Algoritmo de multiplicación de Karatsuba

Presenta: González Cárdenas Ángel Aquilez

1. Introducción

Partiendo de la conjetura que Andrey Kolmogorov realiza en 1960 durante su seminario en la Universidad Estatal de Moscú, donde establece que el método tradicional de multiplicar dos números (ambos de n-dígitos) requeriría una cantidad de operaciones elementales proporcional a n^2, o $\mathcal{O}(n^2)$, es donde Anatoly Alexeyevich Karatsuba (de 23 años), encuentra un algoritmo que multiplica dos números de n-dígitos con $\mathcal{O}(n^{\log_2 3})$ operaciones elementales.

2. Algoritmo

2.1. Secuencial

Algoritmo de Karatsuba

procedure KARATSUBA(X,Y) $\triangleright$ X, Y : números de n-dígitos
    $X = x_1 B^m + x_0$
    $Y = y_1 B^m + y_0$
    $XY = (x_1 B^m + x_0)(y_1 B^m + y_0)$

Haciendo

$$\begin{aligned} XY &= x_1 y_1 B^2 m + (x_1 y_0 + x_0 y_1) B^m + x_0 y_0 \\ &= z_2 B^2 m + z_1 B^m + z_0 \end{aligned}$$

donde

$$\begin{aligned} z_2 &= x_1 y_1, \\ z_1 &= x_1 y_0 + x_0 y_1, \\ z_0 &= x_0 y_0 \end{aligned}$$

Karatsuba observó que el producto de X con Y se puede expresar en sólo tres multiplicaciones haciendo

$$\begin{aligned}
z_1 &= x_1y_0 + x_0y_1, \\
&= x_1y_0 + x_0y_1 + x_1y_1 - x_1y_1 + x_0y_0 - x_0y_0 \\
&= x_1y_0 + x_0y_0 + x_0y_1 + x_1y_1 - x_1y_1 - x_0y_0 \\
&= (x_1 + x_0)y_0 + (x_0 + x_1)y_1 - x_1y_1 - x_0y_0 \\
&= (x_1 + x_0)(y_1 + y_0) - x_1y_1 - x_0y_0 \\
&= (x_1 + x_0)(y_1 + y_0) - z_2 - z_0.
\end{aligned}$$

Ejemplo

Con 12345 y 6789, tenemos a $B = 10$, $m = 3$. De $B^m = 10^3 = 1000$, se tiene

$$\begin{aligned}
12345 &= 12 \times 1000 + 345 \\
6789 &= 6 \times 1000 + 789
\end{aligned}$$

Luego, tenemos que

$$\begin{aligned}
z_2 &= 12 \times 6 = 72 \\
z_0 &= 345 \times 789 = 272205 \\
z_1 &= (12 + 345) \times (6 + 789) - z_1 - z_0 \\
&= 357 \times 795 - 72 - 272205 \\
&= 283815 - 72 - 272205 \\
&= 11538
\end{aligned}$$

Como m decrece conforme se agregan los resultados parciales descompuestos, el ejemplo anterior puede expresarse de forma que

$$\begin{aligned}
XY &= z_2(B^m)^2 + z_1(B^m)^1 + z_0 \\
XY &= 72 \times 1000^2 + 11538 \times 1000 + 272205 \\
&= 83810205
\end{aligned}$$

2.2. Recursivo

Sean X, Y dos números de n-dígitos, siendo n un múltiplo de 2.

Algoritmo de Karatsuba (recursivo)

```
1: procedure KARATSUBA(X,Y)
2:     if n = 1 then
3:         return P = XY
4:     else
5:         split X, Y in half:
6:         X = 10^(n/2) x_1 + x_2
7:         Y = 10^(n/2) y_1 + y_2
8:         U = KARATSUBA(x_1, y_1)
9:         V = KARATSUBA(x_2, y_2)
10:        W = KARATSUBA(x_1 - x_2, y_1 - y_2)
11:        Z = U + V - W
12:        P = 10^n U + 10^(n/2) Z + V
13:        return P
```

Y de la fórmula $a \times T(\frac{n}{c}) + b$, donde

a = cantidad de llamadas al caso recursivo,
c = cómo decrece la cardinalidad del problema,
b = sobrecarga (complejidad de lineas adicionales) se tiene

$$T(n) = 3T(\frac{n}{2}) + \mathcal{O}(n)$$

Como $\mathcal{O}(n)$ no determina el crecimiento del algoritmo, puede expresarse

que la complejidad del algoritmo de Karatsuba en su forma recursiva es de

$$T(n) = \mathcal{O}(n^{\log_2 3}) = \mathcal{O}(n^{1.58})$$

Sea $M(n)$ el número de multiplicaciones de un solo dígito que se necesitan para el algoritmo con 2 números de n-dígitos.
Hasta la línea 10, se producen tres llamadas recursivas, por lo tanto:

$$M(n) = 3M(\frac{n}{2})$$

Reemplazando $\frac{n}{2}$ en $M(n)$, se tiene

$$M(\frac{n}{2}) = 3M(\frac{n}{4})$$

entonces

$$M(n) = 9M(\frac{n}{4})$$

Continuando de manera similar, se tiene

$$M(n) = 27M(\frac{n}{8})$$

Por inducción se tiene que para cada $i(i <= k)$,

$$M(n) = 3^i M(\frac{n}{2^i})$$

Haciendo $i = k$,

$$\begin{aligned} M(n) &= 3^k M(\frac{n}{2^k}) \\ &= 3^k M(1) \\ &= 3^k \end{aligned}$$

Luego como $k = \log_2 n$, entonces

$$\begin{aligned} \log_2 M(n) = k, \\ M(n) &= 2^{\log_2 M(n)} \\ &= 2^{k \log_2 3} \\ &= (2^k)^{\log_2 3} \\ &= n^{\log_2 3} \end{aligned}$$

3. Referencias

- Babai, L. Divide and Conquer: The Karatsuba–Ofman algorithm. Retrieved May 30, 2016, recuperado de http://people.cs.uchicago.edu/ laci/HANDOUTS/karatsuba.pdf
- Roughgarden, T. (2017). Algorithms illuminated (part 1): The basics. Soundlikeyourself Publishing.
- Wikipedia contributors. (2023, enero 31). Karatsuba algorithm. Wikipedia, The Free Encyclopedia, Recuperado de: https://en.wikipedia.org/w/index.php?title=Karatsuba_algorithm oldid=1136568213