WS 2005/06

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2005WS/ds/index.html.de

6. Dezember 2005

Satz 147

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

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

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

3.5.3 Berechnung der inversen diskreten Fouriertransformation

Satz 148

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 148 benötigen wir folgendes Lemma:

Lemma 149

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 148.

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 149 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 $\mathbb{Z}$; ($\mathbb{Z} = (\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring).

Definition 150

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 $m \equiv \ell \bmod n$ 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

$$[\ell]_n + [m]_n := [\ell + m]_n, \qquad [\ell]_n \cdot [m]_n := [\ell \cdot m]_n,$$

   und erhält einen kommutativen Ring; er heißt der Restklassenring $\mathbb{Z}$ modulo n und wird mit $\mathbb{Z}/(n)$, oder $\mathbb{Z}/n\mathbb{Z}$ bezeichnet.
6. Die Abbildung $(\mathbb{Z}/(n), +, \cdot) \to (\mathbb{Z}_n, +_n, \cdot_n)$, $[\ell]_n \mapsto$ „Rest der Division von ℓ durch n“ ist ein Ringisomorphismus.

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

Definition 151

Sei $g \in K[x]$ ein Polynom, $\text{grad}(g) \geq 1$. 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 $K[x]$:

1. $h \in [f]_g \iff h$ und f haben bei Polynomdivision durch g denselben Rest.
2. $[f]_g = \{f + hg \ : \ h \in K[x]\} =: f + (g)$ mit $(g) := \{hg : h \in K[x]\} =$ Menge aller Polynome, die durch g teilbar sind.

3. „Kongruenz modulo g“ definiert auf $K[x]$ eine Äquivalenzrelation $\sim_g$: $h \sim_g f \iff h - f$ ist durch g teilbar, und $[f]_g$ ist die Äquivalenzklasse von f.
4. Auf der Menge aller Restklassen $[f]_g$ kann man Addition und Multiplikation wie folgt definieren

$$[f]_g + [h]_g := [f + h]_g, \qquad [f]_g \cdot [h]_g := [f \cdot h]_g,$$

und erhält einen kommutativen Ring; er heißt der Restklassenring $K[x]$ modulo g und wird mit $K[x]/(g)$ bezeichnet.

3.6.2 Eigenschaften von Restklassenringen

Teilt man Polynome durch ein fest gewähltes Polynom g, $\mathrm{grad}(g) \geq 1$, so treten als Reste sämtliche Polynome vom Grad $< d = \mathrm{grad}(g)$ auf. Deshalb setzen wir

$$K[x]_d := \{h \in K[x] : \mathrm{grad}(h) < d\},$$

und definieren auf $K[x]_d$ Addition $+_g$ und Multiplikation $\cdot_g$ wie folgt:

Mit $Rem(f)$ bezeichnen wir den Rest der Polynomdivision von f durch g.

$$f +_g h := f + h, \qquad f \cdot_g h := Rem(f \cdot h).$$

Man prüft leicht nach, dass $(K[x]_d, +_g, \cdot_g)$ ein kommutativer Ring ist.

Satz 152

Sei $g \in K[x]$ ein Polynom, $d = \mathrm{grad}(g) \geq 1$. Dann ist die Abbildung

$$(K[x]/(g), +, \cdot) \to (K[x]_d, +_g, \cdot_g), \quad [f]_g \mapsto Rem(f)$$

ein Ringisomorphismus, die Umkehrabbildung ist gegeben durch $r \mapsto [r]_g$.

Beweis:

Es gilt

1. $$[f]_g = [0]_g \iff g|f \iff Rem(f) = 0$$

2. $$[f]_g + [h]_g = [f+h]_g \mapsto Rem(f+h) = Rem(f) + Rem(h) = Rem(f) +_g Rem(h)$$

3. $$[f]_g \cdot [h]_g = [f \cdot h]_g \mapsto Rem(f \cdot h) = Rem(Rem(f) \cdot Rem(h)) = Rem(f) \cdot_g Rem(h).$$

Aus (1) - (3) folgt, dass obige Abbildung wohldefiniert, injektiv und ein Ringhomomorphismus ist; sie ist auch surjektiv, denn für $f \in K[x]_d$ ist $Rem(f) = f$. □

Satz 153

Sei K ein Körper mit n Elementen, und sei $g \in K[x]$, $d = \mathrm{grad}(g) \geq 1$. Dann besitzt $K[x]/(g)$ genau n^d Elemente.

Beweis:

Nach Satz 152 ist $|K[x]/(g)| = |K[x]_d|$, und offensichtlich gilt $|K[x]_d| = n^d$. □

Definition 154

Ein Polynom $g \in K[x]$ heißt irreduzibel, falls $\mathrm{grad}(g) \geq 1$ gilt und aus $g = g_1 \cdot g_2$ mit $g_1, g_2 \in K[x]$ stets $\mathrm{grad}(g_1) = 0$ oder $\mathrm{grad}(g_2) = 0$ folgt; ansonsten heißt g reduzibel.