info528 : Mathématiques pour l'informatique
TD 0 : les subtilités de la puissance et des polynômes...
SOLUTIONS

Pierre Hyvernat
Laboratoire de mathématiques de l'université de Savoie
bâtiment Chablais, bureau 22, poste : 94 22
email : Pierre.Hyvernat@univ-savoie.fr
www : http://www.lama.univ-savoie.fr/~hyvernat/

Partie 0 : calculs préliminaires instructifs

Question 1. À l'aide d'une calculatrice ou d'un ordinateur, remplissez le tableau suivant. La première colonne indique la complexité en microsecondes d'un algorithme pour une entrée de taille n. Pour chaque colonne, estimez le temps d'exécution de cet algorithme pour une entrée de la taille donnée.

	5	10	50	100	1000	10000
n	5×10^{-6} s	10^{-5} s	5×10^{-5} s	10^{-4} s	10^{-3} s	10^{-2} s
$n\log(n)$	$11{,}6\times10^{-6}$ s	$3{,}32\times10^{-5}$ s	$2{,}82\times10^{-4}$ s	$6{,}64\times10^{-4}$ s	$9{,}97\times10^{-2}$ s	0,133 s
n^2	$2{,}5\times10^{-5}$ s	10^{-4} s	$2{,}5\times10^{-3}$ s	0,01 s	1 s	1 m40 s
n^3	$1{,}3\times10^{-4}$ s	0,001 s	0,125 s	1 s	16 m40 s	11 j13 h
n^5	$3{,}1\times10^{-3}$ s	0,1 s	5 m12 s	2 h 47 m	31 ans	3×10^{6} ans
2^n	$3{,}2\times10^{-5}$ s	10^{-3} s	35 ans	$4\times10^{7}\times10^{9}$ ans	$3.3\times10^{278}\times10^{9}$ ans	$6.3\times10^{2987}\times10^{9}$ ans
2^{2^n}	1 h11 m	$5.7\times10^{285}\times10^{9}$ ans	$10^{10^{15}}\times10^{9}$ ans	???	???	???

rq : l'âge de l'univers est estimé à 13,7 milliards d'années, et il y a environ $3.15.10^7 \approx 2^{25}$ secondes dans une année

Question 2. Quelles sont les classes de complexité "raisonnables" ?

Si on estime que la loi de Moore est valide (la puissance de calcul double tous les deux ans), quelles sont les classes de complexité qui peuvent basculer du "infaisable" dans le "raisonnable" ?

Partie 1 : complexité de la puissance

Question 1. Programmez (en C par exemple) une fonction `puissance` qui prend en argument en entier `n` et un nombre `x` et qui calcule

$$\underbrace{\mathtt{x}\times\mathtt{x}\times\cdots\times\mathtt{x}}_{\mathtt{n}}$$

Vous ne pouvez utiliser que les fonctions arithmetiques usuelles (addition, soustraction multiplication, division, test).

Question 2. En cryptographie, en a souvent besoin de calculer une puissance *modulo* un autre nombre. Modifiez votre fonction pour prendre un argument supplémentaire `m`.

Question 3. Toujours en cryptographie, il arrive fréquemment que l'on ai besoin de calculer des puissances où `n` contient plusieurs centaines de chiffres.

Combien de multiplications sont utilisées par votre algorithme ? Qu'en pensez-vous ?

Question 4. La *méthode chinoise* pour calculer la puissance d'un nombre est basée sur les remarques suivantes :

$$\begin{array}{rcl} x^0 & = & 1 \\ x^{2n} & = & x^n \times x^n \\ x^{2n+1} & = & x^n \times x^n \times x \ . \end{array}$$

Programmez une fonction `puissance_chinoise` récursive qui calcule $\texttt{x}^{\texttt{n}} \bmod \texttt{m}$.

Question 5. Combien de multiplications sont utilisées par votre algorithme ? Qu'en pensez-vous ?

Question 6. Il est possible d'utiliser une variante des formules précédentes :

$$\begin{array}{rcl} x^0 & = & 1 \\ x^{2n} & = & (x \times x)^n \\ x^{2n+1} & = & (x \times x)^n \times x \ . \end{array}$$

Programmez la fonction (récursive) correspondante.

Question 7. La fonction `puissance_chinoise` (première ou seconde variante) est beaucoup plus efficace que la fonction `puissance`. Il reste le problème que les fonctions récursives consomment en général plus de mémoire que les fonctions purement itératives.

Pour transformer la fonction `puissance_chinoise` en fonction itérative, il faut utiliser des *accumulateurs* pour ecrire une fonction récursive terminale ou utiliser une boucle.

Programmez une version itérative de la seconde version de `puissance_chinoise`.

Question 8. Combien de multiplications sont utilisées par notre algorithme pour le calcul de x^{15} ?

En utilisant le fait que $15 = 3 \times 5$, trouvez une méthode pour calculer x^{15} avec moins de multiplications que la méthode chinoise.

Est-ce que cette remarque vous permet de trouver une méthode plus efficace que la méthode chinoise ?

> *Solution :* pour $n = 23$, la méthode chinoise donne 7 multiplications, la méthode des premiers (si p premier : $x^p = x^{p-1} \times x$ et sinon $x^{pn} = (x^p)^n$) donne également 7 multiplications.
>
> L'arbre des puissances (Knuth) donne 23 – 13 – 10 – 5 – 3 – 2 – 1 soit 6 multiplications.
>
> Pour 33 la méthode chinoise est meilleure que la méthode des premiers (8 multiplications contre 9, contre 6 avec l'arbre des puissances).

Partie 2 : subtilité des polynômes

Question 1. Combien de multiplications sont nécessaires pour évaluer un polynôme de degré n sur un entier ? (On suppose que tous les coefficients sont non-nul.)

> *Solution :* si on utilise le calcul efficace des exposants, on trouve $O(\log(n!))$. En utilisant la formule de Stirling ($n! \sim \sqrt{2\pi n}\frac{n^n}{e^n}$), on obtient un nombre de multiplications en $O(n \log(n))$.

Question 2. Quel est le nombre (exact) de multiplications et additions utilisées si on calcule les puissances "normalement", mais en réutilisant les calculs. (On suppose à nouveau que tous les coefficients sont non-nuls.)

Solution : nombre de multiplications est $2n-1$ et le nombres d'additions est n.

Question 3. Même question si on utilise la règle de Horner :

$$c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n \quad = \quad \Big(\ldots \Big(\big((c_n x + c_{n-1}) x + c_{n-2} \big) x + c_{n-3} \Big) \ldots \Big) x + c_0$$

Solution : on utilise n additions et n multiplications.

Question 4. Pensez-vous que l'on peut améliorer la fonction d'évaluation pour les polynômes *creux*. (Les polynômes où la plupart des coefficients sont nuls.)

Solution : pour les polynômes creux, il faut mieux représenter un polynôme par un tableau de couples `(coeff, degre)` trié par degré. Pour évaluer un tels polynôme, on utilise en même temps la méthode de Horner et la puissance chinoise (pour calculer $x^{d_{i+1}-d_i}$