrai, et
- pour tout $n > n_0$, $P(n-1)$ implique que $P(n)$ est vrai, alors
- $P(i)$ est vrai pour tout $i \geq n_0$.

Exemple de preuve par récurrence

Exemple 1.2

Pour tout $n \geq 1$,

$$\sum_{i=1}^n i^3 = \left(\frac{n(n+1)}{2} \right)^2.$$

Démonstration :

Considérons le prédicat $P(n)$ suivant :

$$\sum_{i=1}^n i^3 = \left(\frac{n(n+1)}{2} \right)^2.$$

Nous devons prouver que $P(n)$ est vrai pour tous les entiers $n \geq 1$.

Base de la récurrence ($n = 1$)

D'une part, on voit que :

$$\begin{aligned}\sum_{i=1}^n i^3 &= \sum_{i=1}^1 i^3 \\ &= 1.\end{aligned}$$

D'autre part, on a que :

$$\begin{aligned}\left(\frac{n(n+1)}{2}\right)^2 &= \left(\frac{1(1+1)}{2}\right)^2 \\ &= \left(\frac{2}{2}\right)^2 \\ &= 1.\end{aligned}$$

donc $P(1)$ est vrai.

Pas de récurrence Soit $n > 1$. À démontrer : $P(n-1) \Rightarrow P(n)$.

Supposons que $P(n-1)$ est vrai, c'est-à-dire :

$$\sum_{i=1}^{n-1} i^3 = \left(\frac{n(n-1)}{2} \right)^2 \quad (\text{hypothèse de récurrence})$$

On a d'une part :

$$\begin{aligned}\sum_{i=1}^n i^3 &= \sum_{i=1}^{n-1} i^3 + n^3 \\&= \left(\frac{n(n-1)}{2} \right)^2 + n^3 \quad (\text{par l'hypothèse de récurrence}) \\&= \frac{1}{4} n^2 (n^2 - 2n + 1) + n^3 \\&= \frac{1}{4} n^2 (n^2 + 2n + 1),\end{aligned}$$

et d'autre part :

$$\begin{aligned}\left(\frac{n(n+1)}{2} \right)^2 &= \frac{1}{4} n^2 (n+1)^2 \\&= \frac{1}{4} n^2 (n^2 + 2n + 1),\end{aligned}$$

donc $P(n-1) \Rightarrow P(n)$, et la proposition est démontrée par récurrence.



Preuve par récurrence généralisée

Si

- $P(n_0), P(n_0 + 1), \dots, P(n_0 + k)$ sont vrais, et
- Pour tout $n > n_0 + k$:

$[P(n_0) \text{ et } P(n_0 + 1) \text{ et } \dots \text{ et } P(n - 1)]$ implique $P(n)$

alors

- $P(i)$ est vrai pour tout $i \geq n_0$.

Soit \mathcal{S} une structure définie de façon récursive, c'est-à-dire :

- Il existe un ensemble de base $\mathcal{S}_0 \subseteq \mathcal{S}$,
- Il existe des *règles de construction* R_1, \dots, R_k qui permettent de construire des éléments de \mathcal{S} à partir d'éléments existants :
pour x_1, \dots, x_m , $R_i(x_1, \dots, x_m) \in \mathcal{S}$.

Un parenthésage valide est une structure récursive :

Définition 1.3 (Parenthésage)

Un **parenthésage** est une chaîne ne contenant que les caractères "(" et ")" telle que :

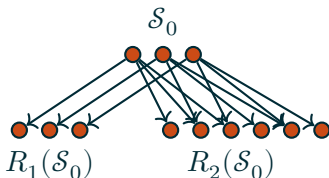
- $\mathcal{S}_0 = \{""\}$
- R_1 : Si p est un parenthésage, alors " (p) " est un parenthésage. Donc : $R_1(p) = "(p)"$.
- R_2 : Si p_1 et p_2 sont des parenthésages, alors la concaténation de p_1 et p_2 est un parenthésage. Donc, $R_2(p_1, p_2) = "p_1p_2"$.

$() \rightarrow (()) \rightarrow (())() \rightarrow ((())) \rightarrow \text{etc...}$

Principe de la récurrence structurelle

Soit P un prédicat sur la structure \mathcal{S} . Pour prouver $P(x)$ pour tout $x \in \mathcal{S}$, il suffit de prouver :

- $P(x)$ pour tout $x \in \mathcal{S}_0$,
- Si $P(x)$ est vrai pour tout $x \in \mathcal{E} \subseteq \mathcal{S}$, alors $P(x)$ est vrai pour tout $x \in R_1(\mathcal{E}) \cup R_2(\mathcal{E}) \cup \dots \cup R_k(\mathcal{E})$.



Exemple 1.4

Tout préfixe, c'est-à-dire une sous-chaîne initiale, d'un parenthésage contient autant ou plus de parenthèses ouvrantes que de parenthèses fermantes.

Démonstration :

Soit $d[s]$ la différence entre le nombre de parenthèses ouvrantes et fermantes d'une chaîne s . Il faut prouver que $d[s] \geq 0$ pour tout préfixe s d'un parenthésage p .

Vérification pour l'ensemble $\mathcal{S}_0 = \{""\}$.

La proposition est trivialement vraie pour la chaîne vide.

Vérification de la règle R_1 .

Supposons que la proposition est vraie pour le parenthésage p .

Alors tout préfixe de (p) est de la forme $(s$, où s est un préfixe de p , ou de la forme (p) . Or :

$$d[(s) = 1 + d[s] \geq 0 \quad \text{et} \quad d[(p)] = d[p] \geq 0.$$

Vérification de la règle R_2 .

Si la proposition est vraie pour p_1 et pour p_2 , alors tout préfixe de la concaténation de p_1 et p_2 est de la forme s_1 , où s_1 est un préfixe de p_1 , ou de la forme $p_1 s_2$, où s_2 est un préfixe de p_2 . Or :

$$d[s_1] \geq 0 \quad \text{et} \quad d[p_1 s_2] = d[p_1] + d[s_2] \geq 0.$$



Notons au passage que les nombres naturels \mathbb{N} forment une structure réursive :

- $\mathcal{S}_0 = \{0\} \subseteq \mathbb{N}$
- $R_1(n) = \text{succ}(n) \in \mathbb{N}$. (Interprétation : $\text{succ}(n) = n + 1$)

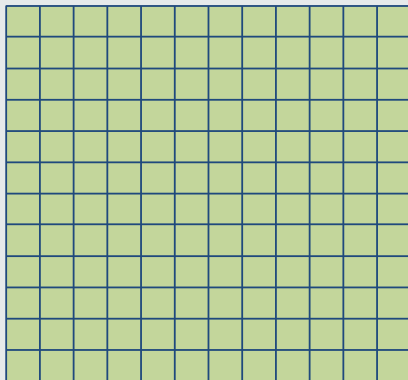
Réurrence structurelle sur $\mathbb{N} \rightarrow$ récurrence « simple ».

Proposition 1.5

Si on place $n + 1$ objets dans n contenants, alors il y aura au moins un contenant avec plus d'un objet.

Problème 1.6

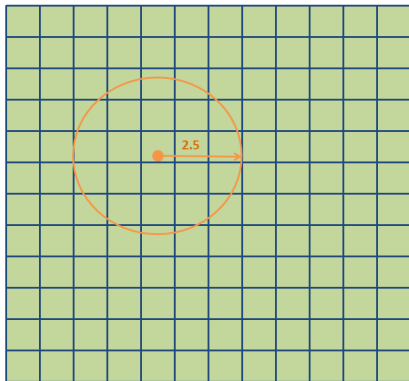
Peut-on placer 13 joueurs sur un terrain $12\text{m} \times 12\text{m}$ afin qu'aucun joueur ne soit situé à 5m ou moins d'un autre ?



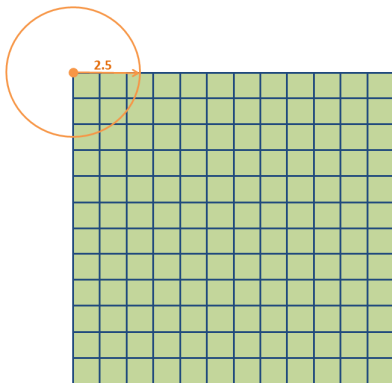
La surface totale : $12 \times 12 = 144$.

La surface interdite par les joueurs :

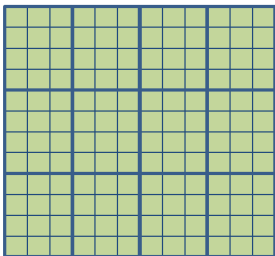
$$13 \times \pi 2.5^2 = 255.26 > 144.$$



Oui mais...



$$(12 + 2.5 + 2.5)(12 + 2.5 + 2.5) = 289 > 255.26.$$



On divise le carré en rectangles de $3\text{m} \times 4\text{m}$. Il y en a 12. Par le principe du pigeonnier, il y aura au moins un rectangle contenant au moins deux joueurs. L'hypoténuse d'un rectangle est de :

$$\sqrt{3^2 + 4^2} = 5 \text{ mètres.}$$

Il y aura forcément deux joueurs séparés de 5m ou moins ! C'est donc impossible...

Preuve par inclusion mutuelle

On prouve que deux ensembles \mathcal{A} et \mathcal{B} sont égaux en vérifiant que :

- $\mathcal{A} \subseteq \mathcal{B}$,
- et $\mathcal{B} \subseteq \mathcal{A}$.

Exemple de preuve par inclusion mutuelle

Théorème 1.7

Soient

$$\mathcal{A} = \left\{ \frac{a}{b} \mid a \in \mathbb{N} \text{ et } b \in \mathbb{N}^* \right\}$$

$$\mathcal{B} = \{x \in \mathbb{R}_+ \mid x \text{ possède un développement} \\ \text{décimal périodique}\},$$

alors $\mathcal{A} = \mathcal{B}$.

Démonstration :

À montrer : $\mathcal{A} \subseteq \mathcal{B}$ et $\mathcal{B} \subseteq \mathcal{A}$.

Soit $\frac{a}{b} \in \mathcal{A}$. Soient r_1, r_2, \dots la suite infinie des restes obtenus par l'algorithme classique de division de l'entier a par l'entier b , comme dans l'exemple de la page suivante.

$$\begin{array}{r}
 3 \overline{) 7} \\
 \underline{0} 0, \textcolor{red}{4} 2 8 5 7 1 \textcolor{red}{4} 2 \dots \\
 r_1 = 3 \quad \textcolor{red}{30} \\
 \underline{28} \\
 r_2 = 2 \quad 20 \\
 \underline{14} \\
 r_3 = 6 \quad 60 \\
 \underline{56} \\
 r_4 = 4 \quad 40 \\
 \underline{35} \\
 r_5 = 5 \quad 50 \\
 \underline{49} \\
 r_6 = 1 \quad 10 \\
 \underline{7} \\
 r_7 = 3 \quad \textcolor{red}{30} \\
 \underline{28} \\
 r_8 = 2 \quad 20 \\
 \underline{14} \\
 \vdots \\
 \ddots
 \end{array}$$

Comme $0 \leq r_i < b$ pour tout i , et comme la valeur de r_{i+1} est déterminée uniquement par la valeur de r_i , alors la suite des restes doit être périodique.

Puisque chaque décimale du résultat étant déterminée par le reste correspondant dans la suite des restes, la suite des décimales est également périodique.

Donc $\frac{a}{b} \in \mathcal{B}$, et $\mathcal{A} \subseteq \mathcal{B}$.

Soit $x \in \mathcal{B}$ avec le développement décimal suivant :

$$x = d_i d_{i-1} \dots d_0 . d_{-1} d_{-2} \dots d_{-j} p_k p_{k-1} \dots p_1 p_k p_{k-1} \dots p_1 \dots$$

où

$$d_i, d_{i-1}, \dots, d_{-j} \text{ et } p_k, p_{k-1}, \dots, p_1$$

sont des chiffres décimaux et où

$$p_k p_{k-1} \dots p_1$$

est la partie périodique du développement de x , comme dans l'exemple qui suit.

$$x = 12.345\textcolor{red}{6789}67896789\dots \quad (i = 1, j = 3, k = 4)$$

$$10^3 x = 12345.\textcolor{red}{6789}67896789\dots$$

$$10^7 x = 123456789.\textcolor{red}{6789}67896789\dots$$

$$(10^7 - 10^3)x = 123456789 - 12345$$

$$x = \frac{123456789 - 12345}{10^7 - 10^3}$$

Comme l'illustre l'exemple, en choisissant :

$$a = d_i d_{i-1} \dots d_{-j} p_k p_{k-1} \dots p_1 - d_i d_{i-1} \dots d_{-j}$$

$$b = 10^{j+k} - 10^j$$

on obtient $x = \frac{a}{b}$.

Donc $x \in \mathcal{A}$ et $\mathcal{B} \subseteq \mathcal{A}$.

Définition 1.8

Soient $f, g : \mathbb{N} \rightarrow \mathbb{R}_+$. On dira que

- f est dans l'ordre de g ,
- ou que g est une borne supérieure asymptotique pour f ,
- ou que f est grand O de g ,
- ou que $f \in O(g)$,

s'il existe des constantes $c, n_0 \in \mathbb{N}$ telles que

$$\forall n \geq n_0 : f(n) \leq cg(n).$$

Proposition 1.9

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} < \infty \Rightarrow f \in O(g),$$

$$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = \infty \Rightarrow f \notin O(g).$$

Exemples :

Si $f(n) = 2n^2 + 3n + \log_2 n + 9999$, alors

$$f(n) \in O(n^2), f(n) \in O(n^3).$$

Si $f(n) = n^{9999}$, alors

$$f(n) \in O(2^n).$$

Si $f(n) = \log_2 n$, alors

$$\forall a > 1 : f(n) \in O(\log_a n)$$

On écrit $f(n) \in O(\log n)$, car $\log_a n = \log_2 n / \log_2 a$.

Si $f(n) = 2n^2 \log_3(\log_3 n) + n^2$, alors

$$f(n) \in O(n^2 \log \log n).$$

Il existe aussi d'autres notations du même type :

Définition 1.10 (Petit o)

On dit que f est petit- o de g , dénoté $f \in o(g)$, si pour tout $c > 0$, il existe un $n_0 \in \mathbb{N}$ tel que $\forall n \geq n_0, f(n) \leq cg(n)$.

$f \in o(g)$ si f croît beaucoup moins rapidement que g .

Définition 1.11

On a également les définitions suivantes :

- $f \in \Omega(g)$ ssi $g \in O(f)$
- $f \in \omega(g)$ ssi $g \in o(f)$
- $f \in \Theta(g)$ ssi $f \in O(g)$ et $f \in \Omega(g)$.

On écrit souvent :

$$\begin{array}{lcl} & = & \text{au lieu de } \in, \\ f(n) = O(n^2) & \text{au lieu de} & f(n) \in O(n^2). \end{array}$$