TD : Multiplication de Karatsuba

Dominique Michelucci, Université de Dijon

18 septembre 2012

La méthode naïve pour multiplier des entiers de n chiffres est en $O(n^2)$. (Par contre la méthode naïve pour additionner est linéaire...).

La multiplication de Karatsuba est plus rapide. Principe : pour multiplier A et B, avec A le plus grand, n chiffres dans la base utilisée, on écrit $A = a_0 + a_1\Omega$ et $B = b_0 + b_1\Omega$, où Ω est la puissance de la base, telle que a_0 et a_1 ont à peu près $n/2$ chiffres.

Calculer naïvement

$$A \times B = (a_0 + a_1\Omega)(b_0 + b_1\Omega) = (a_1 \times b_1)\Omega^2 + (a_0 \times b_1 + a_1 \times b_0)\Omega + (a_0 \times b_0)$$

en effectuant 4 produits sur des nombres deux fois plus courts est toujours en $O(n^2)$: en effet résoudre l'équation $T(n) = 4T(n/2)$, ou bien $T(n) = 4T(n/2)+n$ donne $T(n) = O(n^2)$. Vérifions :

Indication de preuve. Calculons d'abord la table de $T(1) = 1, T(n) = 4T(n/2)$ pour simplifier :

$\log_2 n$	n	$T(n)$
0	1	1
1	2	$4 = 2^2$
2	4	$16 = 4^2$
3	8	$64 = 8^2$
4	16	$256 = 16^2$

Clairement $T(n) = n^2 = O(n^2)$ sur ces exemples, et on le prouve trivialement par récurrence. Ensuite considérer $T(1) = 1, T(n) = 4T(n/2) + n$ a pour effet d'introduire des termes parasites, de plus bas degré, qui ne vont pas modifier le fait que $T(n) = O(n^2)$. Il vous est conseillé de le faire, en "travail à la maison" !

L'idée de Karatsuba est de n'utiliser que 3 multiplications, au lieu de 4. Il utilise davantage d'additions (ou soustractions), mais elles sont en temps linéaire.

$$AB = (a_1 \times b_1)\Omega^2 + ((a_0 + a_1) \times (b_0 + b_1) - a_1 \times b_1 - a_0 \times b_0)\Omega + (a_0 \times b_0)$$

Cette méthode est en $O(n^{\log_2 3}) = O(n^{1.5849625007211563})$. C'est la solution de l'équation de récurence de $T(n) = 3T(n/2) + n$. Vérifions le :

Indication de preuve. Considérons d'abord, pour simplifier, $T(1) = 1, T(n) =$

$3T(n/2)$. Calculons la table :

$\log_2 n$	n	$T(n)$
0	1	$1 = 3^0$
1	2	$3 = 3^1$
2	4	$9 = 3^2$
3	8	$27 = 3^3$
4	16	$81 = 3^4$

Elle suggère que $T(n) = 3^{\log_2 n}$, ce qui est facilement prouvé par récurrence (Faites le à la maison !). Ensuite, il faut prouver que $3^{\log_2 n} = O(n^{\log_2 3})$:

$$\begin{aligned} T(n) &= 3^{\log_2 n}. \text{ Or } 3 = 2^{\log_2 3} \\ &= (2^{\log_2 3})^{\log_2 n} \text{ mais } (a^b)^c = a^{b\times c} \\ &= 2^{(\log_2 3)(\log_2 n)} \\ &= 2^{(\log_2 n)(\log_2 3)} \\ &= (2^{(\log_2 n)})^{\log_2 3} \\ &= n^{\log_2 3} = O(n^{\log_2 3}) \end{aligned}$$

CQFD. Ensuite, considérer $T(n) = 3T(n/2)+n$ ne fait qu'ajouter des termes parasites, de plus bas degré. Faites le "à la maison".

N'a t-on rien oublié ? Les retenues ! Il faut les propager. Montrer que ce post traitement est linéaire en n.

Il y a des métodes plus compliquées et plus efficaces pour le produit, en gros en $O(n \log n)$ (je néglige des facteurs $\log(\log n)$...).

Aparté : conversion entre $\log_e X$ et $\log_k X$

Retrouvez la relation entre $\log_e X$ et $\log_k X$, où e est la base naturelle des log népériens.

Solution (à ne pas lire tout de suite...). Soit $X > 0$ un nombre. Soit $x = \log_k X \Leftrightarrow k^x = k^{\log_k X} = X$. Soit $x' = \log_e X' \Leftrightarrow e^{x'} = e^{\log_e X} = X$. Donc $X = k^x = e^{x'}$. D'où :

$$\log_e X = \log_e k^x = x \log_e k = (\log_k X)(\log_e k)$$

D'où : $\log_k X = \frac{\log_e X}{\log_e k}$ ou encore : $\frac{\log_e X}{\log_k X} = \log_e k$: tous les logarithmes sont proportionnels entre eux. Cela justifie la notation $O(\log b)$, où on ne précise pas la base du log.