Multiplicação de inteiros gigantescos

KT cap 5.5

Multiplicação de inteiros gigantescos

$n :=$ número de algarismos.

Problema: Dados dois números inteiros $X[1 \mathinner{.\,.} n]$ e $Y[1 \mathinner{.\,.} n]$, 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

Multiplicação de inteiros gigantescos

$n :=$ número de algarismos.

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

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

Sai:

$X \cdot Y$

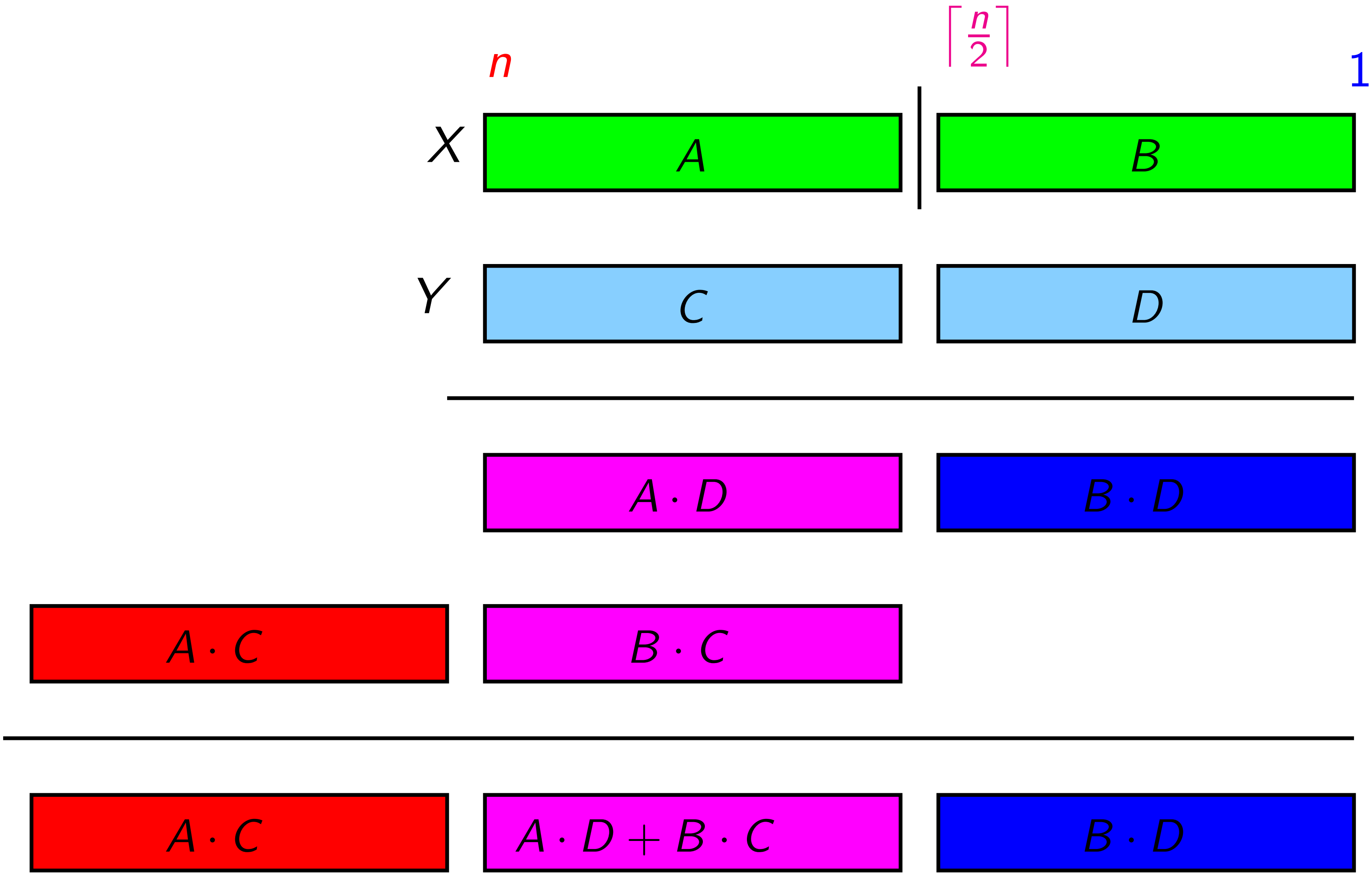
23																						1
5	8	4	4	0	8	7	2	8	6	7	0	2	7	1	4	1	0	2	9	5	1	2

Algoritmo do ensino fundamental

$$
\begin{array}{ccccccccccccccccc}
&&&&&&&&& \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
&&&&&&&& \times & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
\cline{9-17}
&&&&&&&& \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast \\
&&&&&&& \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \\
&&&&&& \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast && \\
&&&&& \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast &&& \\
&&&& \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast &&&& \\
&&& \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast &&&&& \\
&& \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast &&&&&& \\
& \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast &&&&&&& \\
\hline
\ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast & \ast
\end{array}
$$

$$\boxed{\text{O algoritmo do ensino fundamental é } \Theta(n^2).}$$

Divisão e conquista



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

Exemplo

	4			1
X	3	1	4	1

	4			1
Y	5	9	3	6

Exemplo

$$
\begin{array}{c|c|c|c|c|}
\multicolumn{1}{c}{} & \multicolumn{1}{c}{\color{red}{4}} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{\color{blue}{1}} \\
\cline{2-5}
X & 3 & 1 & 4 & 1 \\
\cline{2-5}
\end{array}
\qquad
\begin{array}{c|c|c|c|c|}
\multicolumn{1}{c}{} & \multicolumn{1}{c}{\color{red}{4}} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} & \multicolumn{1}{c}{\color{blue}{1}} \\
\cline{2-5}
Y & 5 & 9 & 3 & 6 \\
\cline{2-5}
\end{array}
$$

$$
\begin{array}{c|c|c|}
\cline{2-3}
A & 3 & 1 \\
\cline{2-3}
\end{array}
\qquad
\begin{array}{c|c|c|}
\cline{2-3}
B & 4 & 1 \\
\cline{2-3}
\end{array}
\qquad
\begin{array}{c|c|c|}
\cline{2-3}
C & 5 & 9 \\
\cline{2-3}
\end{array}
\qquad
\begin{array}{c|c|c|}
\cline{2-3}
D & 3 & 6 \\
\cline{2-3}
\end{array}
$$

Exemplo

$$\begin{array}{cc}
 & \color{red}{4} \quad\quad\quad \color{blue}{1} \\
X & \boxed{3}\boxed{1}\boxed{4}\boxed{1}
\end{array}
\qquad
\begin{array}{cc}
 & \color{red}{4} \quad\quad\quad \color{blue}{1} \\
Y & \boxed{5}\boxed{9}\boxed{3}\boxed{6}
\end{array}$$

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

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

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

$B \cdot D = 1476$

$$\begin{array}{lcccccccc}
A \cdot C & 1 & 8 & 2 & 9 & 0 & 0 & 0 & 0 \\
(A \cdot D + B \cdot C) & & & 3 & 5 & 3 & 5 & 0 & 0 \\
B \cdot D & & & & & 1 & 4 & 7 & 6 \\
\hline
X \cdot Y = & 1 & 8 & 6 & 4 & 4 & 9 & 7 & 6
\end{array}$$

Algoritmo de Multi-DC

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

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

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

Consumo de tempo

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

Nosso estudo de recorrências sugere que a solução da recorrência

$$\begin{aligned} T(1) &= \Theta(1) \\ T(n) &= T(\lfloor n/2 \rfloor) + 3\,T(\lceil n/2 \rceil) + \Theta(n) \quad \text{para } n = 2, 3, 4, \ldots \end{aligned}$$

está na mesma classe Θ que a solução de

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

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 $X = a\,b$ e $Y = c\,d$.

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

Pensar pequeno

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 $X \cdot Y$?

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

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

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

Pensar pequeno

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

Suponha $X = a\,b$ e $Y = c\,d$.

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

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

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

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

Solução mais barata?

Pensar pequeno

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

Suponha $X = a\,b$ e $Y = c\,d$.

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

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

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

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

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

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

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

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

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

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

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

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

Exemplo

$$X = \overbrace{\underline{21}}^{a}\overbrace{\underline{33}}^{b} \qquad Y = \overbrace{\underline{23}}^{c}\overbrace{\underline{12}}^{d} \qquad X \cdot Y = \ ?$$

$$ac = \ ? \qquad bd = \ ? \qquad (a+b)(c+d) = \ ?$$

Exemplo

$$X = \overset{a}{\overline{21}}\overset{b}{\overline{33}} \qquad Y = \overset{c}{\overline{23}}\overset{d}{\overline{12}} \qquad X \cdot Y = \;?$$

$$ac = \;? \qquad bd = \;? \qquad (a+b)(c+d) = \;?$$

Exemplo

$$X = \overset{a}{\underline{21}}\overset{b}{\underline{33}} \quad Y = \overset{c}{\underline{23}}\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$\boxed{ac} = \ ? \quad bd = \ ? \qquad (a+b)(c+d) = \ ?$$

$$X = 21 \quad Y = 23 \qquad X \cdot Y = \ ?$$

$$ac = \ ? \quad bd = \ ? \qquad (a+b)(c+d) = \ ?$$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \;?$$

$$\boxed{ac =} \;? \qquad bd = \;? \qquad (a+b)(c+d) = \;?$$

$$X = \overset{a}{\underline{2}}\,\overset{b}{\underline{1}} \qquad Y = \overset{c}{\underline{2}}\,\overset{d}{\underline{3}} \qquad X \cdot Y = \;?$$

$$ac = \;? \qquad bd = \;? \qquad (a+b)(c+d) = \;?$$

Exemplo

$$
\begin{aligned}
X &= \overset{a}{\overline{21}}\,\overset{b}{\overline{33}} & Y &= \overset{c}{\overline{23}}\,\overset{d}{\overline{12}} & X \cdot Y &= ? \\
\boxed{ac} &= ? & bd &= ? & (a+b)(c+d) &= ?
\end{aligned}
$$

$$
\begin{aligned}
X &= \overset{a}{\overline{2}}\,\overset{b}{\overline{1}} & Y &= \overset{c}{\overline{2}}\,\overset{d}{\overline{3}} & X \cdot Y &= ? \\
ac &= ? & bd &= ? & (a+b)(c+d) &= ?
\end{aligned}
$$

Exemplo

$$X = \overset{a}{21}\overset{b}{33} \quad Y = \overset{c}{23}\overset{d}{12} \qquad X \cdot Y = \ ?$$

$$\boxed{ac =} \ ? \quad bd = \ ? \qquad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{2}\overset{b}{1} \quad Y = \overset{c}{2}\overset{d}{3} \qquad X \cdot Y = \ ?$$

$$\boxed{ac =} \ ? \quad bd = \ ? \qquad (a+b)(c+d) = \ ?$$

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

Exemplo

$$X = \underbrace{\underset{a}{21}}\underset{b}{33} \quad Y = \underset{c}{23}\underset{d}{12} \qquad X \cdot Y = ?$$

$$\boxed{ac =} \; ? \quad bd = ? \qquad (a+b)(c+d) = ?$$

$$X = \underset{a}{2}\underset{b}{1} \quad Y = \underset{c}{2}\underset{d}{3} \qquad X \cdot Y = ?$$

$$\boxed{ac =} \; ? \quad bd = ? \qquad (a+b)(c+d) = ?$$

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

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \; ?$$

$$\boxed{ac =} \; ? \qquad bd = \; ? \qquad (a+b)(c+d) = \; ?$$

$$X = \overset{a}{\underline{2}}\,\overset{b}{\underline{1}} \qquad Y = \overset{c}{\underline{2}}\,\overset{d}{\underline{3}} \qquad X \cdot Y = \; ?$$

$$ac = 4 \qquad bd = \; ? \qquad (a+b)(c+d) = \; ?$$

Exemplo

$$X = \overset{a}{21}\overset{b}{33} \quad Y = \overset{c}{23}\overset{d}{12} \quad X \cdot Y = ?$$

$$\boxed{ac =} \; ? \quad bd = \; ? \quad (a+b)(c+d) = \; ?$$

$$X = \overset{a}{2}\overset{b}{1} \quad Y = \overset{c}{2}\overset{d}{3} \quad X \cdot Y = ?$$

$$ac = 4 \quad bd = \; ? \quad (a+b)(c+d) = \; ?$$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \quad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \; ?$$

$$\boxed{ac =} \; ? \quad bd = \; ? \qquad (a+b)(c+d) = \; ?$$

$$X = \overset{a}{\underline{2}}\,\overset{b}{\underline{1}} \quad Y = \overset{c}{\underline{2}}\,\overset{d}{\underline{3}} \qquad X \cdot Y = \; ?$$

$$ac = \; 4 \quad \boxed{bd =} \; ? \qquad (a+b)(c+d) = \; ?$$

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

Exemplo

$$X = \overset{a}{\underline{21}}\overset{b}{\underline{33}} \quad Y = \overset{c}{\underline{23}}\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$\boxed{ac} = \ ? \quad bd = \ ? \qquad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{\underline{2}}\overset{b}{\underline{1}} \quad Y = \overset{c}{\underline{2}}\overset{d}{\underline{3}} \qquad X \cdot Y = \ ?$$

$$ac = \ 4 \quad \boxed{bd} = \ ? \qquad (a+b)(c+d) = \ ?$$

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

Exemplo

$$X = \overset{a}{\overline{21}}\,\overset{b}{\overline{33}} \qquad Y = \overset{c}{\overline{23}}\,\overset{d}{\overline{12}} \qquad X \cdot Y = \;?$$

$$\boxed{ac =} \;? \qquad bd = \;? \qquad (a+b)(c+d) = \;?$$

$$X = \overset{a}{\overline{2}}\,\overset{b}{\overline{1}} \qquad Y = \overset{c}{\overline{2}}\,\overset{d}{\overline{3}} \qquad X \cdot Y = \;?$$

$$ac = 4 \qquad bd = 3 \qquad (a+b)(c+d) = \;?$$

Exemplo

$$X = \overset{a}{\overline{21}}\,\overset{b}{\overline{33}} \qquad Y = \overset{c}{\overline{23}}\,\overset{d}{\overline{12}} \qquad X \cdot Y = ?$$

$$\boxed{ac} = ? \qquad bd = ? \qquad (a+b)(c+d) = ?$$

$$X = \overset{a}{\overline{2}}\,\overset{b}{\overline{1}} \qquad Y = \overset{c}{\overline{2}}\,\overset{d}{\overline{3}} \qquad X \cdot Y = ?$$

$$ac = 4 \qquad bd = 3 \qquad \underbrace{(a+b)}_{3}\underbrace{(c+d)}_{5} = ?$$

Exemplo

$$X = \overset{a}{21}\overset{b}{33} \qquad Y = \overset{c}{23}\overset{d}{12} \qquad X \cdot Y = \ ?$$

$$\boxed{ac =} \ ? \qquad bd = \ ? \qquad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{2}\overset{b}{1} \qquad Y = \overset{c}{2}\overset{d}{3} \qquad X \cdot Y = \ ?$$

$$ac = 4 \qquad bd = 3 \qquad \boxed{\underbrace{(a+b)}_{3}\underbrace{(c+d)}_{5}} = \ ?$$

$$X = 3 \qquad Y = 5 \qquad X \cdot Y =$$

Exemplo

$$X = \overset{a}{21}\overset{b}{33} \quad Y = \overset{c}{23}\overset{d}{12} \qquad X \cdot Y = \; ?$$

$$\boxed{ac = } \; ? \qquad bd = \; ? \qquad (a+b)(c+d) = \; ?$$

$$X = \overset{a}{2}\overset{b}{1} \quad Y = \overset{c}{2}\overset{d}{3} \qquad X \cdot Y = \; ?$$

$$ac = \; 4 \qquad bd = \; 3 \qquad \boxed{\underbrace{(a+b)}_{3}\underbrace{(c+d)}_{5}} = \; ?$$

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

Exemplo

$$X = \overset{a}{\underline{21}}\overset{b}{\underline{33}} \quad Y = \overset{c}{\underline{23}}\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$\boxed{{\color{red}ac} =} \ ? \quad {\color{blue}bd} = \ ? \qquad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{\underline{2}}\overset{b}{\underline{1}} \quad Y = \overset{c}{\underline{2}}\overset{d}{\underline{3}} \qquad X \cdot Y =$$

$${\color{red}ac} = 4 \quad {\color{blue}bd} = 3 \qquad (a+b)(c+d) = 15$$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$\boxed{ac =}\ ? \qquad bd = \ ? \qquad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{\underline{2}}\,\overset{b}{\underline{1}} \qquad Y = \overset{c}{\underline{2}}\,\overset{d}{\underline{3}} \qquad X \cdot Y = 483$$

$$ac = 4 \qquad bd = 3 \qquad (a+b)(c+d) = 15$$

$15 - 4 - 3 = 8$

Exemplo

$$X = \underbrace{21}_{a}\underbrace{33}_{b} \quad Y = \underbrace{23}_{c}\underbrace{12}_{d} \quad X \cdot Y = \ ?$$

$$\boxed{ac =} \ ? \quad bd = \ ? \quad (a+b)(c+d) = \ ?$$

$$X = 21 \quad Y = 23 \quad X \cdot Y = 483$$

$$ac = 4 \quad bd = 3 \quad (a+b)(c+d) = 15$$

Exemplo

$$X = \overset{a}{\underline{21}}\overset{b}{\underline{33}} \quad Y = \overset{c}{\underline{23}}\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$ac = 483 \quad bd = \ ? \qquad (a+b)(c+d) = \ ?$$

Exemplo

$$X = \overbrace{21}^{a}\overbrace{33}^{b} \quad Y = \overbrace{23}^{c}\overbrace{12}^{d} \qquad X \cdot Y = ?$$

$$ac = 483 \quad bd = ? \qquad (a+b)(c+d) = ?$$

Exemplo

$$X = \overbrace{21}^{a}\overbrace{33}^{b} \qquad Y = \overbrace{23}^{c}\overbrace{12}^{d} \qquad X \cdot Y = ?$$

$$ac = 483 \qquad \boxed{bd} = ? \qquad (a+b)(c+d) = ?$$

$$X = 33 \qquad Y = 12 \qquad X \cdot Y = ?$$

$$ac = ? \qquad bd = ? \qquad (a+b)(c+d) = ?$$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$ac = 483 \qquad \boxed{bd} = \ ? \qquad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{\underline{3}}\,\overset{b}{\underline{3}} \qquad Y = \overset{c}{\underline{1}}\,\overset{d}{\underline{2}} \qquad X \cdot Y =$$

$$ac = \qquad bd = \qquad (a+b)(c+d) =$$

Exemplo

$$\begin{array}{llllll} X = & \overset{a}{\underline{21}}\overset{b}{\underline{33}} & Y = & \overset{c}{\underline{23}}\overset{d}{\underline{12}} & X \cdot Y = & ? \\ ac = & 483 & \boxed{bd} = & ? & (a+b)(c+d) = & ? \end{array}$$

$$\begin{array}{llllll} X = & \overset{a}{\underline{3}}\overset{b}{\underline{3}} & Y = & \overset{c}{\underline{1}}\overset{d}{\underline{2}} & X \cdot Y = & \\ ac = & 3 & bd = & & (a+b)(c+d) = & \end{array}$$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \;?$$

$$\textcolor{red}{ac} = 483 \qquad \boxed{\textcolor{blue}{bd}} = \;? \qquad (a+b)(c+d) = \;?$$

$$X = \overset{a}{\underline{3}}\,\overset{b}{\underline{3}} \qquad Y = \overset{c}{\underline{1}}\,\overset{d}{\underline{2}} \qquad X \cdot Y =$$

$$\textcolor{red}{ac} = 3 \qquad \textcolor{blue}{bd} = \qquad (a+b)(c+d) =$$

Exemplo

$$X = \overset{a}{21}\overset{b}{33} \quad Y = \overset{c}{23}\overset{d}{12} \quad X \cdot Y = \ ?$$

$$ac = 483 \quad \boxed{bd} = \ ? \quad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{3}\overset{b}{3} \quad Y = \overset{c}{1}\overset{d}{2} \quad X \cdot Y =$$

$$ac = 3 \quad bd = 6 \quad (a+b)(c+d) =$$

Exemplo

$$X = \overset{a}{21}\overset{b}{33} \qquad Y = \overset{c}{23}\overset{d}{12} \qquad X \cdot Y = \ ?$$

$$ac = 483 \qquad \boxed{bd} = \ ? \qquad (a+b)(c+d) = \ ?$$

$$X = \overset{a}{3}\overset{b}{3} \qquad Y = \overset{c}{1}\overset{d}{2} \qquad X \cdot Y =$$

$$ac = 3 \qquad bd = 6 \qquad \underbrace{(a+b)}(c+d) =$$

Exemplo

$$X = \overset{a}{\overline{21}}\,\overset{b}{\overline{33}} \quad Y = \overset{c}{\overline{23}}\,\overset{d}{\overline{12}} \qquad X \cdot Y = \; ?$$

$$ac = 483 \quad \boxed{bd} = \; ? \qquad (a+b)(c+d) = \; ?$$

$$X = \overset{a}{\overline{3}}\,\overset{b}{\overline{3}} \quad Y = \overset{c}{\overline{1}}\,\overset{d}{\overline{2}} \qquad X \cdot Y =$$

$$ac = 3 \quad bd = 6 \qquad \underbrace{(a+b)}_{6}(c+d) =$$

Exemplo

$$X = \underbrace{21}_{a}\underbrace{33}_{b} \quad Y = \underbrace{23}_{c}\underbrace{12}_{d} \quad X \cdot Y = \ ?$$

$$ac = 483 \quad \boxed{bd} = \ ? \quad (a+b)(c+d) = \ ?$$

$$X = \underbrace{3}_{a}\underbrace{3}_{b} \quad Y = \underbrace{1}_{c}\underbrace{2}_{d} \quad X \cdot Y =$$

$$ac = 3 \quad bd = 6 \quad \underbrace{(a+b)}_{6}\underbrace{(c+d)}_{} =$$

Exemplo

$$X = \overset{a}{\overline{21}}\,\overset{b}{\overline{33}} \qquad Y = \overset{c}{\overline{23}}\,\overset{d}{\overline{12}} \qquad X \cdot Y = \; ?$$

$$ac = 483 \qquad \boxed{bd} = \; ? \qquad (a+b)(c+d) = \; ?$$

$$X = \overset{a}{\overline{3}}\,\overset{b}{\overline{3}} \qquad Y = \overset{c}{\overline{1}}\,\overset{d}{\overline{2}} \qquad X \cdot Y =$$

$$ac = 3 \qquad bd = 6 \qquad \underbrace{(a+b)}_{6}\underbrace{(c+d)}_{3} = 18$$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \;?$$

$$ac = 483 \qquad \boxed{bd} = \;? \qquad (a+b)(c+d) = \;?$$

$$X = \overset{a}{\underline{3}}\,\overset{b}{\underline{3}} \qquad Y = \overset{c}{\underline{1}}\,\overset{d}{\underline{2}} \qquad X \cdot Y = 396$$

$$ac = 3 \qquad bd = 6 \qquad (a+b)(c+d) = 18$$

$18-3-6=9$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$ac = 483 \qquad \boxed{bd} = \ ? \qquad (a+b)(c+d) = \ ?$$

$$X = 33 \qquad Y = 12 \qquad X \cdot Y = 396$$

$$ac = 3 \qquad bd = 6 \qquad (a+b)(c+d) = 18$$

Exemplo

$$X = \underbrace{21}_{a}\underbrace{33}_{b} \quad Y = \underbrace{23}_{c}\underbrace{12}_{d} \quad X \cdot Y = \; ?$$

$$ac = 483 \quad bd = \boxed{396} \quad (a+b)(c+d) = \; ?$$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$ac = 483 \qquad bd = 396 \qquad \underbrace{(a+b)}(c+d) = \ ?$$

Exemplo

$$X = \overset{a}{\underline{21}}\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$ac = 483 \qquad bd = 396 \qquad \underbrace{(a+b)}_{54}(c+d) = \ ?$$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \ ?$$

$$ac = 483 \qquad bd = 396 \qquad \underbrace{(a+b)}_{54}\underbrace{(c+d)} = \ ?$$

Exemplo

$$X = \overset{a}{\underline{21}}\,\overset{b}{\underline{33}} \qquad Y = \overset{c}{\underline{23}}\,\overset{d}{\underline{12}} \qquad X \cdot Y = \;?$$

$$ac = 483 \qquad bd = 396 \qquad \underbrace{(a+b)}_{54}\underbrace{(c+d)}_{35} = \;?$$

Exemplo

$$X = \underbrace{21}_{a}\underbrace{33}_{b} \quad Y = \underbrace{23}_{c}\underbrace{12}_{d} \quad X \cdot Y = ?$$

$$ac = 483 \quad bd = 396 \quad \boxed{\underbrace{(a+b)}_{54}\underbrace{(c+d)}_{35}} = ?$$

$$X = 54 \quad Y = 35 \quad X \cdot Y = ?$$

$$ac = ? \quad bd = ? \quad (a+b)(c+d) = ?$$

Exemplo

$$\begin{array}{llllll} & \underline{a}\ \underline{b} & & \underline{c}\ \underline{d} & & \\ X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ \color{red}{ac} = & 483 & \color{blue}{bd} = & 396 & \boxed{(a+b)(c+d)} = & ? \end{array}$$

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

Exemplo

$$\begin{array}{llllll} & \overset{a}{\underline{21}}\overset{b}{\underline{33}} & & \overset{c}{\underline{23}}\overset{d}{\underline{12}} & & \\ X = & 2133 & Y = & 2312 & X \cdot Y = & ? \\ ac = & 483 & bd = & 396 & \boxed{(a+b)(c+d)} = & ? \end{array}$$

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

$72 - 15 - 20 = 37$

Exemplo

$$X = \underbrace{21}_{a}\underbrace{33}_{b} \quad Y = \underbrace{23}_{c}\underbrace{12}_{d} \qquad X \cdot Y = \ ?$$

$$ac = 483 \quad bd = 396 \qquad \boxed{(a+b)(c+d)} = \ ?$$

$$X = 54 \quad Y = 35 \qquad X \cdot Y = 1890$$

$$ac = 15 \quad bd = 20 \qquad (a+b)(c+d) = 72$$

$72 - 15 - 20 = 37$

```
  20
 37
15
----
1890
```

Exemplo

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

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

Exemplo

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

Exemplo

$$X = 2133 \quad Y = 2312 \qquad \boxed{X \cdot Y = ?}$$

$$ac = 483 \quad bd = 396 \qquad (a+b)(c+d) = 1890$$

$1890 - 483 - 396 = 1011$

Exemplo

$$X = \textcolor{green}{21}33 \qquad Y = \textcolor{green}{23}12 \qquad \boxed{X \cdot Y = \;?}$$

$$\textcolor{red}{ac} = 483 \qquad \textcolor{blue}{bd} = 396 \qquad (a+b)(c+d) = 1890$$

$$1890 - \textcolor{red}{483} - \textcolor{blue}{396} = 1011$$

$$\begin{array}{ccccccc}
 & & & & \textcolor{blue}{3} & \textcolor{blue}{9} & \textcolor{blue}{6} \\
 & 1 & 0 & 1 & 1 & & \\
\textcolor{red}{4} & \textcolor{red}{8} & \textcolor{red}{3} & & & & \\
\hline
4 & 9 & 3 & 1 & 4 & 9 & 6
\end{array}$$

Exemplo

$$
\begin{array}{llllll}
X = & \color{green}{21}33 & Y = & \color{green}{23}12 & X \cdot Y = & \boxed{4931496} \\
\color{red}{ac} = & 483 & \color{blue}{bd} = & 396 & (a+b)(c+d) = & 1890
\end{array}
$$

$1890 - \color{red}{483} - \color{blue}{396} = 1011$

$$
\begin{array}{ccccccc}
 & & & & \color{blue}{3} & \color{blue}{9} & \color{blue}{6} \\
 & 1 & 0 & 1 & 1 & & \\
\color{red}{4} & \color{red}{8} & \color{red}{3} & & & & \\
\hline
4 & 9 & 3 & 1 & 4 & 9 & 6
\end{array}
$$

Algoritmo Multi

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

```
KARATSUBA (X, Y, n)
    se n ≤ 3 devolva X · Y
    q ← ⌈n/2⌉
    A ← X[q + 1 . . n]        B ← X[1 . . q]
    C ← Y[q + 1 . . n]        D ← Y[1 . . q]
    E ← KARATSUBA(A, C, ⌊n/2⌋)
    F ← KARATSUBA(B, D, ⌈n/2⌉)
    G ← KARATSUBA(A + B, C + D, ⌈n/2⌉ + 1)
    H ← G − F − E
    R ← E × 10^n + H × 10^⌈n/2⌉ + F
    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	$=$	$T(\lceil n/2 \rceil + 1) + \Theta(n)$
8	$=$	$\Theta(n)$
9	$=$	$\Theta(n)$
10	$=$	$\Theta(1)$
total	$=$	$T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + T(\lceil n/2 \rceil + 1) + \Theta(n)$

Consumo de tempo

Nosso estudo de recorrências sugere que a solução da recorrência

$$\begin{aligned} T(n) &= \Theta(1) \quad \text{para } n = 1, 2, 3 \\ T(n) &= T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + T(\lceil n/2 \rceil + 1) + \Theta(n) \quad n \geq 4 \end{aligned}$$

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	$\mathrm{O}(n^{1.585})$
Toom e Cook'63	$\mathrm{O}(n^{1.465})$
(divisão e conquista; generaliza o acima)	
Schönhage e Strassen'71	$\mathrm{O}(n \lg n \lg\lg n)$
(FFT em aneis de tamanho específico)	
Fürer'07	$\mathrm{O}(n \lg n\, 2^{\mathrm{O}(\log^* n)})$
Harvey e van der Hoeven'20	$\mathrm{O}(n \log n)$
(Gaussian ressampling, 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

Multiplicação de matrizes

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

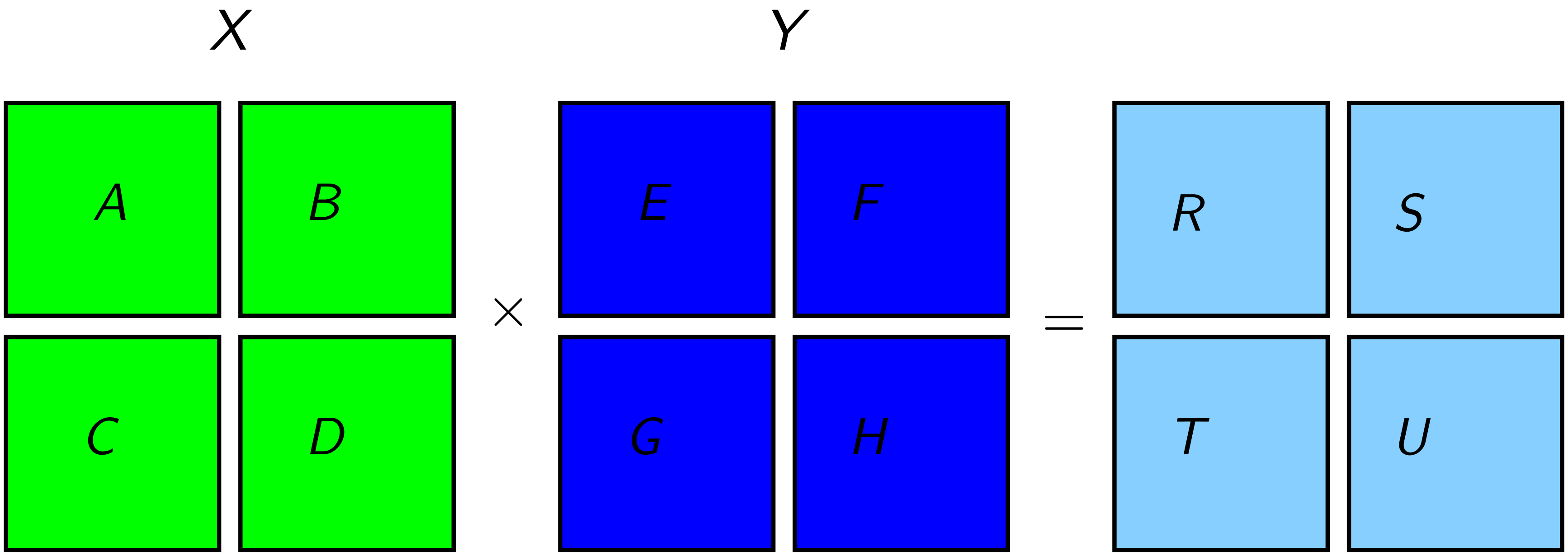
O algoritmo tradicional de multiplicação de matrizes consome tempo $\Theta(n^3)$.

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \times \begin{pmatrix} E & F \\ G & H \end{pmatrix} = \begin{pmatrix} R & S \\ T & U \end{pmatrix}$$

$$\begin{aligned} R &= AE + BG \\ S &= AF + BH \\ T &= CE + DG \\ U &= CF + DH \end{aligned} \tag{1}$$

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 matrizes $X[1\,..\,n, 1\,..\,n]$ e $Y[1\,..\,n, 1\,..\,n]$ e devolve $X \cdot Y$.

```
MULTI-M (X, Y, n)
    se n = 1 devolva X · Y
    (A, B, C, D) ← PARTICIONE(X, n)
    (E, F, G, H) ← PARTICIONE(Y, n)
    R ← MULTI-M(A, E, n/2) + MULTI-M(B, G, n/2)
    S ← MULTI-M(A, F, n/2) + MULTI-M(B, H, n/2)
    T ← MULTI-M(C, E, n/2) + MULTI-M(D, G, n/2)
    U ← MULTI-M(C, F, n/2) + MULTI-M(D, H, n/2)
    P ← CONSTRÓI-MAT(R, S, T, U)
    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	$=$	$\Theta(1)$
total	$=$	$8\,T(n/2) + \Theta(n^2)$

Consumo de tempo

Nosso estudo de recorrências sugere
que a solução da recorrência

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

está na mesma classe Θ que a solução de

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

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

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \times \begin{pmatrix} E & F \\ G & H \end{pmatrix} = \begin{pmatrix} R & S \\ T & U \end{pmatrix}$$

$$\begin{aligned}
P_1 &= A(F - H) = AF - AH \\
P_2 &= (A + B)H = AH + BH \\
P_3 &= (C + D)E = CE + DE \\
P_4 &= D(G - E) = DG - DE \\
P_5 &= (A + D)(E + H) = AE + AH + DE + DH \\
P_6 &= (B - D)(G + H) = BG + BH - DG - DH \\
P_7 &= (A - C)(E + F) = AE + AF - CE - CF
\end{aligned}$$

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

$$
\begin{aligned}
P_1 &= A(F - H) = AF - AH \\
P_2 &= (A + B)H = AH + BH \\
P_3 &= (C + D)E = CE + DE \\
P_4 &= D(G - E) = DG - DE \\
P_5 &= (A + D)(E + H) = AE + AH + DE + DH \\
P_6 &= (B - D)(G + H) = BG + BH - DG - DH \\
P_7 &= (A - C)(E + F) = AE + AF - CE - CFD
\end{aligned}
$$

$$
\begin{aligned}
R &= P_5 + P_4 - P_2 + P_6 = AE + BG \\
S &= P_1 + P_2 = AF + BH \\
T &= P_3 + P_4 = CE + DG \\
U &= P_5 + P_1 - P_3 - P_7 = CF + DH
\end{aligned}
$$

Algoritmo de Strassen

STRASSEN (X, Y, n)

se $n = 1$ **devolva** $X \cdot Y$
$(A, B, C, D) \leftarrow$ PARTICIONE(X, n)
$(E, F, G, H) \leftarrow$ PARTICIONE(Y, n)
$P_1 \leftarrow$ STRASSEN$(A, F - H, n/2)$
$P_2 \leftarrow$ STRASSEN$(A + B, H, n/2)$
$P_3 \leftarrow$ STRASSEN$(C + D, E, n/2)$
$P_4 \leftarrow$ STRASSEN$(D, G - E, n/2)$
$P_5 \leftarrow$ STRASSEN$(A + D, E + H, n/2)$
$P_6 \leftarrow$ STRASSEN$(B - D, G + H, n/2)$
$P_7 \leftarrow$ STRASSEN$(A - C, E + F, n/2)$
$R \leftarrow P_5 + P_4 - P_2 + P_6$
$S \leftarrow P_1 + P_2$
$T \leftarrow P_3 + P_4$
$U \leftarrow P_5 + P_1 - P_3 - P_7$
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

Nosso estudo de recorrências sugere que a solução da recorrência

$$\begin{aligned} T(1) &= \Theta(1) \\ T(n) &= 7\,T(n/2) + \Theta(n^2) \quad \text{para } n = 2, 3, 4, \ldots \end{aligned}$$

está na mesma classe Θ que a solução de

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

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)	$\mathrm{O}(n^{2.807})$
$\vdots$	$\vdots$
Coppersmith e Winograd (1987)	$\mathrm{O}(n^{2.3755})$
Stothers (2010)	$\mathrm{O}(n^{2.3736})$
Williams (2013)	$\mathrm{O}(n^{2.3728642})$
Le Gall (2014)	$\mathrm{O}(n^{2.3728639})$
Alman e Williams (2020)	$\mathrm{O}(n^{2.3728596})$
Duan, Wu e Zhou (2023)	$\mathrm{O}(n^{2.371866})$
Williams, Xu, Xu e Zhou (2024)	$\mathrm{O}(n^{2.371552})$
Alman, Duan, Williams, Xu, Xu e Zhou (2025)	$\mathrm{O}(n^{2.371339})$