Script **generated by TTT**

Title: Mayr: 2012 ds (29.11.2012)

Date: Thu Nov 29 10:27:20 CET 2012

Duration: 80:43 min

Pages: 28

WS 2012/13

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2012WS/ds/

Wintersemester 2012

Inhaltsverzeichnis

Problem: Bijektion i.a. zu komplex.

Definition 145

Ein $\omega \in \mathbb{C}$ heißt primitive n-te Einheitswurzel, wenn $\omega^k \neq 1$ für alle $k = 1, \ldots, n-1$ und $\omega^n = 1$ gilt, d.h. $\operatorname{ord}(\omega) = n$ in $\mathbb{C}^* = \mathbb{C} \setminus 0$.

Bemerkung: Es ist $\omega = e^{2i\pi/n}$ eine primitive n-te Einheitswurzel.

Definition 146

Sei $\omega \in \mathbb{C}$ eine primitive n-te Einheitswurzel, $n \in \mathbb{N}$. Die Abbildung

$$\mathcal{F}_{n,\omega}: \quad \mathbb{C}^n \to \mathbb{C}^n,$$
$$\vec{a} = (a_0, \ldots, a_{n-1}) \mapsto (P_{\vec{a}}(1), P_{\vec{a}}(\omega), \ldots, P_{\vec{a}}(\omega^{n-1}))$$

heißt diskrete Fouriertransformation; wir schreiben auch kurz $\mathcal{F}$ für $\mathcal{F}_{n,\omega}$.

Die Fouriertransformation ist nach Jean Baptiste Joseph Fourier (1768–1830) benannt.

Bemerkung: $\mathcal{F}$ is nach Lemma 144 und anschließender Bemerkung eine Bijektion.

Lemma 147

Seien $\vec{a}, \vec{b} \in \mathbb{C}^n$ so, dass auch $\vec{a} * \vec{b} \in \mathbb{C}^n$. Dann gilt

$$\mathcal{F}(\vec{a} * \vec{b}) = \mathcal{F}(\vec{a}) \cdot \mathcal{F}(\vec{b}).$$

Beweis:
Es gilt

$$\begin{aligned}\mathcal{F}(\vec{a}) \cdot \mathcal{F}(\vec{b}) &= (P_{\vec{a}}(1)P_{\vec{b}}(1), P_{\vec{a}}(\omega)P_{\vec{b}}(\omega), \ldots, P_{\vec{a}}(\omega^{n-1})P_{\vec{b}}(\omega^{n-1})) \\ &= (P_{\vec{c}}(1), P_{\vec{c}}(\omega), \ldots, P_{\vec{c}}(\omega^{n-1})) \\ &= \mathcal{F}(\vec{c}), \quad \text{mit } \vec{c} = \vec{a} * \vec{b}.\end{aligned}$$

Idee: Berechne $\vec{a} * \vec{b}$ vermöge $\mathcal{F}^{-1}(\mathcal{F}(\vec{a}) \cdot \mathcal{F}(\vec{b}))$. Die komponentenweise Multiplikation $F(\vec{a}) \cdot \mathcal{F}(\vec{b})$ benötigt nur $O(n)$ Operationen.

Jedoch: $\mathcal{F}$ ist eine lineare Abbildung $\mathcal{F}(\vec{a}) = F\vec{a}$, mit $F = (\omega^{kl})_{0 \le l,k \le n-1}$. Die Matrixmultiplikation benötigt aber $\Omega(n^2)$ Operationen (also keine offensichtliche Verbesserung im Vergleich zur klassischen Polynom-Multiplikation)!

Ausweg: "Divide and Conquer"!!!

Idee: Berechne $\vec{a} * \vec{b}$ vermöge $\mathcal{F}^{-1}(\mathcal{F}(\vec{a}) \cdot \mathcal{F}(\vec{b}))$. Die komponentenweise Multiplikation $F(\vec{a}) \cdot \mathcal{F}(\vec{b})$ benötigt nur $O(n)$ Operationen.

Jedoch: $\mathcal{F}$ ist eine lineare Abbildung $\mathcal{F}(\vec{a}) = F\vec{a}$, mit $F = (\omega^{kl})_{0 \le l,k \le n-1}$. Die Matrixmultiplikation benötigt aber $\Omega(n^2)$ Operationen (also keine offensichtliche Verbesserung im Vergleich zur klassischen Polynom-Multiplikation)!

Ausweg: "Divide and Conquer"!!!

3.5.2 Berechnung der diskreten Fouriertransformation (FFT)

Sei $n = 2^k$ eine 2er-Potenz. Zerlege $\vec{a} = (a_0, \ldots, a_{n-1})$ in einen

geraden Anteil	$\vec{a}_g = (a_0, a_2, \ldots, a_{n-2})$	und einen
ungeraden Anteil	$\vec{a}_u = (a_1, a_3, \ldots, a_{n-1})$	

Dann gilt:

$$P_{\vec{a}}(x) = P_{\vec{a}_g}(x^2) + xP_{\vec{a}_u}(x^2)\,.$$

Beispiel 148

Sei $\vec{a} = (1, 2, 4, 8)$, also $P_{\vec{a}}(x) = 1 + 2x + 4x^2 + 8x^3$. Damit ist $\vec{a}_g = (1, 4)$ und $\vec{a}_u = (2, 8)$, also

$$\begin{aligned}&P_{\vec{a}_g}(x^2) + xP_{\vec{a}_u}(x^2) \\ &\qquad = 1 \cdot (x^2)^0 + 4 \cdot (x^2)^1 + x \cdot (2 \cdot (x^2)^0 + 8 \cdot (x^2)^1) \\ &\qquad = 1 + 2 \cdot x + 4 \cdot x^2 + 8 \cdot x^3\end{aligned}$$

3.5.2 Berechnung der diskreten Fouriertransformation (FFT)

Sei $n = 2^k$ eine 2er-Potenz. Zerlege $\vec{a} = (a_0, \ldots, a_{n-1})$ in einen

geraden Anteil	$\vec{a}_g = (a_0, a_2, \ldots, a_{n-2})$	und einen
ungeraden Anteil	$\vec{a}_u = (a_1, a_3, \ldots, a_{n-1})$	

Dann gilt:

$$P_{\vec{a}}(x) = P_{\vec{a}_g}(x^2) + xP_{\vec{a}_u}(x^2)\,.$$

Beispiel 148

Sei $\vec{a} = (1, 2, 4, 8)$, also $P_{\vec{a}}(x) = 1 + 2x + 4x^2 + 8x^3$. Damit ist $\vec{a}_g = (1, 4)$ und $\vec{a}_u = (2, 8)$, also

$$\begin{aligned} P_{\vec{a}_g}(x^2) + xP_{\vec{a}_u}(x^2) \\ &= 1 \cdot (x^2)^0 + 4 \cdot (x^2)^1 + x \cdot (2 \cdot (x^2)^0 + 8 \cdot (x^2)^1) \\ &= 1 + 2 \cdot x + 4 \cdot x^2 + 8 \cdot x^3 \end{aligned}$$

Lemma 149

Ist $\mathcal{F}_{\frac{n}{2},\omega^2}(\vec{a}_g) = (c_0, \ldots, c_{\frac{n}{2}-1})$ *und* $\mathcal{F}_{\frac{n}{2},\omega^2}(\vec{a}_u) = (d_0, \ldots, d_{\frac{n}{2}-1})$*, so gilt* $\mathcal{F}_{n,\omega}(\vec{a}) = (e_0, \ldots, e_{n-1})$ *mit*

$$\begin{aligned} e_i &= P_{\vec{a}}(\omega^i) \\ &= P_{\vec{a}_g}(\omega^{2i}) + \omega^i P_{\vec{a}_u}(\omega^{2i}) \\ &= c_i + \omega^i d_i \\ e_{\frac{n}{2}+i} &= P_{\vec{a}}(\omega^{\frac{n}{2}+i}) \\ &= P_{\vec{a}_g}(\omega^{2(\frac{n}{2}+i)}) + \omega^{\frac{n}{2}+i} P_{\vec{a}_u}(\omega^{2(\frac{n}{2}+i)}) \\ &\models c_i + \omega^{\frac{n}{2}+i} d_i \end{aligned}$$

für $i = 0, \ldots, \frac{n}{2} - 1$.

Bem.: ω^2 ist primitive $\frac{n}{2}$-te Einheitswurzel. Natürlich ist $\omega^{2\frac{n}{2}} = 1$.

Dies liefert folgenden Divide-and-Conquer-Algorithmus:

```
DFT(a⃗,ω)
  Eingabe: a⃗ = (a_0,...,a_{n-1}), n = 2^k, ω
  Ausgabe: F_{n,ω}(a⃗) = (e_0,...,e_{n-1})

  if n = 1 then e_0 := a_0
  else
    a⃗_g := (a_0, a_2, ..., a_{n-2})
    a⃗_u := (a_1, a_3, ..., a_{n-1})
    (c_0,...,c_{n/2-1}) :=DFT(a⃗_g, ω^2)
    (d_0,...,d_{n/2-1}) :=DFT(a⃗_u, ω^2)
    for i = 0 to n/2 |- 1 do
      e_i := c_i + ω^i d_i
      e_{n/2+i} := c_i + ω^{n/2+i} d_i
    endfor
  endif
  return(e_0,...,e_{n-1})
```


Satz 150

Der Algorithmus `DFT` *berechnet* $\mathcal{F}_{n,\omega}(\vec{a})$ *auf Eingabe* $n = 2^k$, $\vec{a}$, ω *in* $T(n) = O(n \log n)$ *Operationen.*

Beweis:

Aus dem Algorithmus erhält man folgende Rekursion

$$T(n) = 2T(n/2) + cn$$

mit einer Konstante $c > 0$ und $T(1) = 1$. Mit $n = 2^k$ folgt

$$\begin{aligned} T(2^k) &= 2T(2^{k-1}) + cn = 2(2T(2^{k-2}) + cn/2) + cn \\ &= \ldots = 2^\ell T(2^{k-\ell}) + \ell cn \end{aligned}$$

Satz 150

Der Algorithmus DFT *berechnet* $\mathcal{F}_{n,\omega}(\vec{a})$ *auf Eingabe* $n = 2^k$, $\vec{a}$, ω *in* $T(n) = O(n \log n)$ *Operationen.*

Beweis:

Aus dem Algorithmus erhält man folgende Rekursion

$$T(n) = 2T(n/2) + cn$$

mit einer Konstante $c > 0$ und $T(1) = 1$. Mit $n = 2^k$ folgt

$$T(2^k) = 2T(2^{k-1}) + cn = 2(2T(2^{k-2}) + cn/2) + cn$$
$$= \ldots = 2^\ell T(2^{k-\ell}) + \ell cn$$

Speziell für $\ell = k$ gilt $T(2^k) = kc2^k + 2^k T(1)$, und wir erhalten $T(2^k) = O(2^k k) = O(n \log n)$.

Dies liefert folgenden Divide-and-Conquer-Algorithmus:

DFT($\vec{a}$, ω)
  Eingabe: $\vec{a} = (a_0, \ldots, a_{n-1})$, $n = 2^k$, ω
  Ausgabe: $\mathcal{F}_{n,\omega}(\vec{a}) = (e_0, \ldots, e_{n-1})$

  if $n = 1$ **then** $e_0 := a_0$
  else
    $\vec{a}_g := (a_0, a_2, \ldots, a_{n-2})$
    $\vec{a}_u := (a_1, a_3, \ldots, a_{n-1})$
    $(c_0, \ldots, c_{\frac{n}{2}-1})$:=DFT($\vec{a}_g, \omega^2$)
    $(d_0, \ldots, d_{\frac{n}{2}-1})$:=DFT($\vec{a}_u, \omega^2$)
    for $i = 0$ **to** $\frac{n}{2} - 1$ **do**
      $e_i := c_i + \omega^i d_i$
      $e_{\frac{n}{2}+i} := c_i + \omega^{\frac{n}{2}+i} d_i$
    endfor
  endif
  return$(e_0, \ldots, e_{n-1})$

3.5.3 Berechnung der inversen diskreten Fouriertransformation

Satz 151

Es gilt

$$\mathcal{F}_{n,\omega}^{-1} = \frac{1}{n} \mathcal{F}_{n,\omega^{-1}}.$$

Bemerkung: ω^{-1} ist ebenso eine primitive n-te Einheitswurzel.

Zum Beweis von Satz 151 benötigen wir folgendes Lemma:

Lemma 152

Ist ω *eine primitive* n*-te Einheitswurzel, so gilt*

$$\sum_{j=0}^{n-1} \omega^{kj} = 0$$

für alle $k = 1, \ldots, n-1$.

3.5.3 Berechnung der inversen diskreten Fouriertransformation

Satz 151

Es gilt

$$\mathcal{F}_{n,\omega}^{-1} = \frac{1}{n}\mathcal{F}_{n,\omega^{-1}}.$$

Bemerkung: ω^{-1} ist ebenso eine primitive n-te Einheitswurzel.
Zum Beweis von Satz 151 benötigen wir folgendes Lemma:

Lemma 152

Ist ω eine primitive n-te Einheitswurzel, so gilt

$$\sum_{j=0}^{n-1} \omega^{kj} = 0$$

für alle $k = 1, \ldots, n-1$.

Beweis:

Für jedes $a \in \mathbb{C}$, $a \neq 1$, gilt $\sum_{j=0}^{n-1} a^j = \frac{a^n-1}{a-1}$. Speziell für $a = \omega^k$ ist $a^n = \omega^{kn} = 1$, $(k = 1, \ldots, n-1)$. □

Nun zum Beweis von Satz 151.

Beweis:

Sei $\vec{e} = \mathcal{F}_{n,\omega}(\vec{a}) = (e_0, \ldots, e_{n-1})$. Wir zeigen, dass gilt:

$$\frac{1}{n}\mathcal{F}_{n,\omega^{-1}}(\vec{e}) = \vec{a}$$

$$\begin{aligned} P_{\vec{e}}(\omega^{-k}) &= \sum_{j=0}^{n-1} e_j \omega^{-kj} = \sum_{j=0}^{n-1} P_{\vec{a}}(\omega^j)\omega^{-kj} \\ &= \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} a_i \omega^{ij}\omega^{-kj} = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} \omega^{(i-k)j} = n a_k, \end{aligned}$$

denn nach Lemma 152 ist $\sum_{j=0}^{n-1} \omega^{(i-k)j} = 0$, falls $i \neq k$.

Im Fall $i = k$ gilt $\sum_{j=0}^{n-1} \omega^{(i-k)j} = n$. □

3.5.3 Berechnung der inversen diskreten Fouriertransformation

Satz 151

Es gilt

$$\mathcal{F}_{n,\omega}^{-1} = \frac{1}{n}\mathcal{F}_{n,\omega^{-1}}.$$

Bemerkung: ω^{-1} ist ebenso eine primitive n-te Einheitswurzel.
Zum Beweis von Satz 151 benötigen wir folgendes Lemma:

Lemma 152

Ist ω eine primitive n-te Einheitswurzel, so gilt

$$\sum_{j=0}^{n-1} \omega^{kj} = 0$$

für alle $k = 1, \ldots, n-1$.

Beweis:

Für jedes $a \in \mathbb{C}$, $a \neq 1$, gilt $\sum_{j=0}^{n-1} a^j = \frac{a^n-1}{a-1}$. Speziell für $a = \omega^k$ ist $a^n = \omega^{kn} = 1$, $(k = 1, \ldots, n-1)$. □

Nun zum Beweis von Satz 151.

Beweis:

Sei $\vec{e} = \mathcal{F}_{n,\omega}(\vec{a}) = (e_0, \ldots, e_{n-1})$. Wir zeigen, dass gilt:

$$\frac{1}{n}\mathcal{F}_{n,\omega^{-1}}(\vec{e}) = \vec{a}$$

$$\begin{aligned} P_{\vec{e}}(\omega^{-k}) &= \sum_{j=0}^{n-1} e_j \omega^{-kj} = \sum_{j=0}^{n-1} P_{\vec{a}}(\omega^j)\omega^{-kj} \\ &= \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} a_i \omega^{ij}\omega^{-kj} = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} \omega^{(i-k)j} = n a_k, \end{aligned}$$

denn nach Lemma 152 ist $\sum_{j=0}^{n-1} \omega^{(i-k)j} = 0$, falls $i \neq k$.

Im Fall $i = k$ gilt $\sum_{j=0}^{n-1} \omega^{(i-k)j} = n$. □

3.6 Restklassen in Polynomringen

3.6.1 Einführung und Definitionen

Der Begriff der Restklasse stammt ursprünglich aus der Teilbarkeitslehre in $\mathbb{Z}$; $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring).

Definition 153
Sei n eine fest gewählte ganze Zahl $\neq 0$. Für jedes $\ell \in \mathbb{Z}$ heißt die Menge

$$[\ell]_n := \{m \in \mathbb{Z} : m - \ell \text{ ist durch } n \text{ teilbar}\}$$

die Restklasse von ℓ modulo n.

Beweis:
Für jedes $a \in \mathbb{C}$, $a \neq 1$, gilt $\sum_{j=0}^{n-1} a^j = \frac{a^n - 1}{a-1}$. Speziell für $a = \omega^k$ ist $a^n = \omega^{kn} = 1$, $(k = 1, \ldots, n-1)$. □

Nun zum Beweis von Satz 151.

Beweis:
Sei $\vec{e} = \mathcal{F}_{n,\omega}(\vec{a}) = (e_0, \ldots, e_{n-1})$. Wir zeigen, dass gilt:

$$\frac{1}{n}\mathcal{F}_{n,\omega^{-1}}(\vec{e}) = \vec{a}$$

$$\begin{aligned} P_{\vec{e}}(\omega^{-k}) &= \sum_{j=0}^{n-1} e_j \omega^{-kj} = \sum_{j=0}^{n-1} P_{\vec{a}}(\omega^j)\omega^{-kj} \\ &= \sum_{j=0}^{n-1}\sum_{i=0}^{n-1} a_i \omega^{ij}\omega^{-kj} = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} \omega^{(i-k)j} = n a_k, \end{aligned}$$

denn nach Lemma 152 ist $\sum_{j=0}^{n-1} \omega^{(i-k)j} = 0$, falls $i \neq k$.
Im Fall $i = k$ gilt $\sum_{j=0}^{n-1} \omega^{(i-k)j} = n$. □

3.6 Restklassen in Polynomringen

3.6.1 Einführung und Definitionen

Der Begriff der Restklasse stammt ursprünglich aus der Teilbarkeitslehre in $\mathbb{Z}$; $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring).

Definition 153
Sei n eine fest gewählte ganze Zahl $\neq 0$. Für jedes $\ell \in \mathbb{Z}$ heißt die Menge

$$[\ell]_n := \{m \in \mathbb{Z} : m - \ell \text{ ist durch } n \text{ teilbar}\}$$

die Restklasse von ℓ modulo n.

3.6 Restklassen in Polynomringen

3.6.1 Einführung und Definitionen

Der Begriff der Restklasse stammt ursprünglich aus der Teilbarkeitslehre in $\mathbb{Z}$; $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring).

Definition 153
Sei n eine fest gewählte ganze Zahl $\neq 0$. Für jedes $\ell \in \mathbb{Z}$ heißt die Menge

$$[\ell]_n := \{m \in \mathbb{Z} : m - \ell \text{ ist durch } n \text{ teilbar}\}$$

die Restklasse von ℓ modulo n.

Bemerkungen

1. Für $\ell, m \in \mathbb{Z}$ gilt:
$$m \in [\ell]_n \iff m \bmod n = \ell \bmod n\,.$$
Gilt $m \in [\ell]_n$, so schreibt man auch $m \equiv \ell \bmod n$ oder $m = \ell \bmod n$ und spricht „m kongruent ℓ modulo n".
2. Es gilt $[\ell]_n = \{\ell + kn : k \in \mathbb{Z}\} =: \ell + n\mathbb{Z} =: \ell + (n)$.
3. Da es genau n verschiedene Reste $0, 1, \ldots, n-1$ gibt, gibt es auch genau n verschiedene Restklassen $[0]_n, [1]_n, \ldots, [n-1]_n$.

Bemerkungen

4. Kongruenz modulo n definiert auf $\mathbb{Z}$ eine Äquivalenzrelation $\sim_n$: $m \sim_n \ell :\iff n$ teilt $m - \ell$, und $[\ell]_n$ ist die Äquivalenzklasse von ℓ.
5. Auf der Menge aller Restklassen $[\ell]_n$ kann man Addition und Multiplikation wie folgt definieren
$$[\ell]_n +_n [m]_n := [\ell + m]_n, \qquad [\ell]_n \cdot_n [m]_n := [\ell \cdot m]_n,$$
und erhält einen kommutativen Ring; er heißt der Restklassenring $\mathbb{Z}$ modulo n und wird mit $\mathbb{Z}/(n)$ oder $\mathbb{Z}/n\mathbb{Z}$ oder $\mathbb{Z}_n$ bezeichnet.
6. Die Abbildung $(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +_n, \cdot_n)$, $\ell \mapsto$ „Rest der Division von ℓ durch n" ist ein Ringhomomorphismus.

Bemerkungen

4. Kongruenz modulo n definiert auf $\mathbb{Z}$ eine Äquivalenzrelation $\sim_n$: $m \sim_n \ell :\iff n$ teilt $m - \ell$, und $[\ell]_n$ ist die Äquivalenzklasse von ℓ.
5. Auf der Menge aller Restklassen $[\ell]_n$ kann man Addition und Multiplikation wie folgt definieren
$$[\ell]_n +_n [m]_n := [\ell + m]_n, \qquad [\ell]_n \cdot_n [m]_n := [\ell \cdot m]_n,$$
und erhält einen kommutativen Ring; er heißt der Restklassenring $\mathbb{Z}$ modulo n und wird mit $\mathbb{Z}/(n)$ oder $\mathbb{Z}/n\mathbb{Z}$ oder $\mathbb{Z}_n$ bezeichnet.
6. Die Abbildung $(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +_n, \cdot_n)$, $\ell \mapsto$ „Rest der Division von ℓ durch n" ist ein Ringhomomorphismus.

Bemerkungen

4. Kongruenz modulo n definiert auf $\mathbb{Z}$ eine Äquivalenzrelation $\sim_n$: $m \sim_n \ell :\iff n$ teilt $m - \ell$, und $[\ell]_n$ ist die Äquivalenzklasse von ℓ.
5. Auf der Menge aller Restklassen $[\ell]_n$ kann man Addition und Multiplikation wie folgt definieren
$$[\ell]_n +_n [m]_n := [\ell + m]_n, \qquad [\ell]_n \cdot_n [m]_n := [\ell \cdot m]_n,$$
und erhält einen kommutativen Ring; er heißt der Restklassenring $\mathbb{Z}$ modulo n und wird mit $\mathbb{Z}/(n)$ oder $\mathbb{Z}/n\mathbb{Z}$ oder $\mathbb{Z}_n$ bezeichnet.
6. Die Abbildung $(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +_n, \cdot_n)$, $\ell \mapsto$ „Rest der Division von ℓ durch n" ist ein Ringhomomorphismus.

Restklassen können auch im Polynomring $K[x]$ (K ein Körper) gebildet werden.

Definition 154

Sei $g \in K[x]$ ein Polynom, $\operatorname{grad}(g) \geq 1$. Für jedes $f \in K[x]$ heißt die Menge

$$[f]_g := \{h \in K[x] : h - f \text{ ist durch } g \text{ teilbar}\}$$

die Restklasse von f modulo g.

Bemerkung: Wie in $\mathbb{Z}$ gilt nun auch im Polynomring $K[x]$: