WS 2012/13

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

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

5. Dezember 2012

ZÜ VII

Übersicht:
Bitte beachten:
Die Zentralübung am Mittwoch, den 12.12.2012 entfällt.

1. Übungsbetrieb:	Mittelklausur am 15. Dezember Nachträgliche Anmeldung Fragen?
2. Wiederholung:	Äquivalenz, Kongruenz, Berechnung von Inversen, Nullteilerfreiheit
3. Thema:	Schnelle Fouriertransformation
4. Vorbereitung:	auf TA Blatt 8: Komplexe Zahlen (VA1) FFT (VA2)

1. Übungsbetrieb: Mittelklausur am 15. Dezember

1.1 Nachträgliche Anmeldung

Eine Anmeldung für die Midterm
erfolgt über TUMonline oder in Sonderfällen persönlich am Infopoint.

Diejenigen Teilnehmer,
die sich nicht über TUMonline angemeldet hatten,
besorgen ihre Anmeldung bitte nachträglich
spätestens bis zum 18.12.2012
persönlich im Infopoint.

Grundsätzlich bei Nichtanmeldung:
Bitte im Hörsaal bei der Aufsicht melden!

Achtung:

Bei Nichtanmeldung kann nicht garantiert werden, dass Sitzplatz und Klausurunterlagen zur Verfügung stehen!

Alle Teilnehmer der Klausuren müssen sich bei der Ausweiskontrolle im Hörsaal ausweisen können!!

1.2 Fragen

?

2. Wiederholungen

2.1 Äquivalenzrelationen

Äquivalenzrelation:
Eine binäre Relation $R \subseteq M \times M$, die reflexiv, transitiv und symmetrisch ist.

Äquivalenzklasse $[x]_R$ einer Äquivalenzrelation R, die x enthält:
Die Menge A aller y, die in Relation $(y, x) \in R$ sind, i.Z. $A = [x]_R$.

Partition:
Menge aller Äquivalenzklassen einer Äquivalenzrelation
$=$
,,Überdeckung einer Menge durch
eine Menge von disjunkten Mengen"

2.2 Kongruenzrelation

Eine Äquivalenzrelation über der Trägermenge einer Algebra nennt man Kongruenzrelation, wenn die Relation verträglich ist mit den Operationen.

Z.B.:

Seien $A = (S, \circ)$ eine Algebra
und $\sim$ eine Äquivalenzrelation über S.

Dann betrachten wir die Abbildung $x \to [x]_\sim$, die jedem Element $x \in S$ die Äquivalenzklasse $[x]_\sim$ zuordnet.

$\sim$ ist eine Kongruenzelation bezüglich $\circ$, falls für alle $x_1, x_2, y_1, y_2 \in S$ gilt

$$x_1 \sim x_2 \text{ und } y_1 \sim y_2 \implies [x_1 \circ y_1]_\sim = [x_2 \circ y_2]_\sim .$$

Beispiel: Die Äquivalenz modulo n über ganzen Zahlen.

Die Definition $[x]_n + [y]_n := [x + y]_n$ ist wohldefiniert, da die Äquivalenz modulo n eine Kongruenzrelation ist.

2.3 Berechnung der multiplikatien Inversen

Aufgabe:

Berechnen Sie die multiplikative Inverse von 36 im Körper $\mathbb{Z}_{53}$ der ganzen Zahlen modulo 53.

Lösung:

Man berechnet mit Hilfe des erweiterten Euklidischen Algorithmus ganze Zahlen a, b, so dass gilt

$$a \cdot 53 + b \cdot 36 = 1\,.$$

Dann ist $b \bmod 53$ das gesuchte Inverse von 36.

Wir führen den Euklidischen Algorithmus aus wie folgt.

$$
\begin{aligned}
r_0 &= 53\,, \\
r_1 &= 36\,, \\
r_2 &= 53 \bmod 36 && = r_0 - 1 \cdot r_1 && = 17\,, \\
r_3 &= 36 \bmod 17 && = r_1 - 2 \cdot r_2 && = 2\,, \\
r_4 &= 17 \bmod 2 && = r_2 - 8 \cdot r_3 && = 1\,.
\end{aligned}
$$

Es folgt

$$\mathrm{ggT}(53, 36) = 1\,.$$

Nun führen wir die Erweiterung des Euklidischen Algorithmus z.B. in der Form der Rückeinsetzung aus.

$$
\begin{aligned}
1 &= r_4 \\
&= r_2 - 8r_3 && = r_2 - 8(r_1 - 2r_2) \\
&= -8r_1 + 17r_2 && = -8r_1 + 17(r_0 - r_1) \\
&= 17r_0 - 25r_1 \,.
\end{aligned}
$$

Es folgt $17r_0 - 25r_1 = 1$, mithin, für $a = 17$ und $b = -25$,

$$a \cdot 53 + b \cdot 36 = 1 \,.$$

Das gesuchte Inverse von 36 ist $-25 \bmod 53 = 28$.

2.4 Nullteilerfreiheit

Ein nullteilerfreier Ring ist nicht notwendigerweise ein Körper.

Beweis:

Der Ring der ganzen Zahlen ist nullteilerfrei und trotzdem kein Körper.

Allerdings kann man $\mathbb{Z}$ in den Quotientenkörper $\mathbb{Q}$ einbetten.

Das kann man auf Polynomringe verallgemeinern.

3. Thema: Fourier Transformation

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.

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

Frage:
Wie ist die (diskrete) Fouriertransformierte $\mathcal{F}_{n,\omega}(\vec{a})$ definiert?

Antwort:
$\mathcal{F}_{n,\omega}(\vec{a})$ ist der Vektor der Werte des Polynoms p an den n „Stützstellen" $1, \omega, \omega^2, \ldots, \omega^{n-1}$.

Formal:

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

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

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

Dann gilt:

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

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

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

für $i = 0, \ldots, \frac{n}{2} - 1$.

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

Frage:
Wodurch wird bei der Berechnung nach obigem Algorithmus Berechnungsaufwand eingespart?

Antwort:

Die Polynome $P_{\vec{a}_g}$ und $P_{\vec{a}_u}$ müssen nur an der Hälfte der Stützstellen berechnet werden.

Bei Quadratbildung aller ω^i wiederholen sich alle Werte der unteren Hälfte der Gaußschen Ebene.

4. Vorbereitung auf TA Blatt 8

4.1 VA 1, Komplexe Zahlen

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

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 $\mathbb{Z}_n$.

2. 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).

Eulersche e-Funktion:

$$e^{i\varphi} = \cos\varphi \ + \ i \cdot \sin\varphi\,.$$

4.2 VA 2, DFT

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

Berechnen Sie die (diskrete) Fouriertransformierte

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

durch Ausführung des Divide-and-Conquer Algorithmus $\texttt{DFT}(\vec{a}, \omega)$.

Lösung:

Wir bestimmen die diskrete Fouriertransformierte $\mathcal{F}_{8,\omega}(\vec{a})$ des Polynoms

$$P_{\vec{a}} = 2 + x + 2x^2 + x^3 + 2x^4 + x^5 + 2x^6 + x^7$$

mit $\omega = \frac{1}{\sqrt{2}}(1+i)$ als primitiver Einheitswurzel.

In der Ausführung von $\texttt{DFT}(\vec{a}, \omega)$ werden

im ersten rekursiven Aufruf die Fouriertransformierten

$\mathcal{F}_{4,\omega'}(\vec{a}_g)$ bzw. $\mathcal{F}_{4,\omega'}(\vec{a}_u)$ zu den Polynomen $P_{\vec{a}_g}$ bzw. $P_{\vec{a}_u}$

der geraden bzw. ungeraden Koeffizienten $\vec{a}_g$ bzw. $\vec{a}_u$ von p
mit $\omega' = \omega^2 = i$ als der primitiven Einheitswurzel
bestimmt,

d.h.,

es werden die Werte von $\vec{a}_g$ bzw. $\vec{a}_u$ an den Stützstellen
$1, \omega', \omega'^2, \omega'^3$, bestimmt.

Abschließend wird aus diesen Werten dann $\mathcal{F}_{8,\omega}(\vec{a})$ berechnet.

In dem vorliegenden Fall

$$P_{\vec{a}} = 2 + x + 2x^2 + x^3 + 2x^4 + x^5 + 2x^6 + x^7$$

haben diese Polynome $P_{\vec{a}_g}$ und $P_{\vec{a}_u}$
die Koeffizienten $(2, 2, 2, 2)$ bzw. $(1, 1, 1, 1)$ und die Form

$$P_{\vec{a}_g} = 2 + 2x + 2x^2 + 2x^3$$

bzw.

$$P_{\vec{a}_u} = 1 + x + x^2 + x^3\,.$$

Berechnung von $\mathcal{F}_{4,\omega'}(\vec{a}_u)$:

Wir nehmen an, dass uns der rekursive Aufruf für $\vec{a}_u = (1,1,1,1)$ die Zwischenergebnisse von TA 2.1(i), Blatt 8 liefert.

Danach gilt

$$\mathcal{F}_{4,\omega'}(\vec{a}_u) = \mathtt{DFT}((1,1,1,1),\omega') = (4,0,0,0)\,.$$

Berechnung von $\mathcal{F}_{4,\omega'}(\vec{a}_g)$:

Mit $\vec{a}_g = (2,2,2,2)$ werden die jeweils verdoppelten Zwischenergebnisse von vorhin berechnet. Danach gilt mit entsprechender Ausführung

$$\mathcal{F}_{4,\omega'}(\vec{a}_g) = \mathtt{DFT}((2,2,2,2),\omega') = (8,0,0,0)\,.$$

Berechnung von $\mathcal{F}_{8,\omega}(\vec{a})$:

Wir übernehmen die Bezeichnungsweisen von Lemma 149 der Vorlesung, d. h.

$$\begin{aligned}
\mathcal{F}_{4,\omega'}(\vec{a}_g) &= (c_0, c_1, c_2, c_3) = (8, 0, 0, 0)\,,\\
\mathcal{F}_{4,\omega'}(\vec{a}_u) &= (d_0, d_1, d_2, d_3) = (4, 0, 0, 0)\,,\\
\mathcal{F}_{8,\omega'}(\vec{a}) &= (e_0, e_1, e_2, e_3, e_4, e_5, e_6, e_7)\,.
\end{aligned}$$

und berechnen

$$
\begin{aligned}
e_0 &= c_0 + \omega^0 d_0 &&= 8 + 4 &&= 12\,,\\
e_1 &= c_1 + \omega^1 d_1 &&= 0 + 0\omega &&= 0\,,\\
e_2 &= c_2 + \omega^2 d_2 &&= 0 + 0i &&= 0\,,\\
e_3 &= c_3 + \omega^3 d_3 &&= 0 + 0\omega i &&= 0\,,
\end{aligned}
$$

$$
\begin{aligned}
e_4 &= c_0 + \omega^4 d_0 &&= 8 - 4 &&= 4\,,\\
e_5 &= c_1 + \omega^5 d_1 &&= 0 - 0\omega &&= 0\,,\\
e_6 &= c_2 + \omega^6 d_2 &&= 0 - 0i &&= 0\,,\\
e_7 &= c_3 + \omega^7 d_3 &&= 0 - 0\omega i &&= 0\,.
\end{aligned}
$$

Es gilt also

$$\texttt{DFT}((2,1,2,1,2,1,2,1),\omega) = (12,0,0,0,4,0,0,0)\,.$$