ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Section d'Informatique et de Systèmes de Communication

Corrigé de la série 2 24 Mars 2006

1. Induction

a) Pour $n = 1$ l'affirmation est clairement vraie. Supposons maintenant le résultat prouvé pour n et montrons-le pour $n + 1$.

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n \cdot (1+x) \\ &\geq (1+nx)\cdot(1+x), \quad \text{puisque } x \geq -1 \text{ et par hypothèse d'induction} \\ &= 1 + nx + x + \underbrace{nx^2}_{\geq 0} \\ &\geq 1 + (n+1)x\end{aligned}$$

Ceci prouve le résultat.

b) Il est trivial de vérifier le résultat pour $n = 1$. Montrons-le pour $n + 1$ sous l'hypothèse qu'il est vrai pour n. Nous commençons par l'inégalité à gauche.

Par l'utilisation de l'hypothèse d'induction nous avons

$$\begin{aligned}2(\sqrt{n+2}-1) &= 2(\sqrt{n+2}-\sqrt{n+1}+\sqrt{n+1}-1) \\ &< 2(\sqrt{n+2}-\sqrt{n+1}) + 1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}}.\end{aligned}$$

L'affirmation est donc prouvée si nous montrons que pour tout $n \in \mathbb{N}$, nous avons

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

Comme la fonction $\sqrt{\cdot}$ est concave, nous avons, par le développement limité autour de $n + 1$,

$$\sqrt{n+2} \leq \sqrt{n+1} + \frac{1}{2\sqrt{n+1}}.$$

En insérant ceci dans (1), nous obtenons l'inégalité

$$2\left(\frac{1}{2\sqrt{n+1}}\right) \leq \frac{1}{\sqrt{n+1}},$$

qui est certainement vraie. Donc (1) est aussi vraie, et l'affirmation en suit.

Il reste à prouver la deuxième inégalité. Nous supposons de nouveau le résultat prouvé pour n et considérons le cas pour $n + 1$. Alors

$$1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} + \frac{1}{\sqrt{n+1}} < 2\sqrt{n} + \frac{1}{\sqrt{n+1}}.$$

Pour conclure, il reste donc à voir que

$$2\sqrt{n} + \frac{1}{\sqrt{n+1}} \leq 2\sqrt{n+1}. \tag{2}$$

Nous pourrions de nouveau utiliser la convexité de la racine et un développement limité autour de $n+1$. Alternativement nous pouvons prendre la démarche suivante pour prouver (2): en multipliant par $\sqrt{n+1}$ et soustraction de 1, on obtient l'inégalité équivalente

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

On vérifie que cette identité est vraie en l'élevant au carré et en simplifiant ensuite. Nous omettons ces calcul faciles. Il en suit que l'inégalité (2) est vraie, terminant la preuve.

2. Induction

Il est clair que la propriéte $P(n)$ est fausse pour $n \geq 2$, il doit donc y avoir une erreur dans la preuve.

En effet cette erreur a lieu du passage de $P(1)$ à $P(2)$. A la troisième ligne en partant du bas on choisit $e_2 \in C$ tel que $e_2 \neq f$ et $e_2 \neq e_1$. Puisqu'on a aussi $e_1 \neq f$, on a besoin de 3 elements (élèves) distincts de C, ce qui n'est pas possible si $n+1 = 2$, puisque dans ce cas la classe C ne comporte que 2 élèves.

Bien que tous les autres passages de $P(n)$ à $P(n+1)$ sont justes, puisque $P(2)$ est fausse on ne peut rien en déduire.

3. La notation O

a) On pose $f(n) = n^2 + 100$, $g(n) = n^2$. Si on prend $n_0 = 1$ et $c = 101$, on voit que $c \cdot g(n) - f(n) = 101 \cdot n^2 - n^2 - 100 = 100 \cdot (n^2 - 1) \geq 0$ pour tout $n \geq 1$. On a donc $f(n) \leq c \cdot g(n)$ pour tout $n \geq n_0$. (Bien sûr, il y a beaucoup de valeurs possibles pour n_0 et c.) Ainsi nous avons montré que $f(n) = O(g(n))$.

Maintenant si on pose $n_0' = 1$ et $c' = 1$ on voit que pour tout $n \geq n_0'$ on a $n^2 \leq c' \cdot (n^2 + 100)$, et donc $g(n) = O(f(n))$.

On a donc par définition $f(n) = \Theta(g(n))$.

b) Il existe $n_0, n_0' \in N$ et $c, c' \in \mathbb{R}_{\geq 0}$ tels que:

$$n \geq n_0 \implies f(n) \leq c \cdot g(n)$$

$$n \geq n_0' \implies g(n) \leq c' \cdot h(n)$$

Prenons $n_0'' = \max(n_0, n_0')$ et $c'' = c \cdot c'$. On voit que si $n \geq n_0''$ alors on aura $n \geq n_0$ et $n \geq n_0'$, et donc

$$n \geq n_0'' \implies f(n) \leq c \cdot g(n) \leq c \cdot c' \cdot h(n) = c'' \cdot h(n)$$

et donc par définition $f(n) = O(h(n))$.

c) On rappelle que $f(n) = o(g(n)) \implies f(n) = O(g(n))$.

$\lim_{n\to\infty} \frac{\log_2(n)}{n} = 0$. Donc $\log_2(n) = o(n)$, donc $\log_2(n) = O(n)$ et donc par définition $n = \Omega(\log_2(n))$.

d) Par hypothèse il existe $n_0 \in \mathbb{N}$ et $c \in \mathbb{R}_{\geq 0}$ avec:

$$\begin{aligned} n \geq n_0 &\implies f(n) \leq c \cdot g(n) \\ &\implies a \cdot f(n) \leq a \cdot c \cdot g(n) \\ &\implies a \cdot f(n) \leq \tfrac{b}{b} a \cdot c \cdot g(n) \\ &\implies a \cdot f(n) \leq \tfrac{ac}{b} \cdot b \cdot g(n) \\ &\implies a \cdot f(n) \leq c' \cdot b \cdot g(n) \end{aligned}$$

où $c' = \frac{ac}{b}$. Donc en mettant n_0 et c' dans la définition on voit que $a \cdot f(n) = O(b \cdot g(n))$.

e) On rappelle de nouveau que $f(n) = o(g(n)) \implies f(n) = O(g(n))$. Posons $f(n) = n^d$ et $g(n) = a^n$.

$$\lim_{n\to\infty} \frac{n^d}{a^n} = \lim_{n\to\infty} e^{\ln \frac{n^d}{a^n}} = \lim_{n\to\infty} e^{d\cdot\ln n - n\cdot\ln a} = 0$$

puisque $a > 1$, donc $\ln a > 0$ et donc

$$\lim_{n\to\infty} d \cdot \ln n - n \cdot \ln a = -\infty$$

Ainsi puisque $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$ on a $f(n) = o(g(n))$, et donc $f(n) = O(g(n))$.

f)

	$f(n)$	$g(n)$	$f = O(g)$	$f = \Omega(g)$	$f = \Theta(g)$	$f = o(g)$
(1)	$n^{1/100}$	$\sqrt{n}$	Vrai	Faux	Faux	Vrai
(2)	$\ln(n)$	$\ln^2(n)$	Vrai	Faux	Faux	Vrai
(3)	$\sqrt{n}$	$\ln^2(n)$	Faux	Vrai	Faux	Faux
(4)	2^n	$n!$	Vrai	Faux	Faux	Vrai
(5)	$\log_2(n)$	$\log_3(n)$	Vrai	Vrai	Vrai	Faux
(6)	$\ln(n)$	$\ln\ln(n)$	Faux	Vrai	Faux	Faux
(7)	$2^{\ln(n)}$	n^2	Vrai	Faux	Faux	Vrai
(8)	2^n	$n^{\ln\ln(n)}$	Faux	Vrai	Faux	Faux
(9)	$2^{\sqrt{\ln(n)}}$	$\sqrt{n}$	Vrai	Faux	Faux	Vrai

Nous utilisons souvent le fait que

$$f(n) = o(g(n)) \implies f(n) = O(g(n))$$

Il est souvent plus rapide de montrer que $f(n) = o(g(n))$.

(1)
$$\lim_{n\to\infty} \frac{n^{1/100}}{\sqrt{n}} = \lim_{n\to\infty} n^{-49/100} = 0.$$

Donc $f(n) = o(g(n))$.

(2)
$$\lim_{n\to\infty} \frac{\ln n}{\ln^2 n} = \lim_{n\to\infty} \frac{1}{\ln n} = 0$$

Donc $f(n) = o(g(n))$.

(3) On a:
$$\lim_{n\to\infty} \frac{\ln^2 n}{\sqrt{n}} = \lim_{n\to\infty} e^{\ln \frac{\ln^2 n}{\sqrt{n}}} = \lim_{n\to\infty} e^{2\ln\ln n - (1/2)\ln n} = \lim_{n\to\infty} e^{h(n)} = 0$$

En effet, si on pose le changement de variable $x = \ln n$ on voit que $\lim_{n\to\infty} x = \infty$, et donc
$$\lim_{n\to\infty} h(n) = \lim_{n\to\infty} 2\ln\ln n - \frac{1}{2}\ln n = \lim_{x\to\infty} 2\ln x - \frac{x}{2} = -\infty$$

Donc $g(n) = o(f(n))$.

(4) Pour tout n on a $\frac{2^n}{n!} > 0$, et pour tout $n > 3$:
$$\frac{2^n}{n!} = \frac{2\cdot\ldots\cdot 2}{1\cdot\ldots\cdot n} = 2\cdot\frac{2\cdot\ldots\cdot 2}{3\cdot\ldots\cdot n} < 2\cdot(\frac{2}{3})^{n-2}$$

Or on sait que
$$\lim_{n\to\infty} 2\cdot(\frac{2}{3})^{n-2} = 0$$

Donc $f(n) = o(g(n))$.

(5) On a:
$$\log_2 n = \frac{\log_3 n}{\log_3 2}$$

Quand on a $f(n) = k\cdot g(n)$ pour une constante k on a toujours $f(n) = \Theta(g(n))$.

(6) Si on pose le changement de variable $x = \ln n$, on voit d'abord que $\lim_{n\to\infty} x = \infty$. On a donc
$$\lim_{n\to\infty} \frac{\ln\ln n}{\ln n} = \lim_{x\to\infty} \frac{\ln x}{x} = 0$$

et donc $g(n) = o(f(n))$.

(7) On voit d'abord que $2^{\ln(n)} = 2^{\frac{\log_2(n)}{\log_2(e)}} = n^{\frac{1}{\log_2(e)}}$. On remarque ensuite que $\frac{1}{\log_2(e)} \simeq 0.693 < 2$. Ainsi:

$$\lim_{n\to\infty} \frac{2^{\ln(n)}}{n^2} = \lim_{n\to\infty} \frac{n^{\frac{1}{\log_2(e)}}}{n^2} = \lim_{n\to\infty} n^{\alpha} = 0$$

puisque $\alpha = \frac{1}{\log_2(e)} - 2 < 0$. Et donc on a $f(n) = o(g(n))$.

(8) On voit que:

$$\lim_{n\to\infty} \frac{n^{\ln\ln n}}{2^n} = \lim_{n\to\infty} e^{\ln\ln n \cdot \ln n - n\ln 2} = 0$$

et donc $g(n) = o(f(n))$.

(9)

$$\lim_{n\to\infty} \frac{2^{\sqrt{\ln n}}}{\sqrt{n}} = \lim_{n\to\infty} e^{\sqrt{\ln n}\cdot\ln 2 - \frac{1}{2}\ln n} = 0$$

et donc $f(n) = o(g(n))$.

4. L'algorithme de Karatsuba

a) Quand $p(x)$ un polynôme, nous l'écrivons parfois p pour simplifier la notation.

f et g sont des polynômes de degré 1. On sépare f en deux polynômes de degré 0: $f_0(x) = a$ et $f_1(x) = b$. De même on a $g_0(x) = \alpha$ et $g_1(x) = \beta$. On fait maintenant:

$$\begin{array}{rcll} h_0 & := & f_0 \cdot g_0 = a \cdot \alpha & \text{(1 multiplication)} \\ h_2 & := & f_1 \cdot g_1 = b \cdot \beta & \text{(1 multiplication)} \\ u & := & f_0 + f_1 = a + b & \\ v & := & g_0 + g_1 = \alpha + \beta & \\ A & := & u \cdot v = (a+b)\cdot(\alpha+\beta) & \text{(1 multiplication)} \\ h_1 & := & A - h_0 - h_2 & \end{array}$$

Et on obtient ainsi h_0, h_1 et h_2, les coefficients du produit. On a donc fait 3 multiplications d'éléments de $\mathbb{R}$: $a \cdot \alpha$, $b \cdot \beta$, et $(a+b)\cdot(\alpha+\beta)$.

b) il faut multiplier chaque coefficient de f par chaque coefficient de g, donc $4 \cdot 4 = 16$ multiplications.

c) On a $f(x) = f_0(x) + f_1(x) * x^2$ (voir le cours p. 34), et de même pour $g(x)$, ce qui nous donne:

$$\begin{array}{rcl} f_0 & = & 1 + 2x \\ f_1 & = & 1 + 2x \\ g_0 & = & 2 + 2x \\ g_1 & = & 1 + x \\ u & = & 2 + 4x \\ v & = & 3 + 3x \end{array}$$

d) On veut trouver

$$f(x) \cdot g(x) = h(x) = h_0(x) + h_1(x) \cdot x^2 + h_2(x) \cdot x^4$$

où $h_0(x), h_1(x)$ et $h_2(x)$ sont des polynômes de degré 2 (voir le cours).

On calcule d'abord $h_0 = f_0 \cdot g_0 = (1 + 2x)(2 + 2x)$. Pour ce, on utilise de nouveau l'algorithme de Karatsuba. Posons $h_0 = a + bx + cx^2$. On fait $a = 1 \cdot 2 = 2$, $b = 2 \cdot 2 = 4$ et $A = (1+2) \cdot (2+2) = 12$. Finalement, pour obtenir b on fait $b = A - a - b = 12 - 2 - 4 = 6$. On a donc trouvé $h_0 = 2 + 6x + 4x^2$, en 3 multiplications.

Ensuite il nous faut trouver $h_2 = f_1 \cdot g_1 = (1 + 2x)(1 + 1x)$. On utlise de nouveau l'algorithme de Karatsuba, pour obtenir $h_2 = (1 + 3x + 2x^2)$, en 3 multiplications.

Nous devons ensuite calculer $A = (f_0 + f_1) \cdot (g_0 + g_1) = (2 + 4x) \cdot (3 + 3x)$. On peut de nouveau utiliser l'algorithme de Karatsuba, pour obtenir $A = 6 + 18x + 12x^2$ en 3 multiplications.

On obtient $h_1 = A - h_0 - h_2 = (6+18x+12x^2) - (2+6x+4x^2) - (1+3x+2x^2) = 3+9x+6x^2$.

Ainsi, on a trouvé:

$$\begin{aligned} h(x) &= h_0(x) + h_1(x) \cdot x^2 + h_2(x) \cdot x^4 \\ &= (2 + 6x + 4x^2) + (3 + 9x + 6x^2) \cdot x^2 + (1 + 3x + 2x^2) \cdot x^4 \\ &= 2 + 6x + 7x^2 + 9x^3 + 7x^4 + 3x^5 + 2x^6 \end{aligned}$$

On remarque que pour trouver h à partir de h_0, h_1, et h_2 nous n'avons pas eu besoin de faire de multiplications (seulement des additions).

Ils nous a donc fallu exactement 9 multiplications de réels (remarquons cependant que nous avons aussi dû faire des additions de réels).

e) * La première décomposition effectué par l'algorithme de Karatsuba non-modifié résulte en les trois multiplications suivante:

(1) $[(0 + f_1)x + (f_2 + f_0)] \cdot [(0 + g_1)x + (g_2 + g_0)]$ (nécessite 3 multiplications)

(2) $(0x + f_2) \cdot (0x + g_2) = f_2 g_2$ (nécessite 1 multiplication)

(3) $(f_1 x + f_0) \cdot (g_1 x + g_0)$ (nécessite 3 multiplications)

Donc en total, on utilise 7 multiplications, toujours une de trop. On peut encore épargner une multiplication en observant que le premier pas ci-dessus calculera $f_1 g_1$, et le troisième aussi. Au lieu de recalculer cela, on peut alors simplement réutiliser le résultat.

5. Elever une matrice au carré

a) Nous connaissons a, c, b et d et voulons calculer:

$$A^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & cb + d^2 \end{pmatrix}$$

Ecrit de cette façon il nous faudrait 8 multiplications pour calculer A^2. Elles ne sont cependant pas toutes nécessaires, en effet en peut réécrire notre matrice comme suit:

$$A^2 = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & bc + d^2 \end{pmatrix}$$

La multiplication sur $\mathbb{R}$ est commutative et distributive, cette dernière matrice est donc bien égale à A^2. On voit que bc apparait deux fois, mais il nous suffit le calculer une seule fois. Les factorisations nous permettent également de remplacer deux multiplications par une seule. Pour calculer a^2 nous avons donc besoin des 5 multiplications suivantes: $a * a, d * d, b * c, b * (a + d), c * (a + d)$.

On remarque qu'il nous faut aussi 4 additions d'éléments de $\mathbb{R}$.

b) Malheureusement cet algorithme ne peut pas être généralisé pour élever des matrices de taille quelconque au carré. Nous illustrerons maintenant pourquoi, dans ce cas, on ne peut pas appliquer la technique diviser-pour-régner pour généraliser l'algorithme.

De manière générale, un algorithme diviser-pour-régner réduit les problèmes de taille n à des sous-problèmes du même type de plus petite taille. Par exemple, l'algorithme de Karatsuba réduit le calcul de deux polynomes de degré $< 2n$ au calcul de trois produits de polynômes de degre $< n$. De manière similaire, l'algorithme de Strassen permet de réduire le calcul du produit matriciel de deux matrices de taille $2n \times 2n$ à des produits matriciels de taille n.

Supposons que a, b, c et d sont elles-mêmes des matrices $n \times n$, et que la matrice A que nous aimerions élever au carré est donc une matrice $2n \times 2n$.

La technique diviser-pour-régner consisterait maintenant en la réduction du calcul du carré de la $2n \times 2n$-matrice A au calcul de carrés de matrices de taille $n \times n$.

Mais les produits des a, b, c, d comme obtenus sous le point précédent ne sont pas tous des carrés! Nous ne pourrons donc pas récursivement utiliser le même algorithme pour effectuer ces calculs. Nous aurons besoin d'un algorithme de multiplication de matrices général à la place.

Un deuxième problème est que nous avons utilisé la commutativité de la multiplication dans $\mathbb{R}$ pour trouver nos produits. Les formules ne resteront donc pas valides si a, b, c et d sont des matrices, parce que le produit matriciel n'est pas, en général, commutatif.