

Multiplicação de inteiros gigantesco

KT cap 5.5

Multiplicação de inteiros gigantesco

n := número de algarismos.

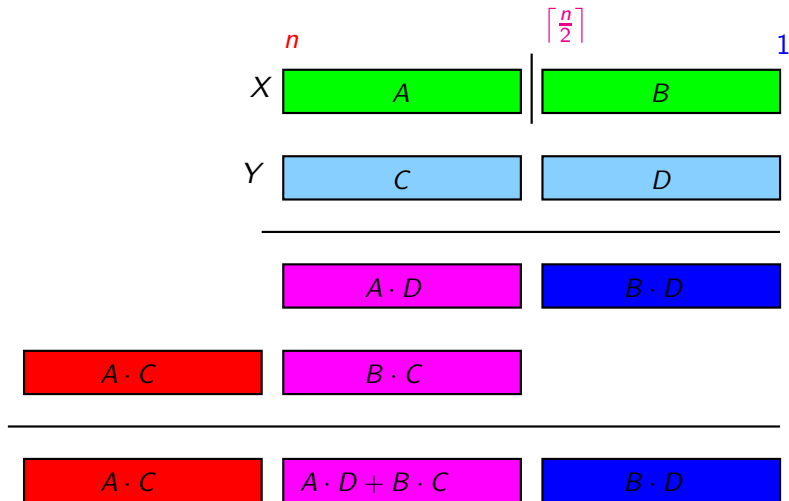
Problema: Dados dois números inteiros $X[1..n]$ e $Y[1..n]$, calcular o **produto** $X \cdot Y$.

Exemplo com $n = 12$.

Entra:

		12										1
X	9	2	3	4	5	5	4	5	6	2	9	8
Y	0	6	3	2	8	4	9	9	3	8	4	4

Divisão e conquista



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

Exemplo

X

	4		1	
3	1	4	1	

Y

	4		1	
5	9	3	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  $F \leftarrow \text{MULT}(B, D, \lceil n/2 \rceil)$ 
7  $G \leftarrow \text{MULT}(A, D, \lceil n/2 \rceil)$ 
8  $H \leftarrow \text{MULT}(B, C, \lceil n/2 \rceil)$ 
9  $R \leftarrow E \times 10^n + (G + H) \times 10^{\lceil n/2 \rceil} + F$ 
10 devolva  $R$ 
```

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

Consumo de tempo

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

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 Θ** que a solução de

$$T'(n) = 4T'(n/2) + n$$

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

Conclusões

$$T'(n) \text{ é } \Theta(n^2).$$

$$T(n) \text{ é } \Theta(n^2).$$

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

Tanto trabalho por nada ...
Será?!?

Pensar pequeno

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 $X \cdot Y$?

Pensar pequeno

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:

$$\begin{array}{r} X \qquad \qquad a \qquad b \\ Y \qquad \qquad c \qquad d \\ \hline \qquad \qquad \qquad ad \qquad bd \\ \qquad \qquad \qquad \qquad \qquad \qquad \\ \qquad \qquad \qquad ac \qquad bc \\ \hline X \cdot Y \quad ac \quad ad + bc \quad bd \end{array}$$

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

Pensar pequeno

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:

$$\begin{array}{r} X \qquad \qquad a \qquad b \\ Y \qquad \qquad c \qquad d \\ \hline \qquad \qquad \qquad ad \qquad bd \\ \qquad \qquad ac \qquad bc \\ \hline X \cdot Y \quad ac \quad ad + bc \quad bd \end{array}$$

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

Solução mais barata?

Pensar pequeno

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:

$$\begin{array}{r} X \qquad \qquad a \qquad b \\ Y \qquad \qquad c \qquad d \\ \hline \qquad \qquad \qquad ad \qquad bd \\ \qquad \qquad \qquad \qquad \qquad \qquad \\ \qquad \qquad \qquad \qquad \qquad \qquad \\ \qquad \qquad \qquad \qquad \qquad \qquad \\ \hline X \cdot Y \quad ac \quad ad + bc \quad bd \end{array}$$

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

Solução mais barata? Gauss faz por R\$ 3,06!

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

$$\begin{array}{r} X \qquad \qquad a \qquad b \\ Y \qquad \qquad c \qquad d \\ \hline \qquad \qquad \qquad ad \qquad bd \\ \qquad \qquad ac \qquad bc \\ \hline X \cdot Y \quad ac \quad ad + bc \quad bd \end{array}$$

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

$$\begin{array}{r} X \qquad \qquad a \qquad b \\ Y \qquad \qquad c \qquad d \\ \hline \qquad \qquad \qquad ad \qquad bd \\ \qquad \qquad ac \qquad bc \\ \hline X \cdot Y \quad ac \quad ad + bc \quad bd \end{array}$$

$$(a + b)(c + d) = ac + ad + bc + bd \Rightarrow$$

$$ad + bc = (a + b)(c + d) - ac - bd$$

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

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

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & ? & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & ? & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

$$\begin{array}{llll} X = & 21 & Y = & 23 & X \cdot Y = & ? \\ ac = & ? & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

Exemplo

$$\begin{array}{lll} X = 2133 & Y = 2312 & X \cdot Y = ? \\ ac = ? & bd = ? & (a+b)(c+d) = ? \end{array}$$

$$\begin{array}{lll} X = 21 & Y = 23 & X \cdot Y = ? \\ ac = ? & bd = ? & (a+b)(c+d) = ? \end{array}$$

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

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & ? & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

$$\begin{array}{llll} X = & 21 & Y = & 23 & X \cdot Y = & ? \\ ac = & 4 & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & ? & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

$$\begin{array}{llll} X = & 21 & Y = & 23 & X \cdot Y = & ? \\ ac = & 4 & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

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

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & ? & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

$$\begin{array}{llll} X = & 21 & Y = & 23 & X \cdot Y = & ? \\ ac = & 4 & bd = & 3 & (a + b)(c + d) = & ? \end{array}$$

Exemplo

$$\begin{array}{lll} X = 2133 & Y = 2312 & X \cdot Y = ? \\ ac = ? & bd = ? & (a+b)(c+d) = ? \end{array}$$

$$\begin{array}{lll} X = 21 & Y = 23 & X \cdot Y = ? \\ ac = 4 & bd = 3 & (a+b)(c+d) = ? \end{array}$$

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

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & ? & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

$$\begin{array}{llll} X = & 21 & Y = & 23 & X \cdot Y = & 483 \\ ac = & 4 & bd = & 3 & (a + b)(c + d) = & 15 \end{array}$$

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & 483 & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & 483 & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

$$\begin{array}{llll} X = & 33 & Y = & 12 & X \cdot Y = & ? \\ ac = & ? & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & 483 & bd = & ? & (a + b)(c + d) = & ? \end{array}$$

$$\begin{array}{llll} X = & 33 & Y = & 12 & X \cdot Y = & 396 \\ ac = & 3 & bd = & 6 & (a + b)(c + d) = & 18 \end{array}$$

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & 483 & bd = & 396 & (a + b)(c + d) = & ? \end{array}$$

Exemplo

$$\begin{aligned} X &= 2133 & Y &= 2312 & X \cdot Y &= ? \\ ac &= 483 & bd &= 396 & (a+b)(c+d) &= ? \end{aligned}$$

$$\begin{aligned} X &= 54 & Y &= 35 & X \cdot Y &= ? \\ ac &= ? & bd &= ? & (a+b)(c+d) &= ? \end{aligned}$$

Exemplo

$$\begin{array}{llll} X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & 483 & bd = & 396 & (a + b)(c + d) = & ? \end{array}$$

$$\begin{array}{llll} X = & 54 & Y = & 35 & X \cdot Y = & 1890 \\ ac = & 15 & bd = & 20 & (a + b)(c + d) = & 72 \end{array}$$

Exemplo

$$\begin{array}{l} X = 2133 \quad Y = 2312 \quad X \cdot Y = ? \\ ac = 483 \quad bd = 396 \quad (a + b)(c + d) = 1890 \end{array}$$

Exemplo

$$\begin{array}{l} X = 2133 \quad Y = 2312 \quad X \cdot Y = 4931496 \\ ac = 483 \quad bd = 396 \quad (a + b)(c + d) = 1890 \end{array}$$

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 $E \leftarrow \text{KARATSUBA}(A, C, \lfloor n/2 \rfloor)$
- 6 $F \leftarrow \text{KARATSUBA}(B, D, \lceil n/2 \rceil)$
- 7 $G \leftarrow \text{KARATSUBA}(A + B, C + D, \lceil n/2 \rceil + 1)$
- 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

linha	todas as execuções da linha
1	$= \Theta(1)$
2	$= \Theta(1)$
3	$= \Theta(n)$
4	$= \Theta(n)$
5	$= T(\lfloor n/2 \rfloor)$
6	$= T(\lceil n/2 \rceil)$
7	$= T(\lceil n/2 \rceil + 1)$
8	$= \Theta(n)$
9	$= \Theta(n)$
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

$$T(n) = \Theta(1) \quad \text{para } n = 1, 2, 3$$

$$T(n) = T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + T(\lceil n/2 \rceil + 1) + \Theta(n) \quad n \geq 4$$

está na mesma classe Θ que a solução de

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

n	1	2	4	8	16	32	64	128	256	512
$T'(n)$	1	5	19	65	211	665	2059	6305	19171	58025

Conclusões

$T'(n)$ é $\Theta(n^{\lg 3})$.

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 anéis de tamanho específico)

Fürer '07

$$O(n \lg n 2^{O(\log^* n)})$$

Harvey e van der Hoeven '20

$$O(n \log n)$$

(Gaussian resampling, multidimensional DFT,
Nussbaumer's fast polynomial transforms)

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 $\Theta(n^3)$.

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

$$r = ae + bg$$

$$s = af + bh$$

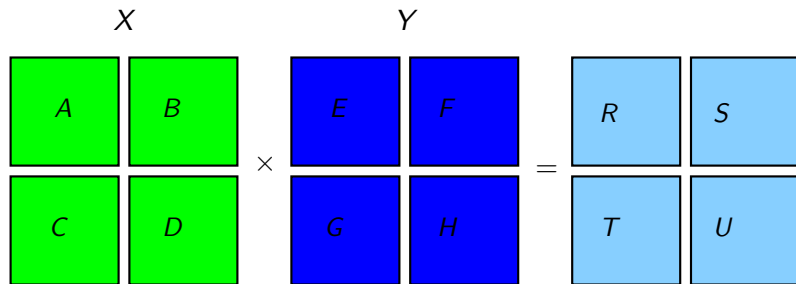
$$t = ce + dg$$

$$u = cf + dh$$

(1)

Solução custa R\$ 8,04

Divisão e conquista



$$R = AE + BG$$

$$S = AF + BH$$

$$T = CE + DG$$

$$U = CF + DH$$

Algoritmo de Multi-Mat

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

MULTI-M (X, Y, n)

- 1 se $n = 1$ devolva $X \cdot Y$
- 2 $(A, B, C, D) \leftarrow \text{PARTICIONE}(X, n)$
- 3 $(E, F, G, H) \leftarrow \text{PARTICIONE}(Y, n)$
- 4 $R \leftarrow \text{MULTI-M}(A, E, n/2) + \text{MULTI-M}(B, G, n/2)$
- 5 $S \leftarrow \text{MULTI-M}(A, F, n/2) + \text{MULTI-M}(B, H, n/2)$
- 6 $T \leftarrow \text{MULTI-M}(C, E, n/2) + \text{MULTI-M}(D, G, n/2)$
- 7 $U \leftarrow \text{MULTI-M}(C, F, n/2) + \text{MULTI-M}(D, H, n/2)$
- 8 $P \leftarrow \text{CONSTRÓI-MAT}(R, S, T, U)$
- 9 devolva P

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

Consumo de tempo

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

Consumo de tempo

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

$$\begin{aligned}T(1) &= \Theta(1) \\T(n) &= 8 T(n/2) + \Theta(n^2) \quad \text{para } n = 2, 3, 4, \dots\end{aligned}$$

está na **mesma classe Θ** que a solução de

$$T'(n) = 8T'(n/2) + n^2$$

n	1	2	4	8	16	32	64	128	256
$T'(n)$	1	12	112	960	7936	64512	520192	4177920	33488896

Conclusões

$T'(n)$ é $\Theta(n^3)$.

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

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

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

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

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

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

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

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

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

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

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

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

Algoritmo de Strassen

STRASSEN (X, Y, n)

- 1 se $n = 1$ devolva $X \cdot Y$
- 2 $(A, B, C, D) \leftarrow$ PARTICIONE(X, n)
- 3 $(E, F, G, H) \leftarrow$ PARTICIONE(Y, n)
- 4 $P_1 \leftarrow$ STRASSEN($A, F - H, n/2$)
- 5 $P_2 \leftarrow$ STRASSEN($A + B, H, n/2$)
- 6 $P_3 \leftarrow$ STRASSEN($C + D, E, n/2$)
- 7 $P_4 \leftarrow$ STRASSEN($D, G - E, n/2$)
- 8 $P_5 \leftarrow$ STRASSEN($A + D, E + H, n/2$)
- 9 $P_6 \leftarrow$ STRASSEN($B - D, G + H, n/2$)
- 10 $P_7 \leftarrow$ 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 $P \leftarrow$ CONSTRÓI-MAT(R, S, T, U)

Consumo de tempo

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

Consumo de tempo

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 Θ** 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

$T'(n)$ é $\Theta(n^{\lg 7})$.

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)	$O(n^{2.807})$
⋮	⋮
Coppersmith e Winograd (1987)	$O(n^{2.3755})$
Stothers (2010)	$O(n^{2.3736})$
Williams (2013)	$O(n^{2.3728642})$
Le Gall (2014)	$O(n^{2.3728639})$
Alman e Williams (2020)	$O(n^{2.3728596})$