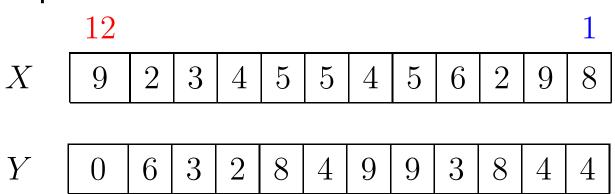
Multiplicação de inteiros gigantescos

n := número de algarismos.

Agradeço à Profa. Cristina Fernandes do IME-USP

Problema: Dados dois números inteiros X[1..n] e Y[1..n] calcular o produto $X \cdot Y$.

Entra: Exemplo com n = 12

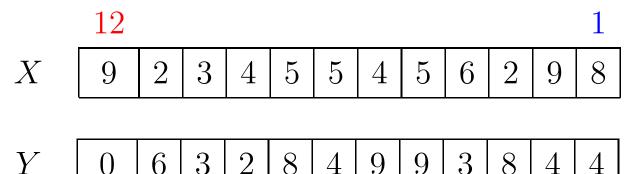


Multiplicação de inteiros gigantescos

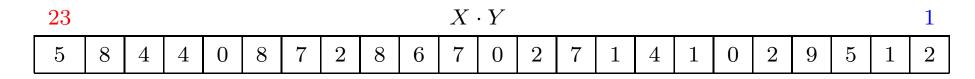
n := número de algarismos.

Problema: Dados dois números inteiros X[1..n] e Y[1..n] calcular o produto $X \cdot Y$.

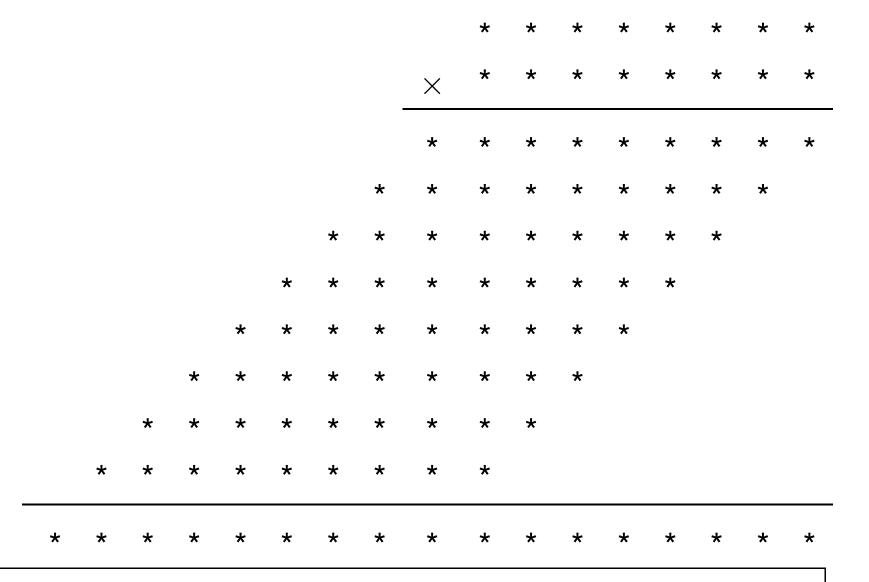
Entra: Exemplo com n = 12



Sai:

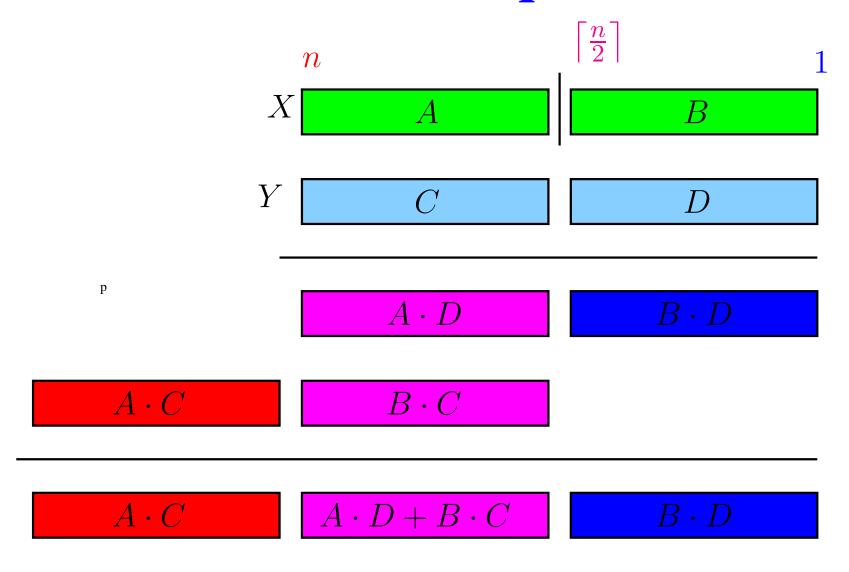


Algoritmo do ensino fundamental



O algoritmo do ensino fundamental é $\Theta(n^2)$.

Divisão e conquista



$$X \cdot Y = A \cdot C \times 10^n + (A \cdot D + B \cdot C) \times 10^{\lceil n/2 \rceil} + B \cdot D$$

 $A \ \boxed{3} \ \boxed{1} \quad B \ \boxed{4} \ \boxed{1} \quad C \ \boxed{5} \ \boxed{9} \quad D \ \boxed{3} \ \boxed{6}$

$$A \begin{bmatrix} 3 & 1 \end{bmatrix} \quad B \begin{bmatrix} 4 & 1 \end{bmatrix} \quad C \begin{bmatrix} 5 & 9 \end{bmatrix} \quad D \begin{bmatrix} 3 & 6 \end{bmatrix}$$

$$X \cdot Y = A \cdot C \times 10^4 + (A \cdot D + B \cdot C) \times 10^2 + B \cdot D$$

 $A \cdot C = 1829$ $(A \cdot D + B \cdot C) = 1116 + 2419 = 3535$
 $B \cdot D = 1476$

$$A \cdot C$$
 1 8 2 9 0 0 0 0 0 ($A \cdot D + B \cdot C$) 3 5 3 5 0 0 $A \cdot D$ 1 4 7 6 $A \cdot C$ 1 8 6 4 4 9 7 6

Algoritmo de Multi-DC

Algoritmo recebe inteiros X[1..n] e Y[1..n] e devolve $X \cdot Y$.

```
MULT(X,Y,n)
  1 se n=1 devolva X \cdot Y
 2 q \leftarrow \lceil n/2 \rceil
 3 A \leftarrow X[q+1..n] B \leftarrow X[1..q]
  4 C \leftarrow Y[q+1..n] D \leftarrow Y[1..q]
  5 E \leftarrow \text{MULT}(A, C, \lfloor n/2 \rfloor)
  6 F \leftarrow \mathsf{MULT}(B, D, \lceil n/2 \rceil)
     G \leftarrow \mathsf{MULT}(A, D, \lceil n/2 \rceil)
     H \leftarrow \mathsf{MULT}(B, C, \lceil n/2 \rceil)
       R \leftarrow E \times 10^n + (G + H) \times 10^{\lceil n/2 \rceil} + F
       devolva R
```

T(n) =consumo de tempo do algoritmo para multiplicar dois inteiros com n algarismos.

Consumo de tempo

```
todas as execuções da linha
linha
        = \Theta(1)
  2 = \Theta(1)
  3 = \Theta(n)
  \mathbf{4} = \Theta(n)
  5 = T(|n/2|)
  6 = T(\lceil n/2 \rceil)
  7 = T(\lceil n/2 \rceil)
  8 = T(\lceil n/2 \rceil)
  9 = \Theta(n)
 10
     = \Theta(n)
total = T(\lfloor n/2 \rfloor) + 3T(\lceil n/2 \rceil) + \Theta(n)
```

Consumo de tempo

Sabemos que

$$T(1) = \Theta(1)$$

$$T(n) = T(\lfloor n/2 \rfloor) + 3T(\lceil n/2 \rceil) + \Theta(n) \quad \text{para } n = 2, 3, 4, \dots$$

está na mesma classe ⊖ que a solução de

$$T'(n) = 4T'(n/2) + \frac{n}{n}$$

n	1	2	4	8	16	32	64	128	256	512
T'(n)	1	6	28	120	496	2016	8128	32640	130816	523776

Conclusões

$$T'(n) \notin \Theta(n^2)$$
.

$$T(n)$$
 é $\Theta(n^2)$.

O consumo de tempo do algoritmo MULT é $\Theta(n^2)$.

Tanto trabalho por nada ... Será?!?

Olhar para números com 2 algarismos (n=2).

Suponha $X=a\,b$ e $Y=c\,d$. Se cada multiplicação custa R\$ 1,00 e cada soma custa R\$ 0,01, quanto custa $X\cdot Y$?

Olhar para números com 2 algarismos (n=2).

Suponha X = ab e Y = cd.

Se cada multiplicação custa R\$ 1,00 e cada soma custa R\$ 0,01, quanto custa $X \cdot Y$?

Eis $X \cdot Y$ por R\$ 4,03:

$$X \cdot Y = ac \times 10^2 + (ad + bc) \times 10^1 + bd$$

Olhar para números com 2 algarismos (n=2).

Suponha X = ab e Y = cd.

Se cada multiplicação custa R\$ 1,00 e cada soma custa R\$ 0,01, quanto custa $X \cdot Y$?

Eis $X \cdot Y$ por R\$ 4,03:

$$X \cdot Y = ac \times 10^2 + (ad + bc) \times 10^1 + bd$$

Solução mais barata?

Olhar para números com 2 algarismos (n=2).

Suponha X = ab e Y = cd.

Se cada multiplicação custa R\$ 1,00 e cada soma custa R\$ 0,01, quanto custa $X \cdot Y$?

Eis $X \cdot Y$ por R\$ 4,03:

$$X \cdot Y = ac \times 10^2 + (ad + bc) \times 10^1 + bd$$

Solução mais barata?

Gauss faz por R\$ 3,06!

$X \cdot Y$ por apenas R\$ 3,06

X		a	b
Y		c	d
		ad	bd
	ac	bc	
$\overline{X \cdot Y}$	ac	ad + bc	\overline{bd}

$X \cdot Y$ por apenas R\$ 3,06

$$(a+b)(c+d) = \frac{ac}{ad} + \frac{bc}{bc} + \frac{bd}{bd} \Rightarrow$$
$$\frac{ad}{bc} = (a+b)(c+d) - \frac{ac}{bd} - \frac{bd}{bd}$$

$$g = (a+b)(c+d)$$
 $e = ac$ $f = bd$ $h = g - e - f$

$$X \cdot Y$$
 (por R\$ 3,06) = $e \times 10^2 + h \times 10^1 + f$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$ $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 21$$
 $Y = 23$ $X \cdot Y = ?$ $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 21$$
 $Y = 23$ $X \cdot Y = ?$
 $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 2 \quad Y = 2 \quad X \cdot Y = 4$$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 21$$
 $Y = 23$ $X \cdot Y = ?$ $ac = 4$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 21$$
 $Y = 23$ $X \cdot Y = ?$
 $ac = 4$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 1 \quad Y = 3 \quad X \cdot Y = 3$$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 21$$
 $Y = 23$ $X \cdot Y = ?$
 $ac = 4$ $bd = 3$ $(a+b)(c+d) = ?$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 21$$
 $Y = 23$ $X \cdot Y = ?$
 $ac = 4$ $bd = 3$ $(a+b)(c+d) = ?$

$$X = 3 \quad Y = 5 \quad X \cdot Y = 15$$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$ $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 21$$
 $Y = 23$ $X \cdot Y = 483$
 $ac = 4$ $bd = 3$ $(a+b)(c+d) = 15$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = 483$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = 483$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 33$$
 $Y = 12$ $X \cdot Y = ?$
 $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = 483$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 33$$
 $Y = 12$ $X \cdot Y = 396$
 $ac = 3$ $bd = 6$ $(a+b)(c+d) = 18$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = 483$ $bd = 396$ $(a+b)(c+d) = ?$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = 483$ $bd = 396$ $(a+b)(c+d) = ?$

$$X = 54$$
 $Y = 35$ $X \cdot Y = ?$
 $ac = ?$ $bd = ?$ $(a+b)(c+d) = ?$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = 483$ $bd = 396$ $(a+b)(c+d) = ?$

$$X = 54$$
 $Y = 35$ $X \cdot Y = 1890$
 $ac = 15$ $bd = 20$ $(a+b)(c+d) = 72$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = ?$
 $ac = 483$ $bd = 396$ $(a+b)(c+d) = 1890$

$$X = 2133$$
 $Y = 2312$ $X \cdot Y = 4931496$
 $ac = 483$ $bd = 396$ $(a+b)(c+d) = 1890$

Algoritmo Multi

Algoritmo recebe inteiros X[1...n] e Y[1...n] e devolve $X \cdot Y$ (Karatsuba e Ofman).

```
KARATSUBA (X, Y, n)
 1 se n \leq 3 devolva X \cdot Y
 2 q \leftarrow \lceil n/2 \rceil
 3 A \leftarrow X[q+1..n] B \leftarrow X[1..q]
 4 C \leftarrow Y[q+1..n] D \leftarrow Y[1..q]
 5 E \leftarrow \mathsf{KARATSUBA}(A, C, \lfloor n/2 \rfloor)
 6 F \leftarrow \mathsf{KARATSUBA}(B, D, \lceil n/2 \rceil)
     G \leftarrow \mathsf{KARATSUBA}(A+B,C+D,\lceil n/2 \rceil + 1)
 8 H \leftarrow G - F - E
 9 R \leftarrow E \times 10^n + H \times 10^{\lceil n/2 \rceil} + F
10 devolva R
```

T(n) = consumo de tempo do algoritmo para multiplicar dois inteiros com n algarismos.

Consumo de tempo

```
todas as execuções da linha
        = \Theta(1)
    = \Theta(1)
 3 = \Theta(n)
 \mathbf{4} = \Theta(n)
 5 = T(|n/2|)
 6 = T(\lceil n/2 \rceil)
 7 = T(\lceil n/2 \rceil + 1)
 8 = \Theta(n)
     = \Theta(n)
 10 = \Theta(n)
total = T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + T(\lceil n/2 \rceil + 1) + \Theta(n)
```

Consumo de tempo

Sabemos que

$$\begin{array}{lcl} T(n) &=& \Theta(1) & \mathsf{para} \; n = 1, 2, 3 \\ T(n) &=& T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + T(\lceil n/2 \rceil + 1) + \Theta(n) & n \geq 4 \end{array}$$

está na mesma classe ⊖ que a solução de

$$T'(n) = 3T'(n/2) + n$$

Conclusões

$$T'(n) \notin \Theta(n^{\lg 3}).$$

Logo
$$T(n)$$
 é $\Theta(n^{\lg 3})$.

O consumo de tempo do algoritmo KARATSUBA é $\Theta(n^{\lg 3})$ (1,584 < $\lg 3$ < 1,585).

Mais conclusões

Consumo de tempo de algoritmos para multiplicação de inteiros:

Jardim de infância $\Theta(n \, 10^n)$

Ensino fundamental $\Theta(n^2)$

Karatsuba e Ofman'60 $O(n^{1.585})$

Toom e Cook'63 $O(n^{1.465})$

(divisão e conquista; generaliza o acima)

Schönhage e Strassen'71 $O(n \lg n \lg \lg n)$

(FFT em aneis de tamanho específico)

Fürer'07 $O(n \lg n 2^{O(\log^* n)})$

Ambiente experimental

A plataforma utilizada nos experimentos é um PC rodando Linux Debian ?.? com um processador Pentium II de 233 MHz e 128MB de memória RAM.

Os códigos estão compilados com o gcc versão 2.7.2.1 e opção de compilação -O2.

As implementações comparadas neste experimento são as do algoritmo do ensino fundamental e do algoritmo KARATSUBA.

O programa foi escrito por Carl Burch:

http://www-2.cs.cmu.edu/~cburch/251/karat/.

Resultados experimentais

n	Ensino Fund.	KARATSUBA
4	0.005662	0.005815
8	0.010141	0.010600
16	0.020406	0.023643
32	0.051744	0.060335
64	0.155788	0.165563
128	0.532198	0.470810
256	1.941748	1.369863
512	7.352941	4.032258

Tempos em 10^3 segundos.

Multiplicação de matrizes

Problema: Dadas duas matrizes X[1..n,1..n] e Y[1..n,1..n] calcular o produto $X \cdot Y$.

O algoritmo tradicional de multiplicação de matrizes consome tempo $\Theta(n^3)$.

$$\left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \times \left(\begin{array}{cc} e & f \\ g & h \end{array}\right) = \left(\begin{array}{cc} r & s \\ t & u \end{array}\right)$$

$$r = ae + bg$$

$$s = af + bh$$

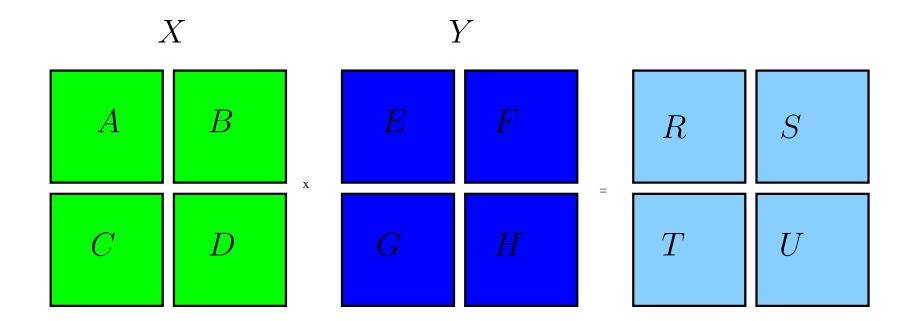
$$t = ce + dg$$

$$u = cf + dh$$

Solução custa R\$ 8,04

(1)

Divisão e conquista



$$R = AE + BG$$
$$S = AF + BH$$

$$T = CE + DG$$

$$U = CF + DH$$

2)

Algoritmo de Multi-Mat

Algoritmo recebe inteiros X[1 ... n] e Y[1 ... n] e devolve $X \cdot Y$.

```
MULTI-M(X,Y,n)
      se n=1 devolva X \cdot Y
    (A, B, C, D) \leftarrow \mathsf{PARTICIONE}(X, n)
    (E, F, G, H) \leftarrow \mathsf{PARTICIONE}(Y, n)
      R \leftarrow \text{MULTI-M}(A, E, n/2) + \text{MULTI-M}(B, G, n/2)
    S \leftarrow \mathsf{MULTI-M}(A, F, n/2) + \mathsf{MULTI-M}(B, H, n/2)
     T \leftarrow \mathsf{MULTI-M}(C, E, n/2) + \mathsf{MULTI-M}(D, G, n/2)
      U \leftarrow \mathsf{MULTI-M}(C, F, n/2) + \mathsf{MULTI-M}(D, H, n/2)
      P \leftarrow \mathsf{CONSTROI\text{-}MAT}(R, S, T, U)
      devolva P
```

T(n) = consumo de tempo do algoritmo para multiplicar duas matrizes de n linhas e n colunas.

linha todas as execuções da linha

1 =
$$\Theta(1)$$

2 = $\Theta(n^2)$
3 = $\Theta(n^2)$
4 = $T(n/2) + T(n/2)$
5 = $T(n/2) + T(n/2)$
6 = $T(n/2) + T(n/2)$
7 = $T(n/2) + T(n/2)$
8 = $\Theta(n^2)$
9 = $\Theta(n^2)$

total =
$$8T(n/2) + \Theta(n^2)$$

As dicas no nosso estudo de recorrências sugere que a solução da recorrência

$$T(1) = \Theta(1)$$

$$T(n) = 8T(n/2) + \Theta(n^2) \quad \text{para } n = 2, 3, 4, \dots$$

está na mesma classe ⊖ que a solução de

$$T'(n) = 8T'(n/2) + \frac{n^2}{n^2}$$

γ	\imath	1	2	4	8	16	32	64	128	256
T'	$\overline{(n)}$	1	12	112	960	7936	64512	520192	4177920	3348889

Conclusões

$$T'(n) \notin \Theta(n^3)$$
.

Logo
$$T(n)$$
 é $\Theta(n^3)$.

O consumo de tempo do algoritmo MULTI-M é $\Theta(n^3)$.

Strassen: $X \cdot Y$ por apenas R\$ 7,18

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

Strassen: $X \cdot Y$ por apenas R\$ 7,18

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

$$p_1 = a(f - h) = af - ah$$

$$p_2 = (a + b)h = ah + bh$$

$$p_3 = (c + d)e = ce + de$$

$$p_4 = d(g - e) = dg - de$$

$$p_5 = (a + d)(e + h) = ae + ah + de + dh$$

 $p_6 = (b-d)(g+h) = bg + bh - dg - dh$

$$p_7 = (a - c)(e + f) = ae + af - ce - cf$$

Strassen: $X \cdot Y$ por apenas R\$ 7,18

$$p_1 = a(f - h) = af - ah$$

 $p_2 = (a + b)h = ah + bh$
 $p_3 = (c + d)e = ce + de$
 $p_4 = d(g - e) = dg - de$
 $p_5 = (a + d)(e + h) = ae + ah + de + dh$
 $p_6 = (b - d)(g + h) = bg + bh - dg - dh$
 $p_7 = (a - c)(e + f) = ae + af - ce - cfd$

$$r = p_5 + p_4 - p_2 + p_6 = ae + bg$$

$$s = p_1 + p_2 = af + bh$$

$$t = p_3 + p_4 = ce + dg$$

$$u = p_5 + p_1 - p_3 - p_7 = cf + dh$$

Algoritmo de Strassen

```
STRASSEN (X, Y, n)
     se n=1 devolva X \cdot Y
 2 (A, B, C, D) \leftarrow \mathsf{PARTICIONE}(X, n)
 3 (E, F, G, H) \leftarrow \mathsf{PARTICIONE}(Y, n)
 4 P_1 \leftarrow \mathsf{STRASSEN}(A, F - H, n/2)
 5 P_2 \leftarrow \mathsf{STRASSEN}(A+B,H,n/2)
 6 P_3 \leftarrow \mathsf{STRASSEN}(C+D, E, n/2)
 7 P_4 \leftarrow \mathsf{STRASSEN}(D, G - E, n/2)
 8 P_5 \leftarrow \mathsf{STRASSEN}(A+D,E+H,n/2)
    P_6 \leftarrow \mathsf{STRASSEN}(B-D,G+H,n/2)
10 P_7 \leftarrow \text{STRASSEN}(A-C, E+F, n/2)
11 R \leftarrow P_5 + P_4 - P_2 + P_6
12 S \leftarrow P_1 + P_2
13 T \leftarrow P_3 + P_4
14 U \leftarrow P_5 + P_1 - P_3 - P_7
15 devolva P \leftarrow \text{CONSTROI-MAT}(R, S, T, U)
```

linha	todas as execuções da linha			
1	=	$\Theta(1)$		
2-3	=	$\Theta(n^2)$		
4-10	=	$7, T(n/2) + \Theta(n^2)$		
11-14	=	$\Theta(n^2)$		
15	=	$\Theta(n^2)$		

total = $7T(n/2) + \Theta(n^2)$

As dicas no nosso estudo de recorrências sugere que a solução da recorrência

$$T(1) = \Theta(1)$$

$$T(n) = 7T(n/2) + \Theta(n^2) \quad \text{para } n = 2, 3, 4, \dots$$

está na mesma classe ⊖ que a solução de

$$T'(n) = 7T'(n/2) + n^2$$

	n	1	2	4	8	16	32	64	128	256
•	T'(n)	1	11	93	715	5261	37851	269053	1899755	13363821

Conclusões

$$T'(n) \notin \Theta(n^{\lg 7}).$$

Logo
$$T(n)$$
 é $\Theta(n^{\lg 7})$.

O consumo de tempo do algoritmo STRASSEN é $\Theta(n^{\lg 7})$ (2,80 < $\lg 7 <$ 2,81).

Mais conclusões

Consumo de tempo de algoritmos para multiplicação de matrizes:

Ensino fundamental	$\Theta(n^3)$
Strassen (1969)	$\mathcal{O}(n^{2.807})$
	:
Coppersmith e Winograd (1987)	$O(n^{2.3755})$
Stothers (2010)	$\mathcal{O}(n^{2.3736})$
Williams (2011)	$O(n^{2.3728642})$
Le Gall (2014)	$O(n^{2.3728639})$