WS 2010/11

Zentralübung zur Vorlesung Diskrete Strukturen

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2010WS/ds/uebung/

15. Dezember 2010

ZÜ VIII

Übersicht:

1. Übungsbetrieb: Weihnachtswoche und Termine
2. Thema: Fouriertransformation: VA 3, TA 3, Blatt 8.

1. Übungsbetrieb Weihnachtswoche und Termine

1.1 Weihnachtswoche

Nächste Woche findet normaler Übungsbetrieb bis einschließlich Donnerstag, den 23.12.2010 statt.

1.2 Termine

Der Abgabetermin für Hausaufgaben von Blatt 10 ist
Dienstag, den 11.1.2011.

Die Tutoraufgaben von Blatt 10 werden in den Übungen von Montag, den 10.1.2011 bis Donnerstag, den 14.1.2011 bearbeitet.

Die Ergebnisse der Klausur werden per Codeliste noch vor Weihnachten auf der Übungswebseite stehen.

Klausureinsicht wird Mitte Januar sein.
Der Termin wird auf der Übungswebseite bekanntgegeben werden.

Fragen?

2. Thema: Fouriertransformation

2.1 VA 3, Blatt 8

Wir betrachten den Körper $\mathbb{C}$ der komplexen Zahlen.
Es sei $i \in \mathbb{C}$ mit $i^2 = -1$.

Zeigen Sie, dass für jedes $n \in \mathbb{N}$ die komplexe Zahl $e^{\frac{2\pi i}{n}}$ eine multiplikative Untergruppe W_n von $\mathbb{C}$ erzeugt, die isomorph ist zu $\mathbb{Z}_n$.

Stellen Sie W_n in der Gaußchen Zahlenebene dar und machen Sie sich klar, was in Ihrer Darstellung die Multiplikation in W_n bedeutet.

Lösung:

$\mathbb{C}$ ist zusammen mit der Multiplikation keine Gruppe.

Gleichwohl gibt es Teilmengen von $\mathbb{C}$, die zusammen mit der Multiplikation eine Gruppe bilden. Wir sprechen in diesem Fall von multiplikativen Untergruppen von $\mathbb{C}$.

Eine maximale multiplikative Untergruppe in $\mathbb{C}$ ist $\mathbb{C} \setminus \{0\}$.

Trivialerweise bildet auch $\{0\}$ zusammen mit der Multiplikation eine Untergruppe.

Eine multiplikative Untergruppe von $\mathbb{C}$,
die irgendein von 0 verschiedenes Element enthält,
kann die 0 nicht enthalten.

Wegen $e^{\frac{2\pi i}{n}} \neq 0$ sind deshalb die

von $e^{\frac{2\pi i}{n}}$ erzeugten multiplikativen Untergruppen

gleichzeitig Untergruppen der multiplikativen Gruppe $\mathbb{C} \setminus \{0\}$.

Sei

$$W_n = \{(e^{\frac{2\pi i}{n}})^k\,;\, k \in \mathbb{Z}\} \subseteq \mathbb{C} \setminus \{0\}\,.$$

W_n ist die von $e^{\frac{2\pi i}{n}}$ erzeugte (zyklische) multiplikative Untergruppe von $\mathbb{C} \setminus \{0\}$.

Nun gilt

$$W_n = \{e^{\frac{2\pi i}{n}}, e^{\frac{2(2\pi i)}{n}}, \ldots, e^{\frac{k(2\pi i)}{n}}, \ldots, e^{\frac{n(2\pi i)}{n}} = 1\}\,.$$

Die Abbildung

$$\phi(e^{\frac{k(2\pi i)}{n}}) = k \bmod n$$

ist eine Isomorphie von W_n auf $\mathbb{Z}_n$ wegen

$$\begin{aligned}
\phi(x \cdot y) &= \phi(e^{\frac{k_x(2\pi i)}{n}} e^{\frac{k_y(2\pi i)}{n}}) \\
&= \phi(e^{\frac{(k_x+k_y)(2\pi i)}{n}}) \\
&= (k_x + k_y) \bmod n \\
&= \phi(x) +_n \phi(y)\,.
\end{aligned}$$

In der Gaußchen Zahlenebene liegen die Elemente von W_n auf einem Kreis von Punkten mit Abstand 1 zum Nullpunkt.

Die Multiplikation einer komplexen Zahl z mit $e^{\frac{k(2\pi i)}{n}}$

$$z \cdot e^{\frac{k(2\pi i)}{n}}$$

bedeutet dann eine Drehung des Vektors z um den Winkel $\frac{k(2\pi)}{n}$ im Gegenuhrzeigersinn (bei positivem k).

2.2 TA 3, Blatt 8

1. Sei $p(x) \in \mathbb{C}[x]$ ein Polynom vom Grad $n-1$ mit den Koeffizienten $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$, d. h.

$$p(x) = P_{\vec{a}}(x)\,.$$

Wir betrachten speziell
$n = 8$, $\vec{a} = (1, 1, 1, 1, 1, 1, 1, 1)$ und $\omega = e^{\frac{2\pi i}{8}}$.

Berechnen Sie die Fouriertransformierte

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

i) Durch Ausführung des Divide-and-Conquer Algorithmus `DFT`$(\vec{a}, \omega)$.

ii) Durch direkte Berechnung unter Ausnutzung der Formel

$$x^n - 1 = (x^{n-1} + \ldots + x^2 + x + 1)(x-1)\,.$$

Lösung:

Wir bestimmen die diskrete Fouriertransformierte des Polynoms $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7$ mit $\omega = \frac{1}{\sqrt{2}}(1+i)$ als Einheitswurzel.

i) Ausführung $\texttt{DFT}(\vec{a}, \omega)$:

Nach dem rekursiven Verfahren der Vorlesung ist es dazu erforderlich die Fouriertransformierten zu den Polynomen der geraden und ungeraden Koeffizienten mit ω^2 zu bestimmen.

In diesem Fall haben diese Polynome beide genau die Koeffizienten $(1, 1, 1, 1)$ und die Form $1 + x + x^2 + x^3$ und $\omega' = \omega^2 = i$.

Im nächsten rekursiven Aufruf bestimmt man die

Fouriertransformierte von $1 + x$ mit $\omega'' = \omega^4 = -1$ und zuletzt die

Fouriertransformierte von 1 mit $\omega''' = \omega^8 = 1$.

Es gilt

$DFT((1), \omega''' = 1) = (e_0)$

mit $e_0 = 1$ und dieser Wert ist dann auch das c_0 und das d_0 für den nächsten Schritt.

Es folgt

$DFT((1,1), \omega'' = -1) = (e'_0, e'_1)$

mit

$$\begin{aligned} e'_0 &= c_0 + (\omega'')^0 d_0 = 1 + 1 = 2 \quad \text{und} \\ e'_1 &= c_0 + (\omega'')^1 d_0 = 1 - 1 = 0\,. \end{aligned}$$

Damit kennen wir auch die c's und d's für den nächsten Schritt, nämlich

$c'_0 = d'_0 = e'_0 = 2$ und
$c'_1 = d'_1 = e'_1 = 0$.

Im folgenden eliminieren wir sofort die c und d's.

Im nächsten Rekursionsschritt ergibt sich

$DFT((1,1,1,1), \omega' = i) = (e''_0, e''_1, e''_2, e''_3)$

mit

$$\begin{aligned}
e''_0 &= e'_0 + (\omega')^0 e'_0 = 2 + 2 = 4 \\
e''_1 &= e'_1 + (\omega')^1 e'_1 = 0 + 0i = 0 \\
e''_2 &= e'_0 + (\omega')^2 e'_0 = 2 - 2 = 0 \\
e''_3 &= e'_1 + (\omega')^3 e'_1 = 0 - 0i = 0
\end{aligned}$$

Wieder können wir die c's und d's für den nächsten Schritt wie folgt bestimmen:

$$c'_0 = d'_0 = e'_0 = 4,$$
$$c'_1 = d'_1 = e'_1 = 0,$$
$$c'_2 = d'_2 = e'_2 = 0 \quad \text{und}$$
$$c'_3 = d'_3 = e'_3 = 0.$$

Letzter Schritt:

$DFT((1,1,1,1,1,1,1,1), \omega = \frac{1}{\sqrt{2}}(1+i)) = (e_0''', \ldots, e_7''')$

mit

$$\begin{aligned}
e_0''' &= e_0'' + \omega^0 e_0'' = 4 + 4 = 8 \\
e_1''' &= e_1'' + \omega^1 e_1'' = 0 + 0\omega = 0 \\
e_2''' &= e_2'' + \omega^2 e_2'' = 0 + 0i = 0 \\
e_3''' &= e_3'' + \omega^3 e_3'' = 0 + 0\omega i = 0 \\
e_4''' &= e_0'' + \omega^4 e_0'' = 4 - 4 = 0 \\
e_5''' &= e_1'' + \omega^5 e_1'' = 0 - 0\omega = 0 \\
e_6''' &= e_2'' + \omega^6 e_2'' = 0 - 0i = 0 \\
e_7''' &= e_3'' + \omega^7 e_3'' = 0 - 0\omega i = 0
\end{aligned}$$

Ergebnis: $DFT((1,1,1,1,1,1,1,1), \omega) = (8,0,0,0,0,0,0,0)$.

ii) Direkte Berechnung von $DFT((1,1,1,1,1,1,1,1),\omega)$ unter Ausnutzung der Formel

$$x^n - 1 = (x^{n-1} + \ldots + x^2 + x + 1)(x-1)\,.$$

Am einfachsten ist es, Lemma 152 der Vorlesung zu benutzen. Es gibt aber nun die folgende Alternative.

Wir setzen
$p(x) = x^8 - 1$,
$q(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ und
$r(x) = x - 1$.

Man kann leicht nachrechnen, daß $p(x) = q(x)r(x)$.

Wir setzen

$DFT(\vec{q},\omega) = DFT((1,1,1,1,1,1,1,1),\omega) = (e_0''',\dots,e_7''')$ und
$DFT(\vec{r},\omega) = DFT((-1,1,0,0,0,0,0,0),\omega) = (\zeta_0,\dots,\zeta_7)$.

Da die Werte der diskreten Fouriertransformierten genau die Stützstellen der Polynome an den Potenzen der Einheitswurzeln sind, gilt:

$$e_k'''\zeta_k = q(\omega^k)r(\omega^k) = p(\omega^k) = (\omega^k)^8 - 1 = 0$$

und

$$\zeta_k = \omega^k - 1 = e^{k\cdot\frac{2\pi i}{8}} - 1\,.$$

Für $k \neq 0$ ist damit $\zeta_k \neq 0$ und man kann die Gleichung nach e_k''' auflösen, wobei sich $e_k''' = 0$ ergibt.

Für $k = 0$ ist $e^{k\frac{2\pi i}{8}} = 1$

und einfaches Einsetzen ergibt
$e_0''' = q(1) = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 = 8$.