Schnelle Exponentiation von Matrizen (A326)

Von Yulia Nikirova und Andriy Manucharyan

Team 147

Überblick

1. Einleitung
2. Genauigkeit
3. Bignum-Datenstruktur
4. Karazuba-Multiplikation und Addition
5. Schnelle Exponentiation
6. Performanzanalyse der beiden Exponentiationen
7. Fazit

Einleitung

$$\begin{pmatrix} x_{n-1} & x_n \\ x_n & x_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^n \qquad \lim_{n\to\infty} 1 + \frac{x_n}{x_{n+1}} = \sqrt{2}$$

Berechnung der Genauigkeit

$$n > 1 + \frac{1}{2} \cdot \log_2 10 \cdot \log_{10} \frac{1}{\varepsilon}$$

Berechnung der Genauigkeit

$$n > 1 + \frac{1}{2} \cdot \log_2 10 \cdot \log_{10} \frac{1}{\varepsilon}$$

$$\log_2 10 \approx 3.3$$

$$n = \lceil 1 + 1.65 \cdot \log_{10} \frac{1}{\varepsilon} \rceil$$

Bignum-Datenstruktur

$$1|00000000000000000000000000000000|00000000000000000000110110010011$$

$array[0]$	$array[1]$	$array[2]$
00000000000000000000110110010011	00000000000000000000000000000000	1

Karazuba-Multiplikation

$$A = ax + b \qquad B = cx + d$$

Karazuba-Multiplikation

$$A = ax + b \qquad B = cx + d$$

$$AB = ac \cdot x^2 + ((a+b) \cdot (c+d) - ac - bd) \cdot x + bd$$

Schnelle Exponentiation

$$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^6 \qquad 6_{10} = 110_2$$

$$\begin{pmatrix} x_{n-1} & x_n \\ x_n & x_{n+1} \end{pmatrix}^2 = \begin{pmatrix} x_{n-1} \cdot x_{n-1} + x_n \cdot x_n & x_{n-1} \cdot x_n + x_n \cdot x_{n+1} \\ x_{n-1} \cdot x_n + x_n \cdot x_{n+1} + x_n & x_n \cdot x_n + x_{n+1} \cdot x_{n+1} \end{pmatrix}$$

Schnelle Exponentiation

$$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^6$$

$$6_{10} = 110_2$$

$$QMQ$$

Schnelle Exponentiation

$$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^6$$

$$6_{10} = 110_2$$

1. $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$

$$QMQ$$

Schnelle Exponentiation

$$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^6$$

$$6_{10} = 110_2$$

$$QMQ$$

1. $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 5 & 12 \end{pmatrix}$

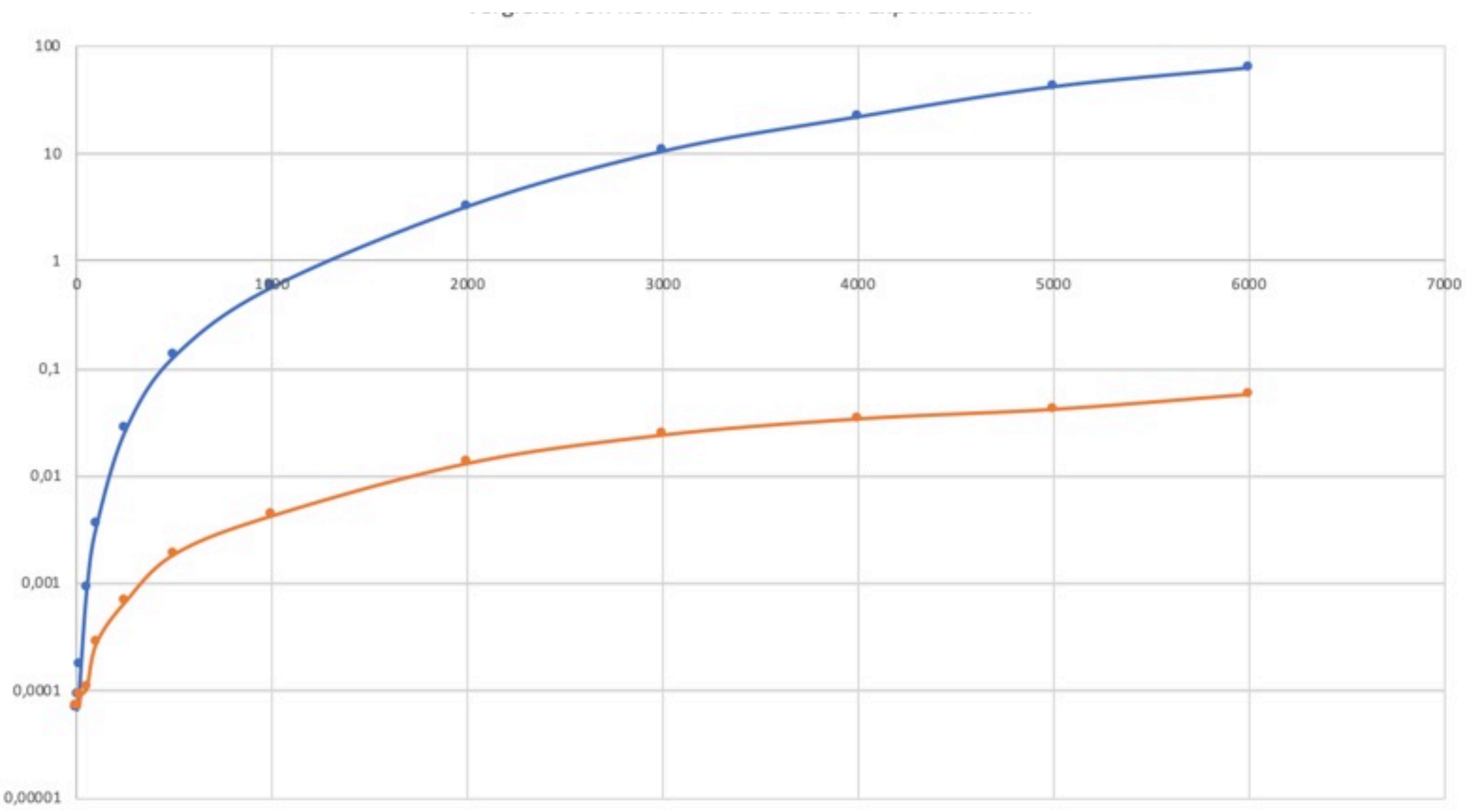
Schnelle Exponentiation

$$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^6 = \begin{pmatrix} 29 & 70 \\ 70 & 169 \end{pmatrix}$$

$$6_{10} = 110_2$$

1. $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 5 & 12 \end{pmatrix}$
3. $\begin{pmatrix} 2 & 5 \\ 5 & 12 \end{pmatrix}^2 = \begin{pmatrix} 29 & 70 \\ 70 & 169 \end{pmatrix}$

Vergleich der binären Exponentiation zur „naiven“



Fazit

Vielen Dank für Ihre Aufmerksamkeit!