



# Schnelle Polynomauswertung

$$\begin{bmatrix} 1 & x_0 & (x_0)^2 & \dots & (x_0)^{n-1} \\ 1 & x_1 & (x_1)^2 & \dots & (x_1)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n/2-1} & (x_{n/2-1})^2 & \dots & (x_{n/2-1})^{n-1} \\ \hline 1 & -x_0 & (-x_0)^2 & \dots & (-x_0)^{n-1} \\ 1 & -x_1 & (-x_1)^2 & \dots & (-x_1)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & -x_{n/2-1} & (-x_{n/2-1})^2 & \dots & (-x_{n/2-1})^{n-1} \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ \vdots \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_{n/2-1}) \\ \hline P(-x_0) \\ P(-x_1) \\ \vdots \\ P(-x_{n/2-1}) \end{bmatrix}$$

Einsparung: Wir benötigen nur das Produkt der oberen Matrixhälfte, für untere Hälfte gilt: alles gleich bis auf Vorzeichenwechsel für ungerade Exponenten

# Schnelle Polynomauswertung

Obere Hälfte: 
$$\begin{bmatrix} 1 & x_0 & (x_0)^2 & \dots & (x_0)^{n-1} \\ 1 & x_1 & (x_1)^2 & \dots & (x_1)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n/2-1} & (x_{n/2-1})^2 & \dots & (x_{n/2-1})^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ \vdots \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_{n/2-1}) \end{bmatrix}$$

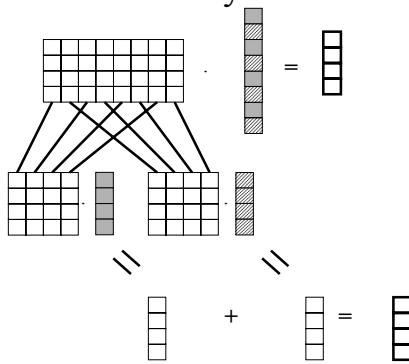
nach geraden und ungeraden Exponenten aufgeteilt:

$$\begin{bmatrix} 1 & (x_0)^2 & \dots & (x_0)^{n-2} \\ 1 & (x_1)^2 & \dots & (x_1)^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & (x_{n/2-1})^2 & \dots & (x_{n/2-1})^{n-2} \end{bmatrix} \begin{bmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{bmatrix} = \begin{bmatrix} G(x_0) \\ G(x_1) \\ \vdots \\ G(x_{n/2-1}) \end{bmatrix} \quad G(x_k) = \sum_{i=0}^{n/2-1} a_{2i} x_k^{2i}$$

$$\begin{bmatrix} x_0 & (x_0)^3 & \dots & (x_0)^{n-1} \\ x_1 & (x_1)^3 & \dots & (x_1)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ -x_{n/2-1} & (-x_{n/2-1})^3 & \dots & (-x_{n/2-1})^{n-1} \end{bmatrix} \begin{bmatrix} a_1 \\ a_3 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} U(x_0) \\ U(x_1) \\ \vdots \\ U(x_{n/2-1}) \end{bmatrix} \quad U(x_k) = \sum_{i=0}^{n/2-1} a_{2i+1} x_k^{2i+1}$$

$$P(x_k) = G(x_k) + U(x_k)$$

# Schnelle Polynomauswertung



# Schnelle Polynomauswertung

$$G(x) = \sum_{i=0}^{n/2-1} a_{2i} x^{2i} \quad U(x) = \sum_{i=0}^{n/2-1} a_{2i+1} x^{2i+1}$$

$G(x)$  ist ein Polynom  $n/2-1$ -ten Grades in  $x^2$  nämlich

$$G(x) = \sum_{i=0}^{n/2-1} a_{2i} (x^2)^i = P_G(x^2)$$

$U(x)$  läßt sich ähnlich schreiben als

$$U(x) = x \sum_{i=0}^{n/2-1} a_{2i+1} (x^2)^i = x P_U(x^2)$$

aus  $P(x) = G(x) + U(x)$  folgt  $P(x) = P_G(x^2) + x P_U(x^2)$

# Schnelle Polynomauswertung

um also das Matrix-Vektor-Produkt zu berechnen benötigen wir:

$$P_G(x^2) = \sum_{i=0}^{n/2-1} a_{2i} (x^2)^i \quad \text{und}$$

$$P_U(x^2) = x \sum_{i=0}^{n/2-1} a_{2i+1} (x^2)^i$$

$$\begin{bmatrix} 1 & x_0 & (x_0)^2 & \dots & (x_0)^{n-1} \\ 1 & x_1 & (x_1)^2 & \dots & (x_1)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n/2-1} & (x_{n/2-1})^2 & \dots & (x_{n/2-1})^{n-1} \\ \hline 1 & -x_0 & (-x_0)^2 & \dots & (-x_0)^{n-1} \\ 1 & -x_1 & (-x_1)^2 & \dots & (-x_1)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & -x_{n/2-1} & (-x_{n/2-1})^2 & \dots & (-x_{n/2-1})^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ \vdots \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} P(x_0) \\ P(x_1) \\ \vdots \\ P(x_{n/2-1}) \\ \hline P(-x_0) \\ P(-x_1) \\ \vdots \\ P(-x_{n/2-1}) \end{bmatrix}$$

Das sind zwei Probleme der halben Größe, zusätzlich brauchen wir:  $n/2$  Additionen (gerade+ungerade),  $n/2$  Subtraktionen (für  $P(-x)=\dots$ ), 2 mal  $n/2$  Multiplikationen ( $n/2$  je Matrixhälfte für  $P_U(x^2) = x \cdot \dots$ )

Wenn das weiter klappt, ist der Aufwand  $T(n)=2T(n/2)+O(n) = O(n \log n)$

# Schnelle Polynomauswertung

Rekursion läßt sich nicht fortsetzen:

Wir hatten ausgenutzt, daß  $(-x)^2 = x^2$  und konnten so die Matrix „halbieren“.

Wenn wir in die Rekursion einsteigen mit der Berechnung von  $P_U(x^2)$  und  $P_G(x^2)$  dann sind alle Funktionsargumente positiv,

=> „Halbierung“ nicht mehr möglich.

# Schnelle Polynomauswertung

betrachten wir die Berechnung von  $P_G(x^2)$

$$\begin{bmatrix} 1 & (x_0)^2 & \dots & (x_0)^{n-2} \\ 1 & (x_1)^2 & \dots & (x_1)^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & (x_{n/2-1})^2 & \dots & (x_{n/2-1})^{n-2} \end{bmatrix} \begin{bmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{bmatrix} = \begin{bmatrix} P_G(x_0) \\ P_G(x_1) \\ \vdots \\ P_G(x_{n/2-1}) \end{bmatrix}$$

für den Abstieg in die Rekursion wäre gut, wenn  $(x_{n/4})^2 = -(x_0)^2$

das ist der Fall wenn  $x_{j+n/4} = ix_j$

In der nächsten Rekursionsebene sollte dann  $(x_{n/8})^4 = -(x_0)^4$  sein usw.

# Schnelle Polynomauswertung

Wenn  $x_0 = 1$

dann wollen wir, daß  $(x_{n/4})^2 = -(x_0)^2 \Rightarrow x_{n/4} = \sqrt{-1} = i$

$$(x_{n/8})^4 = -(x_0)^4 \Rightarrow x_{n/8} = \sqrt[4]{-1}$$

usw.

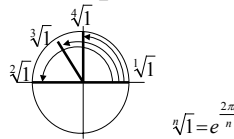
wählen wir also  $x_0 = \omega^0, x_1 = \omega^1, x_2 = \omega^2, \dots, x_{n-1} = \omega^{n-1}$

wobei  $\omega^n = 1$ , und  $\omega^j \neq 1$  für  $0 < j < n$

$\omega$  ist  $n$ -te Einheitswurzel

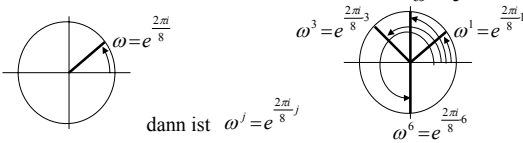
# Darstellung komplexer Exponenten

Die  $n$ -te Einheitswurzel liegt auf dem Einheitskreis nach einem  $n$ -tel des Vollkreises,



läßt sich auch schreiben als  $e^{j \frac{2\pi}{n}}$

Für  $n=8$  ist  $\omega$  ein Achtel des Vollkreises



dann ist  $\omega^j = e^{j \frac{2\pi}{n}}$

# Schnelle Polynomauswertung

Wir erhalten also zur Auswertung von Polynomen die folgende Matrix:

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^{2^2} & \dots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{(n-1)2} & \dots & \omega^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} P(1) \\ P(\omega) \\ P(\omega^2) \\ \vdots \\ P(\omega^{n-1}) \end{bmatrix}$$

Diese Matrix ist die DFT-Matrix für  $n$ , und  $(P(1), P(\omega), \dots, P(\omega^{n-1}))$  ist die diskrete Fouriertransformierte des Vektors  $a_0, a_1, \dots, a_{n-1}$

# Schnelle Polynomauswertung

Ein paar DFT Matrizen:

$$DFT_1 = [1] \quad \omega = \sqrt[1]{1} = 1$$

$$DFT_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \omega = \sqrt[2]{1} = -1$$

$$DFT_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \quad \omega = \sqrt[4]{1} = i$$

# Polynommultiplikation mit FFT

Wir können also ein Polynom an  $n$  Stellen in  $O(n \log n)$  auswerten.

Was fehlt noch zur Polynommultiplikation?

Die Rückumwandlung in die Koeffizientendarstellung:

Da  $DFT$  invertierbar ist, gilt

$$[DFT] \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} P(1) \\ P(\omega) \\ \vdots \\ P(\omega^{(n-1)}) \end{bmatrix} \Rightarrow \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = [DFT]^{-1} \begin{bmatrix} P(1) \\ P(\omega) \\ \vdots \\ P(\omega^{(n-1)}) \end{bmatrix}$$

# Inverse Fouriertransformation

DFT

DFT<sup>-1</sup>

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^{2^2} & \dots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{(n-1)^2} & \dots & \omega^{(n-1)(n-1)} \end{bmatrix} \cdot \frac{1}{n} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1/\omega & 1/\omega^2 & \dots & 1/\omega^{n-1} \\ 1 & 1/\omega^2 & 1/\omega^{2^2} & \dots & 1/\omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1/\omega^{n-1} & 1/\omega^{(n-1)^2} & \dots & 1/\omega^{(n-1)(n-1)} \end{bmatrix}$$

Es ist offensichtlich, daß wenn  $\omega$   $n$ -te Einheitswurzel ist, dann ist auch  $1/\omega$   $n$ -te Einheitswurzel.

# Polynommultiplikation mit FFT

Beispiel:  $P = x + 2$   $Q = 2x - 1$

$$DFT_4 \cdot P = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & i^2 & i^3 \\ 1 & i^2 & i^4 & i^6 \\ 1 & i^3 & i^6 & i^9 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 2+1 \\ 2+i \\ 2+i^2 \\ 2+i^3 \end{bmatrix} = F(P) \quad DFT_4 \cdot Q = DFT_4 \cdot \begin{bmatrix} -1 \\ -1+2i \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \\ -1+2i \\ -1+2i^2 \\ -1+2i^3 \end{bmatrix} = F(Q)$$

FFT

$O(n \log n)$

$$F(P) \circ F(Q) = \begin{bmatrix} 2+1 \\ 2+i \\ 2+i^2 \\ 2+i^3 \end{bmatrix} \cdot \begin{bmatrix} -1+2i \\ -1+2i^2 \\ -1+2i^3 \\ -1+2i^4 \end{bmatrix} = \begin{bmatrix} 3 \\ -2+4i-i+2i^2 \\ -2+4i^2-i^2+2i^4 \\ -2+4i^3-i^3+2i^6 \end{bmatrix} = \begin{bmatrix} 3 \\ -4+3i \\ -3 \\ -4-3i \end{bmatrix}$$

koeffizientenweise Multiplikation  $O(n)$

$$\frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1/i & 1/i^2 & 1/i^3 \\ 1 & 1/i^2 & 1/i^4 & 1/i^6 \\ 1 & 1/i^3 & 1/i^6 & 1/i^9 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ -4+3i \\ -3 \\ -4-3i \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 3-4+3i-3-4-3i \\ 3-4/i+3-3/i^2-4/i^3-3/i^2 \\ 3-4/i^2+3/i-3/i^2-4/i^6-3/i^5 \\ 3-4/i^3+3/i^2-3/i^6-4/i^9-3/i^8 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} -8 \\ 12 \\ 8 \\ 0 \end{bmatrix} = \begin{bmatrix} -2 \\ 3 \\ 2 \\ 0 \end{bmatrix}$$

FFT<sup>-1</sup>

$O(n \log n)$

$$\Rightarrow (PQ)(x) = 2x^2 + 3x - 2$$

# Polynommultiplikation mit FFT

Beispiel: Auswertung mit FFT

$$DFT_4 \cdot P = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & i^2 & i^3 \\ 1 & i^2 & i^4 & i^6 \\ 1 & i^3 & i^6 & i^9 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 2+1 \\ 2+i \\ 2+i^2 \\ 2+i^3 \end{bmatrix} = \begin{bmatrix} 3 \\ 2+i \\ 1 \\ 2-i \end{bmatrix} = F(P)$$

obere Hälfte:

untere Hälfte:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & i^2 & i^3 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \\ 0 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \end{bmatrix} + \begin{bmatrix} 1 \\ i \end{bmatrix} = \begin{bmatrix} 3 \\ 2+i \end{bmatrix}$$

$$\begin{bmatrix} 1 & i^2 & i^4 & i^6 \\ 1 & i^4 & i^6 & i^9 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \\ 0 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 0 \end{bmatrix} + \begin{bmatrix} -1 & -1 \\ -i & i \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \end{bmatrix} + \begin{bmatrix} -1 \\ -i \end{bmatrix} = \begin{bmatrix} 1 \\ 2-i \end{bmatrix}$$