Chapitre 1

Introduction, notions préliminaires

Introduction

Quelles sont les limites ultimes de l'informatique ?

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

Par exemple, un correcteur automatique de TP ?

Un compilateur optimisant ?

Déterminer si un polynôme à plusieurs variables posssède 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 ?

L'informatique théorique peut-elle déterminer si les *MACs* sont plus puissants que les *PCs* ?

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 ?

Révision des techniques de preuves

- par contradiction
- par induction
- par induction généralisée
- par induction 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.

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

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

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

D'où :

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

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

On a alors que 2 divise a et $b \ldots$

Contradiction ! ($\mathrm{PGCD}(a, b) = 1$)

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

Preuve par induction

Soit P un prédicat sur les entiers naturels, c'est-à-dire P est une fonction $\mathbb{N} \to \{\langle \textsc{Vrai} \rangle, \langle \textsc{Faux} \rangle\}$.

Si

- $P(n_0)$ est vrai,
- pour tout $n > n_0$: $P(n-1)$ est vrai implique $P(n)$ est vrai,

alors

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

Exemple de preuve par induction

Exemple 1.2.

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

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 l'induction : $(n = 1)$

$$\begin{aligned}
\sum_{i=1}^{n} i^3 &= \sum_{i=1}^{1} i^3 \\
&= 1 \\
&= \left(\frac{1(1+1)}{2}\right)^2 \\
&= \left(\frac{n(n+1)}{2}\right)^2,
\end{aligned}$$

donc $P(1)$ est vrai.

Pas d'induction : Soit $n > 1$. À montrer : $P(n-1) \Rightarrow P(n)$.

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

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

On a :

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

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

Preuve par induction généralisée

Si

- $P(n_0), P(n_0+1), \ldots, P(n_0+k)$ sont vrais,
- pour tout $n > n_0 + k$:
  $[P(n_0)$ et $P(n_0+1)$ et $\ldots$ et $P(n-1)]$ implique $P(n)$,

alors

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

Preuve par induction structurelle

Soit P un prédicat sur les éléments d'un ensemble $\mathcal{E}$ défini de façon récursive, c'est-à-dire :

- $\mathcal{S}_0 \subseteq \mathcal{E}$,
- $\mathcal{S} \subseteq \mathcal{E}$ implique $R_1(\mathcal{S}), R_2(\mathcal{S}), \ldots, R_k(\mathcal{S}) \subseteq \mathcal{E}$,

où $R_1, R_2, \ldots, R_k$ sont des règles de construction.

Pour prouver $P(x)$ pour tout $x \in \mathcal{E}$, il suffit de prouver :

- $P(x)$ pour tout $x \in \mathcal{S}_0$,
- $P(x)$ pour tout $x \in \mathcal{S} \subseteq \mathcal{E}$ implique
  $P(x)$ pour tout $x \in R_1(\mathcal{S}) \cup R_2(\mathcal{S}) \cup \ldots \cup R_k(\mathcal{S})$.

Exemple de preuve par induction structurelle

Définition 1.3. Un parenthésage non vide est une chaîne ne contenant que les caractères (et) telle que :

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

▲

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.

Remarquons que l'énoncé est trivialement vrai pour le préfixe *vide* d'un parenthésage.

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 $()$.

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 préxixe 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 :

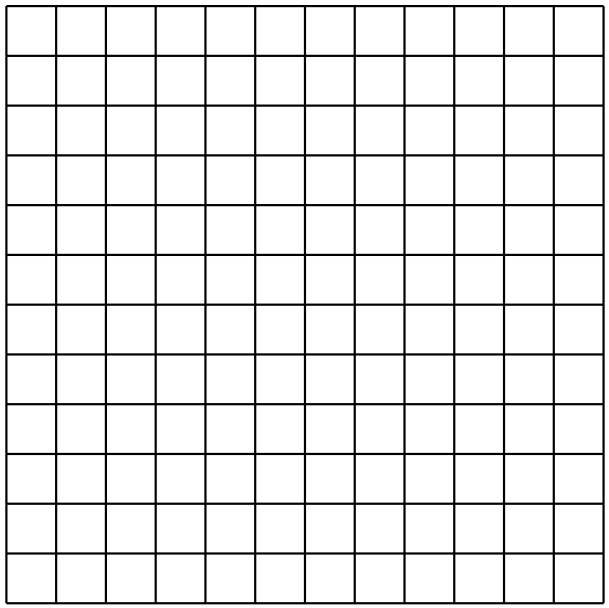
$$d[s_1] \geq 0 \quad \text{et} \quad d[p_1 s_2] = d[p_1] + d[s_2] \geq 0.$$

▲

Principe du pigeonnier

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 12m$\times$12m de façon à ce 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...

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

Il faut trouver autre chose !

On divise le carré en rectangles de 3m×4m. 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 donc 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

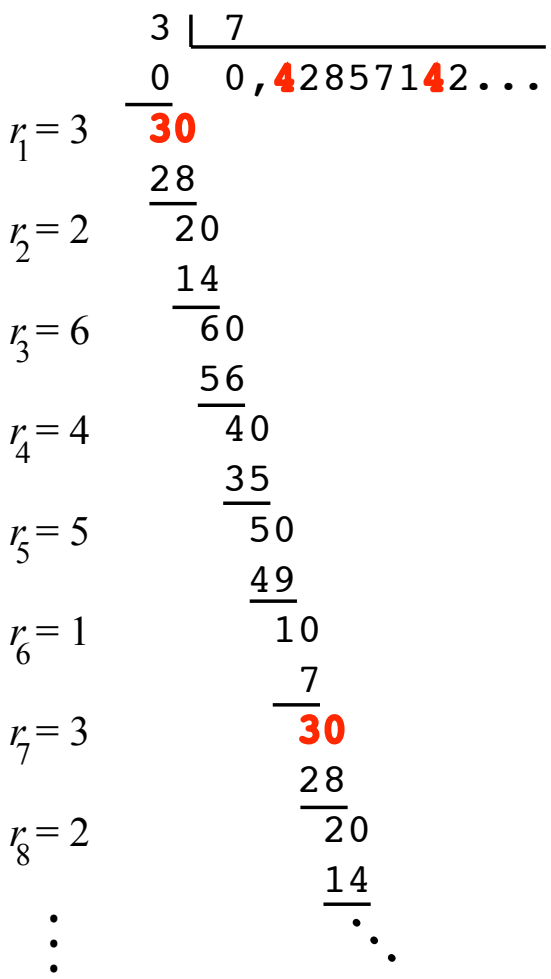
$$\begin{aligned} \mathcal{A} &= \{\frac{a}{b} \mid a \in \mathbb{N} \text{ et } b \in \mathbb{N}^*\} \\ \mathcal{B} &= \{x \in \mathbb{R}_+ \mid x \text{ possède un développement décimal périodique}\}, \end{aligned}$$

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

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

Soit $\frac{a}{b} \in \mathcal{A}$. Soient $r_1, r_2, \ldots$ 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 figure 1.1.

Figure 1.1.


3 | 7
0 0,4285714 2...
30
28
20
14
60
56
40
35
50
49
10
7
30
28
20
14
$r_1 = 3$
$r_2 = 2$
$r_3 = 6$
$r_4 = 4$
$r_5 = 5$
$r_6 = 1$
$r_7 = 3$
$r_8 = 2$

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.

Chaque décimale du résultat étant déterminée par le reste correspondant dans la suite des restes, alors 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.

$$
\begin{aligned}
x &= 12.345\color{red}{6789}67896789\ldots \qquad (i=1,\ j=3,\ k=4)\\
10^3 x &= 12345.\color{red}{6789}67896789\ldots\\
10^7 x &= 123456789.\color{red}{6789}67896789\ldots\\
(10^7-10^3)x &= 123456789-12345\\
x &= \frac{123456789-12345}{10^7-10^3}
\end{aligned}
$$

Comme l'illustre l'exemple, en choisissant :

$$\begin{aligned} a &= d_i d_{i-1} \ldots d_{-j} p_k p_{k-1} \ldots p_1 \; - \; d_i d_{i-1} \ldots d_{-j} \\ \\ b &= 10^{j+k} - 10^j \end{aligned}$$

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

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

Notations asymptotiques

Définition 1.8. Soient $f, g : \mathbb{N} \to \mathbb{R}_+$. 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.

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

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

▲

Définition 1.10. Soient $f, g : \mathbb{N} \to \mathbb{R}_+$. On dira que

- f est petit o de g,
- ou que $f \in o(g)$,

si pour toute constante réelle $c > 0$, il existe $n_0 \in \mathbb{N}$ tel que

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

▲

Proposition 1.11.

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0 \ \Rightarrow f \in o(g),$$

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} > 0 \ \Rightarrow f \notin o(g).$$

▲

Exemples 1.12. Si $f(n) = 2n^2 + 3n + \log_2 n + 9999$, alors

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

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

$$f(n) \in O(2^n),\ f(n) \in o(1.0001^n).$$

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

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

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

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

▲

On écrit souvent :

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