Corrigé de l'Examen Algorithmique et complexité

M1 informatique, 2006–2007

1. Rappeler en 3 lignes les formules permettant de calculer de façon rapide M^n, où M est une matrice carrée et n un exposant entier.

Réponse : $M^0 = I$ où I est la matrice identité.

$M^{2n} = (M^2)^n$. Donc puiss$(M, 2n)$ = puiss$(M \times M, n)$. $M^{2n+1} = M \times M^{2n}$, donc puiss$(M, 2n+1) = M \times$ puiss$(M \times M, n)$. A chaque appel récursif, l'exposant est divisé par 2.

2. Quel est l'ordre de grandeur du nombre de multiplications matricielles nécessitées par la méthode précédente pour calculer M^n ?

Réponse : $O(\log n)$ appels récursifs, et donc multiplications matricielles sont nécessaires.

3. La suite de Fibonacci est définie par : $F(0) = F(1) = 1$, $F(n > 1) = F(n-1) + F(n-2)$. Donc, pour $n > 1$, il existe une matrice M telle que le vecteur $(F(n), F(n-1))$ soit égal à $(F(n-1), F(n-2))M$. Précisez la valeur de la matrice M, en 2 lignes.

Réponse :

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

4. Donner les valeurs de $F(0), F(1), F(2), F(3), F(4), F(5), F(6), F(7), F(8), F(9), F(10)$.

Réponse :

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89$$

5. Exprimer $(F(n), F(n-1))$ en fonction du vecteur $(F(1), F(0))$ et de la matrice M précédente (répondre en 2 lignes au maximum).

Réponse :

$$(F(n), F(n-1)) = (F(1), F(0)) \times M^{n-1}$$

Donc l'exponentiation rapide permet de calculer $F(n)$ en $O(\log_2 n)$ produits de matrice 2×2.

6. En déduire une méthode rapide pour calculer $F(n)$. Quel est son coût ? Répondre en 1 ligne au maximum.

Réponse : Donc l'exponentiation rapide permet de calculer $F(n)$ en $O(\log_2 n)$ produits de matrice 2×2.

7. Généraliser la méthode précédente au calcul de $G(n)$, où G est la suite définie par : $G(0) = g_0, G(1) = g_1, G(2) = g_2, G(n > 2) = a \times G(n-1) +$

$b \times G(n-2) + c \times G(n-3)$; g_0, g_1, g_2, a, b, c désignent des constantes connues. Répondre en 5 lignes maximum.

Réponse :

$$(G(n), G(n-1), G(n-2)) = (G(n-1), G(n-2), G(n-3))M, M = \begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \\ c & 0 & 0 \end{pmatrix}$$

$$(G(n), G(n-1), G(n-2)) = (g_2, g_1, g_0)M^{n-2}$$

8. Les termes de la suite de Fibonacci sont les coefficients de la série

$$S(z) = \frac{1}{1 - z - z^2} = 1 + z + 2z^2 + 3z^3 + 5z^4 + 8z^5 + \ldots$$

Comme les termes de beaucoup de suites sont les coefficients de séries $p(z)/q(z)$, où p et q sont des polynômes en z, il est intéressant de disposer d'une méthode efficace pour calculer les coefficients de telles séries. Considérez la série

$$T(z) = \frac{1}{a_0 + a_1 z + a_2 z^2 + a_3 z^3} = q_0 + q_1 z + q_2 z^2 + q_3 z_3 + q_4 z^4 + \ldots$$

Les termes a_i sont donnés, et $a_0 \neq 0$. Par définition :

$$(a_0 + a_1 z + a_2 z^2 + a_3 z^3)(q_0 + q_1 z + q_2 z^2 + q_3 z_3 + q_4 z^4 + \ldots) = 1$$

et comme :

$$\begin{array}{ll} (& a_0 + a_1 z + a_2 z^2 + a_3 z^3)(q_0 + q_1 z + q_2 z^2 + q_3 z_3 + q_4 z^4 + \ldots) \\ = & (a0q0) \\ + & (a_0 q_1 + a_1 q_0) z \\ + & (a_0 q_2 + a_1 q_1 + a_2 q_0) z^2 \\ + & (a_0 q_3 + a_1 q_2 + a_2 q_1 + a_3 q_0) z^3 \\ + & (a_0 q_4 + a_1 q_3 + a_2 q_2 + a_3 q_1) z^4 + \ldots \end{array}$$

les coefficients q_i s'en déduisent :

$$\begin{array}{lcl} q_0 & = & 1/a_0 \\ q_1 & = & -a_1 q_0/a_0 \\ q_2 & = & -(a_1 q_1 + a_2 q_0)/a_0 \\ q_3 & = & -(a_1 q_2 + a_2 q_1 + a_3 q_0)/a_0 \\ q_4 & = & -(a_1 q_3 + a_2 q_2 + a_3 q_1)/a_0 \\ q_5 & = & -(a_1 q_4 + a_2 q_3 + a_3 q_2)/a_0 \\ q_k & = & -(a_1 q_{k-1} + a_2 q_{k-2} + a_3 q_{k-3})/a_0 \end{array}$$

Déduisez en que le vecteur (q_k, q_{k-1}, q_{k-2}) est égal au produit du vecteur $(q_{k-1}, q_{k-2}, q_{k-3})$ par une matrice W que vous préciserez (3 lignes au plus).

Réponse :

$$(q_k, q_{k-1}, q_{k-2}) = (q_{k-1}, q_{k-2}, q_{k-3}) \times W, \quad W = \begin{pmatrix} -a_1/a_0 & 1 & 0 \\ -a_2/a_0 & 0 & 1 \\ -a_3/a_0 & 0 & 0 \end{pmatrix}$$

9. Exprimez (q_k, q_{k-1}, q_{k-2}) en fonction de (q_2, q_1, q_0) et de W. Répondre en 1 ligne au plus.

Réponse :

$$(q_k, q_{k-1}, q_{k-2}) = (q_2, q_1, q_0) \times W^{k-2}$$

10. En supposant que la fonction $C(q, i)$ rende le coefficient du monôme z^i dans la série $1/q(z)$, quel est le coefficient du monôme z^i dans la série $z^k/q(z)$?

Réponse : C'est $C(q, i-k)$ (donc il faut que $k \leq i$).

11. En reprenant l'exemple de la série $S(z)$ associée à la suite de Fibonacci :

$$\begin{array}{rcccccccccccc} S(z) & = & 1 & + & z & + & 2z^2 & + & 3z^3 & + & 5z^4 & + & 8z^5 & + & \dots \\ z \times S(z) & = & & & z & + & z^2 & + & 2z^3 & + & 3z^4 & + & 5z^5 & + & \dots \\ z^2 \times S(z) & = & & & & & z^2 & + & z^3 & + & 2z^4 & + & 3z^5 & + & \dots \end{array}$$

vous pouvez vérifier que $S(z) - z \times S(z) - z^2 \times S(z) = 1 \Rightarrow S(z)(1 - z - z^2) = 1$. Proposez une méthode heuristique pour deviner les polynômes p et q d'une relation : $S(z)q(z) = p(z)$, dans le cas où la suite est donnée par ses d premiers termes (vous pouvez supposer $d = 10$).

Réponse : Soit V_0 le vecteur des d premiers termes de la suite, soit $V_1, V_2, \dots V_k$, où V_k est la suite V_0 décalée de k cases vers la droite; elle est complétée avec k termes 0 en tête, et k termes sont tronqués à droite. Soit $e_0 = (1, 0, 0 \dots)$, $e_1 = (0, 1, 0, 0 \dots)$, jusqu'à e_k, nul partout sauf en position k où il vaut 1. Tous les vecteurs ont d éléments. Si les vecteurs $V_0, V_1, \dots V_k, e_0, e_1, \dots e_k$ ne sont pas indépendants (et que il y a moins de p vecteurs, donc $2(k+1) < d$), alors il existe une relation linéaire entre ces vecteurs et elle donne les polynômes, qui sont de degrés k (ou moins).

12. Donnez les premiers termes de la série : $\frac{1}{1-2z}$.

Réponse :

$$\frac{1}{1-2z} = 1 + 2z + 4z^2 + 8z^3 + 16z^4 + 32z^5 + \dots = \sum_{i=0}^{\infty} 2^i z^i$$

13. Soit M une matrice carrée de taille $s \times s$, à coefficients entiers naturels (positifs ou nuls); soit C l'entier le plus grand dans M, et $c = \log_2 C$. Majorer le plus grand entier de M^n.

Réponse : Le plus grand nombre dans M^n est au plus $s^{n-1}C^n$. Son log est $s \log(n-1) + n \log C$.

14. Quand avons nous utilisé le fait que $\log(n!) \approx n \log n$?

Réponse : Par exemple dans l'analyse en complexité des tris optimaux. Il y a $n!$ permutations (ordres possibles) *a priori*. Si chaque comparaison/question

élimine la moitié des permutations possibles, il faut un minimum de $\log_2 n!$ comparaisons pour trier n éléments. Comme $\log_2 n! \approx n \log_2 n$, un tri en $O(n \log_2 n)$ comparisons est optimal.

15. Peut il exister deux polynômes a et b tels que les coefficients de $z^0, z^1, z^2 \ldots$ de la série $a(z)/b(z)$ soient les factorielles de 0, 1, 2 ... ?

Réponse : Supposons qu'ils existent, alors il existe une matrice W telle que:

$$(n!, n-1!, n-s+1!) = (s-1!, s-2!, \ldots 1!, 0!)W^{n-s+1}$$

Mais si C est l'entrée la plus grande dans W, alors le log de l'entrée la plus grande dans W^n est en $O(s \log(n-s) + n \log C)$, ce qui est plus petit que $\log n! \approx n \log n$, pour n assez grand. C'est une contradiction. Donc il n'existe pas une telle série pour la suite des factorielles : elles croissent trop vite, plus vite que toutes les exponentielles C^n.

16. Soient $\phi = (1+\sqrt{5})/2 \approx 1.618\ldots$ et $\phi' = (1-\sqrt{5})/2 \approx -0.618\ldots$. ϕ et ϕ' sont les deux racines du polynôme $z^2 - z - 1 = 0$. Soit la fonction $f(n) = (\phi^{n+1} - \phi'^{n+1})/\sqrt{5}$. Evaluer $f(0), f(1), f(2), f(3), f(4)$?

Réponse :

$$f(0) = (\phi - \phi')/\sqrt{5} = 1$$

$$f(1) = (\phi^2 - \phi'^2)/\sqrt{5} = (\phi + 1 - (\phi' + 1))/\sqrt{5} = 1$$

$$f(2) = (\phi^3 - \phi'^3)/\sqrt{5} = (\phi^2 + \phi - (\phi'^2 + \phi'))/\sqrt{5} = 2$$

$$f(3) = 3, f(4) = 5$$

17. $f(n), n \in \mathbb{N}$ définit une suite, qui a déjà été rencontrée. Dire laquelle et le prouver par récurence.

Réponse : $f(n)$ est $F(n)$, c'est à dire Finonacci de n. C'est vrai pour $n = 0$ et $n = 1$. Admettons que ce soit vrai jusqu'à $k \geq 1$, et prouvons alors que c'est aussi vrai pour $k+1$;

$$\begin{aligned} f(k+1) &= (\phi^{k+2} - \phi'^{k+2})/\sqrt{5} \\ &= ((\phi^{k+1} + \phi^k) - (\phi'^{k+1} + \phi'^k))/\sqrt{5} \\ &= ((\phi^{k+1} + \phi^k)/\sqrt{5} - (\phi'^{k+1} + \phi'^k)/\sqrt{5} \\ &= f(k) + f(k-1) \end{aligned}$$

Les deux premiers termes de f sont égaux à ceux de la suite de Fibonacci, et f vérifie la même relation de récurrence. Donc f est la suite de Fibonacci.

18. Il semble que $f(n)$ puisse être calculée en temps constant : dites comment. Où est le piège?

Réponse : $\phi^n = \exp(n \times \log \phi)$. De même pour $\phi'^n = \exp(n \times \log \phi')$. Un nombre constant d'opérations *flottantes* permet donc de calculer $f(n)$ (en admettant que log et exp nécessitent un nombre constant d'opérations, ce qui est le cas en arithmétique flottante). Le piège est que les calculs flottants sont approchés. Cependant, pour des valeurs de n pas trop grandes, il est possible d'utiliser cette méthode. En fait comme $|\phi'| < 1$, les puissances de ϕ' ont toutes

une valeur absolue inférieure à 1, et donc l'entier le plus proche de $\phi^{n+1}/\sqrt{5} = (\exp((n+1.) \times \log \phi))/\sqrt{5}$ est $f(n)$.

19. Prouver que la suite de Fibonacci, modulo un entier p, est ultimement périodique (périodique, en enlevant un début suffisament long).

Réponse : La suite ne peut prendre que p valeurs distinctes; il n'y a que p^2 couples distincts de valeurs consécutives possibles (pour $F(n)$ et $F(n+1)$). Donc $F(p^2) \mod p, F(p^2+1) \mod p$ est forcément égal à un couple déjà rencontré. Or 2 termes consécutifs déterminent les termes suivants, et les termes entre les deux occurences du couple vont donc se répéter.

En fait la suite est non seulement ultimement périodique, mais périodique. En effet, deux termes consécutifs déterminent le terme précédent. Utilisez ensuite l'argument du paragraphe précédent.

Voici un exemple d'une suite ultimement périodique, mais non périodique : $T_{n+1} = T_n^2 \mod p$. Tout élément a un carré et un seul modulo p, mais seul un élément sur 2 a une (en fait deux) racines carrées modulo p. Exemple, modulo 7, une orbite périodique est : 2, 4, 2 ...; une autre orbite, ultimement périodique, mais non périodique, est : $3, 2, 4, 2, 4, 2, 4 \ldots$. Comme un seul terme suffit à déterminer les termes suivants, la période ne peut être plus longue que p, le nombre d'éléments possibles.

20. L'algorithme suivant permet de calculer la longueur de la période d'une suite ultimement périodique, sans stocker les éléments de la suite dans une table : il utilise une quantité constante de mémoire. La suite $S(t)$ est parcourue en même temps à deux vitesses différentes; le pointeur lent se trouve sur $S(t)$ à l'instant t, pour $t = 0, 1, 2, 3, \ldots$; le pointeur rapide va deux fois plus vite et se trouve sur $S(2t)$ à l'instant t, pour $t = 0, 1, 2, 3, \ldots$; quand $S(t) = S(2t)$ pour $t > 0$, les deux pointeurs se rejoignent. Prouver que cet instant t est un multiple de la période. Ensuite, comment déterminer la période ?

Réponse : Soit $S(b)$ le premier élément de la boucle, et p le nombre d'éléments de la boucle. b est le plus petit indice tel que $S(b) = S(b+p) = S(b+2p) = S(b+kp)$, $k \in \mathbb{N}$. Au temps $b+t, t < p$, le lent se trouve en $b+t$, et le rapide en $b+(b+2t) \mod p$; si le lent et le rapide se rejoignent à cet instant $b+t$, alors $b+t = b+(b+2t) \mod p$; donc $b+t = 0$ modulo p. La date de la rencontre $R = b+t$ est donc un multiple de la période p : $R = kp$. En fait, en toute date multiple de la période et plus grande ou égale à b, le lent et le rapide sont sur le même élément de la boucle.

Pour déterminer la période (seulement un multiple est connu), il suffit de réutiliser la même méthode à partir de l'élément de la rencontre : p instants plus tard, le lent et le rapide se retrouveront sur ce même élément. Comme $R = kp$, on en déduit k. Comme $(k-1)p < b \leq kp$, d'où un intervalle pour b.

Cette méthode est utilisée dans la factorisation rho, de Pollard.