Université Paris Diderot - L3 — Année universitaire 2010–2011

Partiel de Mathématiques Discrètes

Mardi 16 Novembre 2010

Durée : 1 heure 50

Le barème est donné à titre indicatif.

Exercice 1 : Algorithme de Karatsuba (6 points)

L'algorithme de Karatsuba est une application du principe « diviser pour régner »lors de la multiplication de deux entiers :
soient a et b deux entiers à $n = 2^m$ chiffres : $a = a_1 \times 10^{\frac{n}{2}} + a_0$ et $b = b_1 \times 10^{\frac{n}{2}} + b_0$ avec a_0, a_1, b_0 et b_1 ayant $\frac{n}{2} = 2^{m-1}$ chiffres. Alors

$$\begin{aligned} a \times b &= a_1 \times b_1 \times 10^n + (a_0 \times b_1 + a_1 \times b_0) \times 10^{\frac{n}{2}} + a_0 \times b_0 \\ &= a_1 \times b_1 \times 10^n + (a_1 \times b_1 + a_0 \times b_0 - (a_1 - a_0)(b_1 - b_0)) \times 10^{\frac{n}{2}} + a_0 \times b_0 \end{aligned}$$

L'algorithme est donc le suivant :

```
Mult(a,b,n)
 Si n = 1 Alors Retourner a x b
 n1 <- n/2
 temp1 <- Mult(a1,b1,n1)
 temp2 <- Mult(a0,b0,n1)
 temp3 <- Mult(a1-a0,b1-b0,n1)
 Retourner temp1 x 10^(n) + (temp1 + temp2 - temp3) x 10^(n1) + temp2
```

On considère que les décompositions de a en a_1a_0, b en b_1b_0, les multiplications par des puissances de 10 et la division par 2 sont obtenues de façon immédiate et ne comptent donc pas dans un calcul de complexité en temps. Seuls comptent les calculs de `temp1`, `temp2`, `temp3` et les additions-soustractions. On considère que le coût d'une addition, soustraction ou multiplication de deux nombres à 1 chiffre compte pour 1.

1. Montrer que la complexité en temps k_m de l'algorithme de Karatsuba pour deux nombres à $n = 2^m$ chiffres vérifie la récurrence suivante : $\begin{array}{lcl} k_0 &=& 1 \\ k_m &=& 3k_{m-1} + 4 \times 2^m \end{array}$
2. Soit la série génératrice $K(z) = \sum_{m \geqslant 0} k_m z^m$. Montrer qu'elle vérifie l'équation
$$(1 - 3z)K(z) = \frac{1 + 6z}{1 - 2z}.$$
3. Calculer alors k_m en fonction de m, puis k_n en fonction de n.

Exercice 2 : Compositions d'un entier (4 points)

On appelle composition d'un entier n, une suite $(x_1, \dots, x_k)$ d'entiers strictement positifs telle que $n = x_1 + \cdots + x_k$. Les $x_i, 1 \leqslant i \leqslant k$, sont appelés les parts de la composition. Par exemple $(3, 1, 4, 1, 6, 4)$ est une composition en 6 parts de 19.

1. [facultatif] Une composition d'un entier n peut-être vue graphiquement comme le placement de barres verticales entre certains des n points alignés, chaque groupe de points entre deux barres verticales (ou celui à gauche de la barre la plus à gauche, ou encore celui à droite de la barre la plus à droite) représente alors une part de la composition. Par exemple la composition $(3, 1, 4, 1, 6, 4)$ a pour représentation graphique :

   $$. \; . \; . \mid . \mid . \; . \; . \; . \mid . \mid . \; . \; . \; . \; . \; . \mid . \; . \; . \; .$$

   En utilisant la représentation graphique, montrer que le nombre de compositions $c_{k,n}$ de n à k parts est égal à $\binom{n-1}{k-1}$.
2. Soit $C_k(z) = \sum_{n \geqslant 1} c_{k,n} z^n$, la série génératrice des compositions à k parts. Montrer que

   $$C_k(z) = \sum_{n \geqslant 1} \left(\sum_{x_1 + \ldots + x_k = n} 1 \right) z^n.$$
3. Calculer alors l'équation fonctionnelle vérifiée par $C_k(z)$.
4. [facultatif] Déduire des questions 1 et 3 une identité pour $[z^n]C_k(z)$.

Exercice 3 : Involutions (7 points)

Une involution σ de $\{1, \dots, n\}$ est une permutation de $\{1, \dots, n\}$ telle que $\sigma^2 = 12 \dots n$. C'est donc une permutation dont les cycles qui la composent sont de longueurs inférieures ou égales à 2.

Par exemple la permutation $\sigma = 3214 = (13)(2)(4)$ est une involution et on a bien $\sigma^2 = 1234$ car $\sigma(\sigma(1)) = \sigma(3) = 1$, $\sigma(\sigma(2)) = \sigma(2) = 2$, $\sigma(\sigma(3)) = \sigma(1) = 3$ et $\sigma(\sigma(4)) = \sigma(4) = 4$.

1. On note i_n le nombre d'involution de $\{1, \dots, n\}$. Montrer que

   $$i_0 = 1, \quad i_1 = 1 \quad \text{et} \quad \forall n \geqslant 2, \quad i_n = i_{n-1} + (n-1) i_{n-2}$$
2. Soit $I(z)$ la série génératrice exponentielle du nombre d'involutions.
   (a) Montrer que $\qquad I'(z) = (z+1)I(z) \quad (*)$.
   (b) L'ensemble des solutions de l'équation différentielle $(*)$ est $Ce^{z + \frac{z^2}{2}}$ où C est une constante. Déduire de l'équation $(*)$ une formule close pour $I(z)$.
3. Montrer alors que $i_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n!}{2^k (n-2k)! k!}$ où $\lfloor \frac{n}{2} \rfloor$ représente la partie entière de $\frac{n}{2}$.

Exercice 4 : Langages rationnels (3 points)

1. Montrer que le langage $L = \{b^n a^p \mid n, p \in \mathbb{N}$ et n et p sont pairs$\}$ est rationnel.
2. Soit le langage L' de $\{a, b\}^*$ tel que toute occurence du facteur $b^n a^p, n, p \geqslant 1$, n et p maximals, dans un mot de L', soit tel que n ou p est impair (par exemple $a^2 b^4 a^3 ba \in L'$, mais $a^2 b^4 a^3 b^2 a^2 \notin L'$ car le facteur $b^2 a^2$ ne vérifie pas les conditions requises). Montrer sans exhiber d'automate, que L' est rationnel.