

# Musterlösungen zur Vorlesung Effiziente Algorithmen

Frank Wübbeling

19. Dezember 1995

*Achtung:* Die Lösungen enthalten alle nur Ansätze, die in einer korrekten Lösung genauer ausgearbeitet werden müssen!

## 1 Aufgabe 1:

Seien  $A, B$  komplexe  $(n, n)$ -Matrizen. Geben Sie einen Algorithmus an, der das Produkt  $AB$  in höchstens  $3n^3 + O(n^2)$  reellen Multiplikationen und Additionen berechnet.

Lösung:

Der Algorithmus zur schnellen Multiplikation komplexer Zahlen benötigt 3 reelle Multiplikationen. Da er Kommutativität nicht ausnutzt, ist er auch für die Multiplikation komplexer Matrizen anwendbar. Schulmethode zur Durchführung der MP komplexer Matrizen benötigt  $n^3$  komplexe MP, macht  $3n^3$  reelle MP. Seien die zu multiplizierenden Matrizen  $(A + Bi)$  und  $(C + Di)$  mit reellen Matrizen  $A, B, C$  und  $D$ .

$(A + Bi)(C + Di) = AC - BD + i(AD + BC)$ , und

$$(AD + BC) = A(C + D) + (-A + B)C$$

$$(AC - BD) = A(C + D) - (A + B)D$$

Bemerkung: Der Algorithmus benutzt keine Kommutativität und ist deshalb auch auf Matrizen (notfalls auch rekursiv) anwendbar. Für jede einzelne MatrixMP sind  $n^3$  ADD und  $n^3$  MP (reelle) notwendig, macht insgesamt  $3n^3$  ADD und MP.

## 2 Aufgabe 2:

Programmieraufgabe, Abgabe 28.10.1994.

- Schreiben Sie ein Programm, das zwei Zahlen der Länge  $n$  mit  $n^2 + O(n)$  Rechenoperationen und  $2n + O(1)$  Speicherplätzen multipliziert.
- Schreiben Sie ein Programm zur Karatsuba-Multiplikation.
- Stellen Sie fest, ab welchem  $n$  (b) schneller ist als (a).

Lösung:

Siehe Anhang. Lösung in C++. Das Modul stellt einen komplexen Datentyp `longnum` zur Verfügung. Auf dem Datentyp sind Addition, Subtraktion, Konversion von `integer`, Multiplikation und schnelle Multiplikation definiert. Die Grenze, ab der sich eine schnelle Multiplikation lohnt, liegt ungefähr bei 16 (d.h., für Längen unter 16 sollten normale Multiplikationen durchgeführt werden).

## 3 Aufgabe 3:

Zeigen Sie, daß man  $(n, n)$ -Matrizen für gerades  $n$  mit  $\frac{1}{2}n^3 + n^2$  Multiplikationen und  $\frac{3}{2}n^3 + 2n^2 - 2n$  Additionen multiplizieren kann.

Lösung:

Gesucht ist  $c_{i,j} = \sum_l a_{i,l} b_{l,j}$ . Sei  $m = \frac{n}{2}$ . Dann gilt

$$\sum_{l=1}^m (a_{i,l} + b_{l+m,j})(a_{i,l+m} + b_{l,j}) = c_{i,j} + \sum_{l=1}^m (a_{i,l} a_{i,l+m} + b_{l,j} b_{l+m,j})$$

Die Berechnung der linken Seite benötigt  $m$  MP und  $n$  ADD. Die rechte Seite benötigt  $n$  MP und  $m+1$  ADD. Die linke Seite muß  $n^2$ -Mal berechnet werden, macht  $mn^2$  MP. Die rechte Seite muß  $n$  mal berechnet werden (die Produkte sind entweder unabhängig von  $j$  oder  $i$ , macht  $n^2$  MP. Weiter kommen von links  $n^3$  ADD, von rechts  $mn^2$  ADD.

Bemerkung: Der Algorithmus nutzt die Kommutativität des Körpers aus und ist deshalb nicht rekursiv anwendbar.

Die Lösung findet sich bei Knuth, der den Algorithmus nach Winograd zitiert (“... ingenious...”)

## 4 Aufgabe 4:

Zeigen Sie, daß eine irreduzible Darstellung einer abelschen Gruppe den Grad 1 hat.

Lösung:

Sei  $\rho$  eine Darstellung. Sei  $A \in \rho(G)$  nicht die Identität oder ein Vielfaches davon. Dann besitzt  $A$  einen nichttrivialen Eigenraum  $E$  zu einem Eigenwert  $\lambda$ , denn das charakteristische Polynom besitzt über den komplexen Zahlen mindestens eine Nullstelle. Sei  $B \in \rho(G)$ .

$$A \cdot (BE) = B \cdot (AE) = \lambda BE,$$

also ist  $BE \subset E$ .  $E$  ist invarianter Teilraum von  $B$  und  $\rho$  ist reduzibel.

Die erste Lösung wiederholt noch einmal den Beweis zum Lemma von Schur. Einfacher gilt: Sei  $\rho$  eine irreduzible Darstellung. Dann gilt

$$\rho(s)\rho(t) = \rho(st) = \rho(ts) = \rho(t)\rho(s).$$

Also ist nach dem Lemma von Schur  $\rho(s) = \lambda_s I$ . Diese lineare Abbildung läßt jeden eindimensionalen Unterraum invariant. Falls  $\rho$  invariant, so muß gelten daß jeder eindimensionale Unterraum schon der ganze Raum ist, also ist  $\rho$  eindimensional.

## 5 Aufgabe 5:

Sei  $G$  eine Gruppe,  $H$  eine Untergruppe von  $G$  und  $\rho$  eine Darstellung von  $G$  in  $V$ .

- (a) Zeigen Sie, daß  $\sigma := \text{Rest}_H(\rho)$  (die Restriktion von  $\rho$  auf  $H$ ) eine Darstellung von  $H$  in  $V$  ist.
- (b) Zeigen Sie: Falls  $\sigma$  irreduzibel ist, so ist auch  $\rho$  irreduzibel.
- (c) Geben Sie ein Beispiel dafür an, daß  $\sigma$  für ein irreduzibles  $\rho$  reduzibel sein kann.

Lösung:

- (a) klar.
- (b) Falls es keinen Unterraum gibt, der unter den Transformationen aus  $\sigma$  invariant bleibt, so gibt es auch keinen, der unter den Transformationen aus  $\rho$  invariant bleibt. Die Transformationen aus  $\sigma$  sind in denen aus  $\rho$  enthalten.
- (c) Die Diedergruppe besitzt eine irreduzible Darstellung der Ordnung 2 und eine kommutative Untergruppe der Ordnung  $n$ . Nach Aufgabe 4 ist die Darstellung auf dieser Untergruppe reduzibel.

## 6 Aufgabe 6:

Sei  $G$  eine endliche Gruppe und  $H$  ein Normalteiler von  $G$  vom Index  $r$ .  $G = s_1H \cup \dots \cup s_rH$  sei die zugehörige Nebenklassenzerlegung von  $G$ . Dann gibt es zu jedem  $g \in G$  eine Permutation  $\pi(g) \in S_r$  mit  $gs_l \in s_{\pi(g)l}H$ .

Zeigen Sie:

(a)

$$\pi(g_1g_2) = \pi(g_1)\pi(g_2).$$

(b) Ist  $\sigma$  eine Darstellung von  $H$  in dem endlichdimensionalen komplexen Vektorraum  $V$  und für  $l = 1, \dots, r$

$$\rho_l(g) = \sigma(s_{\pi(g)l}^{-1}gs_l), \quad g \in G,$$

so gilt

$$\rho_l(g_1g_2) = \rho_{\pi(g_2)l}(g_1)\rho_l(g_2).$$

(c) Die Abbildung  $\rho : G \mapsto GL(V^r)$ , die für  $u = (u_1, \dots, u_r)^t \in V^r$  definiert ist durch

$$(\rho(g) \cdot u)_l = \rho_{\pi(g)^{-1}l}(g)u_{\pi(g)^{-1}l}, \quad l = 1, \dots, r,$$

ist eine Darstellung von  $G$  in  $V^r$ .  $\rho$  heißt die von  $\sigma$  induzierte Darstellung.

Lösung:

(a)

$$(g_1g_2)s_l = g_1(g_2s_l) \in g_1s_{\pi(g_2)l}H = s_{\pi(g_1)\pi(g_2)l}H.$$

(b)

$$\begin{aligned} \rho_{\pi(g_2)l}(g_1)\rho_l(g_2) &= \sigma(s_{\pi(g_1)\pi(g_2)l}^{-1}g_1s_{\pi(g_2)l})\sigma(s_{\pi(g_2)l}^{-1}g_2s_l) \\ &= \sigma(s_{\pi(g_1)\pi(g_2)l}^{-1}g_1g_2s_l) \\ &= \rho_l(g_1g_2) \end{aligned}$$

(c)

$$\begin{aligned} (\rho(g_1g_2) \cdot u)_l &= \rho_{\pi(g_1g_2)^{-1}l}(g_1g_2)u_{\pi(g_1g_2)^{-1}l} \\ &= \rho_{\pi(g_2)\pi(g_1g_2)^{-1}l}(g_1)\rho_{\pi(g_1g_2)^{-1}l}(g_2)u_{\pi(g_1g_2)^{-1}l} \\ &= \rho_{\pi(g_1)^{-1}l}(g_1)\rho_{\pi(g_2)^{-1}(\pi(g_1)^{-1}l)}u_{\pi(g_2)^{-1}(\pi(g_1)^{-1}l)} \\ &= (\rho(g_1)\rho(g_2) \cdot u)_l \end{aligned}$$

## 7 Aufgabe 7:

Geben Sie ein maximales System von irreduziblen, paarweise inäquivalenten Darstellungen von  $D_n$  für ungerades  $n$  an. Weisen Sie nach, daß die Darstellungen wirklich irreduzibel sind, und daß das System maximal ist.

Lösung:

Definiere:

$$\begin{aligned}\rho_0(d^k) &:= 1; \rho_0(sd^k) := 1 \\ \rho'_0(d^k) &:= 1; \rho'_0(sd^k) := -1 \\ \rho_j(d^k) &:= \begin{pmatrix} \omega^{kj} & 0 \\ 0 & \omega^{-kj} \end{pmatrix}, \rho_j(sd^k) := \begin{pmatrix} 0 & \omega^{-kj} \\ \omega^{kj} & 0 \end{pmatrix}\end{aligned}$$

für  $l = 1 \dots (n-1)/2$ . Man rechnet nach, daß die Darstellungen korrekt definiert sind. (Achtung: Definition im Stiefel ist falsch!)

Irreduzibilität von  $\rho_j$ : Die Matrizen sind diagonalisierbar und besitzen keine gemeinsamen Eigenräume, denn  $\rho_j(d)$  hat EV  $(1, 0)$  und  $(0, 1)$ ,  $\rho_j(s)$  hat EV  $(1, 1)$  und  $(1, -1)$  zu verschiedenen EW.

Inäquivalenz: Die Matrizen haben, solange  $j \leq (n-1)/2$ , alle unterschiedliche Paare von Eigenwerten, sind also nicht ähnlich zueinander und damit inäquivalent.

Vollständigkeit:  $|D_n| = 2n = 1 + 1 + (n-1)/2 * 4$ .

## 8 Aufgabe 8:

Sei  $\rho$  eine Darstellung der Gruppe  $G$  in  $V$ ,  $M$  der Vektorraum der linearen Abbildungen  $T$  von  $V$  in sich, für welche  $T\rho = \rho T$ . Sei  $\rho = c_1\rho_1 + \dots + c_m\rho_m$  mit paarweise inäquivalenten und irreduziblen Darstellungen  $\rho_i$ . Zeigen Sie:

$$\dim(M) = \sum_{i=1}^m c_i^2$$

Lösung:

Sei  $\rho$  so in einer Basis von  $V$  in Matrizen dargestellt, daß  $\rho$  die von Schur angegebene Blockdiagonalform aus Blöcken  $\rho_i$  hat. Sei  $T$  aufgespalten wie  $\rho$ . Dann gilt für die Blöcke von  $T$   $T_{i,j}\rho_j = \rho_i T_{i,j}$ . Nach dem Schurschen Lemma gilt damit  $T_{i,j} = 0$  für inäquivalente Darstellungen, oder  $T_{i,j} = \lambda_{i,j}I$  für äquivalente Darstellungen. Offensichtlich liegt jede Matrix, die diese Bedingungen erfüllt, in  $M$ , und es gilt die angegebene Dimensionsformel.

## 9 Aufgabe 9:

Zeigen Sie, daß man die Multiplikation in  $\mathbb{C}[z]/(z^2 + 1)$  mit zwei komplexen Multiplikationen und vier Additionen ausführen kann. Vorberechnungen auf einem Faktor werden nicht gezählt.

Lösung:

Sei  $z^n + 1 = p_1 p_2$  und  $p_2 q_1 + p_1 q_2 = 1$ . Dann folgt nach dem CRT sofort durch Bildung des Restes bezüglich  $p_1$  und  $p_2$

$$fg = (p_2 q_1 (fg \bmod p_1) + p_1 q_2 (fg \bmod p_2)) \bmod (z^n + 1).$$

Setze  $p_1 := z + i$  und  $p_2 := z - i$ . Dann folgt  $q_2 = -q_1 = \frac{1}{2i}$ .

Sei  $f = a + bz$  und  $g = c + dz$ . Dann ist

$$fg \bmod (z^2 + 1) = ac - bd + (bc + ad)z.$$

Mit der Formel gilt

$$fg \bmod (z^2 + 1) = -\frac{1}{2i}(z - i)((a + bi)(c + di)) + \frac{1}{2i}(z + i)((a - bi)(c - di)).$$

Wenn die konstanten Faktoren dem  $f$  zugeschlagen werden (Vorbereitung), ergibt sich eine Vorschrift, die zwei Multiplikationen benötigt und vier Additionen. Die Bildung von  $a + bi$  und  $a - bi$  wird wieder nicht gezählt.

## 10 Aufgabe 10:

Sei  $\mathbb{F}$  ein Körper und  $x_1, \dots, x_n \in F$ . Die elementarsymmetrischen Funktionen  $\sigma_1^n, \dots, \sigma_n^n$  sind definiert durch

$$\sigma_1^n = x_1 + \dots + x_n = \sum_{i=1}^n x_i$$

$$\sigma_2^n = x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3x_4 + \dots + x_{n-1}x_n = \sum_{i,k=1, i \neq k}^n x_i x_k$$

$\vdots$

$$\sigma_n^n = x_1 \cdot x_2 \cdot \dots \cdot x_n = \prod_{i=1}^n x_i$$

(a) Zeigen Sie für  $m = 2, \dots, n$  die Rekursion

$$\begin{aligned}\sigma_1^m &= x_m + \sigma_1^{m-1} \\ \sigma_j^m &= x_m \sigma_{j-1}^{m-1} + \sigma_j^{m-1}, \quad j = 2, \dots, m-1 \\ \sigma_m^m &= x_m \sigma_{m-1}^{m-1}\end{aligned}$$

mit dem Startwert  $\sigma^1 = x_1$ .

(b) Zeigen Sie, daß  $\sigma_1^n, \dots, \sigma_n^n$  in  $n^2 + O(n)$  Additionen und Multiplikationen berechenbar sind.

Lösung:

(a) klar.

(b) Durch Induktion. Seien  $\sigma_1^n, \dots, \sigma_n^n$  bereits berechnet. Dann benötigt man zur Berechnung von  $\sigma_k^{n+1}$  jeweils höchstens eine Addition und eine Multiplikation, insgesamt genau  $n$  Multiplikationen und  $n$  Additionen. Zur Berechnung der ersten Folge wurden weniger als  $\frac{n^2}{2} + cn$  MP und ADD benötigt, also jetzt weniger als  $\frac{(n+1)^2}{2} + c(n+1)$  MP und ADD.



## 11 Aufgabe 11:

Lösen Sie folgende simultane Kongruenzen:

(a)

$$\begin{aligned}x &\equiv 7 \pmod{30} \\x &\equiv 5 \pmod{77} \text{ in } \mathbb{C}.\end{aligned}$$

(b)

$$\begin{aligned}f &\equiv 2z^2 + 7 \pmod{z^3 - 1} \\f &\equiv z^3 + z + 1 \pmod{z^4 + 1} \text{ in } \mathbb{R}[z].\end{aligned}$$

(a) Obwohl so einfach, mit euklidischem Algorithmus.

$$\begin{aligned}77 : 30 &= 2 R 17 \\30 : 17 &= 1 R 13 \\17 : 13 &= 1 R 4 \\13 : 4 &= 3 R 1 \\4 : 1 &= 4 R 0\end{aligned}$$

Nach endlosem Rechnen:

$$\begin{aligned}13 - 3 \cdot 4 &= 1 \\17 - 13 &= 4 \Rightarrow 3 \cdot 17 - 4 \cdot 13 = 3 \cdot 4 - 13 \Rightarrow 4 \cdot 13 - 3 \cdot 17 = 1 \\30 - 17 &= 13 \Rightarrow 4 \cdot 30 - 7 \cdot 17 = 4 \cdot 13 - 3 \cdot 13 = 1 \\77 - 2 \cdot 30 &= 17 \Rightarrow 7 \cdot 77 - 18 \cdot 30 = 7 \cdot 17 - 4 \cdot 30 \Rightarrow 18 \cdot 30 - 7 \cdot 77 = 1\end{aligned}$$

Eine Lösung ist damit  $5 \cdot 18 \cdot 30 - 7 \cdot 7 \cdot 77 = -1073 = 1237$ .

(b) Siehe oben.

$$\begin{aligned}(z^4 + 1) : (z^3 - 1) &= z & R & z + 1 \\(z^3 - 1) : (z + 1) &= z^2 - z + 1 & R & -2\end{aligned}$$

und damit

$$\begin{aligned}-\frac{1}{2}(z^3 - 1) + \frac{1}{2}(z + 1)(z^2 - z + 1) &= 1 \\(z^4 + 1) - z(z^3 - 1) &= z + 1 \Rightarrow \\ \frac{1}{2}(z^2 - z + 1)(z^4 + 1) - \left(\frac{z}{2}(z^2 - z + 1) + \frac{1}{2}\right)(z^3 - 1) &= \\ \frac{1}{2}(z^2 - z + 1)(z + 1) - \frac{1}{2}(z^3 - 1) &= 1\end{aligned}$$

Wir erhalten also:

$$\frac{1}{2}(z^2 - z + 1)(z^4 + 1) - \frac{1}{2}(z^3 - z^2 + z + 1)(z^3 - 1) = 1.$$

Damit ist die gewünschte Zerlegung erreicht, und eine Lösung ist

$$(2z^2 + 7)\frac{1}{2}(z^2 - z + 1)(z^4 + 1) - (z^3 + z + 1)\frac{1}{2}(z^3 - z^2 + z + 1)(z^3 - 1).$$



### 13 Aufgabe 13:

Geben Sie ein erzeugendes Element für die Gruppe  $M_{25}$  an.

Lösung:

Erzeugende Elemente sind 2, 3, 8, 12, 13, 17, 22 und 23. Gerechnet mit dem Programm im Unterverzeichnis A13. Alternative Lösung: Erzeugende Elemente von  $M_p$  sind auch erzeugende Elemente von  $M_{p^n}$ , also sind 2 und 3 erzeugende Elemente für  $M_{25}$ .

### 14 Aufgabe 14:

Sei  $n = n_1 \cdot \dots \cdot n_r$  mit paarweise teilerfremden Faktoren  $n_1, \dots, n_r$ .

Zeigen Sie die Isomorphie

$$M_n \cong M_{n_1} \odot \dots \odot M_{n_r}.$$

Lösung:

Sei ohne Einschränkung  $r = 2$ . Sei  $c \in M_n$ . Dann ist  $c$  teilerfremd zu  $n$ , also auch zu  $n_1$  und  $n_2$ , und die natürliche Abbildung  $\psi$  von  $c$  auf das Tupel  $(c \bmod n_1, c \bmod n_2)$  ist bijektiv. Gleichzeitig erhält diese Abbildung die Multiplikation, d.h.  $\psi(c_1 c_2) = \psi(c_1) \psi(c_2)$ , und die Gruppen sind isomorph.

## 15 Aufgabe 15:

Die Radix-4-FFT hat für  $n=4^t$ ,  $t \in \mathbb{N}$ , die Form

$$W_n = (I_1 \otimes B_n)(I_n \otimes B_{n/4}) \cdots (I_{n/4} \otimes B_4)P_n$$

mit den Radix-4-Schmetterlingen

$$B_n = \begin{pmatrix} I & D & D^2 & D^3 \\ I & iD & -D^2 & -iD^3 \\ I & -D & D^2 & -D^3 \\ I & -iD & -D^2 & iD^3 \end{pmatrix}$$

mit  $I = I_{n/4}$ ,  $D = D_{n/4}$  und einer Permutationsmatrix  $P_n$ .

Zeigen Sie: Ist  $k = (b_{t-1}, \dots, b_0)_4$  die Darstellung von  $k$  bezüglich der Basis 4, und  $k' = (b_0, \dots, b_{t-1})_4$ , so ist

$$(P_n y)_k = y_{k'}, \quad k = 0, \dots, n-1.$$

Lösung:

Sei  $n = 4m$ . Sei  $p = 4$ . Nach Vorlesung gilt

$$P_n y = (I_p k_2 \otimes P_n) P_{p,m} y.$$

Wir zeigen den Satz durch vollständige Induktion über  $t$ . Für  $t = 1$  ist der Satz klar. Sei der Satz nun für  $P_m$  gültig, d.h.  $P_m(x) = x_{I(x,m)}$ ,  $I$  die Funktion, die ein Bitreversal der Länge  $t = \log_2 m$  auf  $x$  ausführt.

Sei  $k = k_2 + mk_1$ ,  $0 \leq k_1 < p$ . Für die in der Vorlesung definierte Funktion  $P_{p,m}$  gilt  $(P_{p,m} x)_{mk_1+k_2} = x_{k_1+pk_2}$ . Für das Kreuzprodukt gilt  $((I_p \otimes P_m) y)_k = (P_m(y_{k_1m+i}))_{k_2}$ .

Dann gilt

$$\begin{aligned} (P_n y)_k &= ((I_p \otimes P_m) P_{p,m} y)_k \\ &= (P_m(((P_{p,m} y)_{k_1m+i}))_{k_2}) \\ &= (((P_{p,m} y)_{k_1m+i})_{I(k_2,m)}) \\ &= ((y_{pk_1+i})_{I(k_2,m)}) \\ &= y_{k_1m+I(k_2,m)} \\ &= y_{I(k,n)}. \end{aligned}$$

Bemerkung: Der Satz läßt sich noch verallgemeinern. Für den Fall von verschiedenen Primfaktoren, nach denen die Cooley-Tukey-FT ausgeführt wird, definiere für  $n = \prod_{i=0}^m p_i$  und  $0 \leq c_i < p_i$  die Funktion

$$I\left(\sum_{k=0}^m c_k \prod_{i=0}^{k-1} p_i\right) = \sum_{k=0}^m c_k \prod_{i=k+1}^{n-1} p_i.$$

$$P_n(x) = x_{I(m)}.$$

Bemerkung: Für  $n = p_1 p_2$  erhält man  $(Px)_{kp_1+i} = x_{k+ip_2}$ . Betrachtet man  $x$  als  $p_1 \cdot p_2$ -Matrix, so beschreibt  $P$  die Durchführung der Transposition auf der Matrix.

## 16 Aufgabe 16:

Zeigen Sie:

- (a) Für  $n = 2^t$ ,  $t \in \mathbb{N}$ , kommt die Radix-2-FFT mit  $5n \log_2 n$  FLOPs aus.
- (b) Für  $n = 4^t$ ,  $t \in \mathbb{N}$ , kommt die Radix-4-FFT mit  $4.25n \log_2 n$  FLOPs aus.

Lösung:

Beweis nach dem Diagramm der Vorlesung.

- (a) Um den Schmetterling der Vorlesung anwenden zu können, braucht man 2 komplexe Additionen und 1 komplexe Multiplikation, also insgesamt 10 FLOPs. Pro Schritt müssen  $n/2$  Schmetterlinge angewandt werden, die Iterationstiefe ist  $\log_2 n$ . Insgesamt gibt das  $5n \log_2 n$  FLOPs.
- (b) Zur Anwendung der Matrix  $B_n$  müssen zunächst 3 komplexe Multiplikationen durchgeführt werden. Da wir Multiplikationen mit  $i$  nicht zählen (reine Umordnung), brauchen wir bei geschickter Anordnung noch 8 weitere Additionen. Zunächst werden Summe und Differenz von  $x_1$  und  $x_3$  gebildet, dann Summe und Differenz von  $x_2$  und  $x_4$ , durch jeweils eine weitere Addition/Subtraktion erhält man das Ergebnis. Insgesamt erhalten wir damit eine Komplexität von 34 FLOPs zur Anwendung eines Schmetterlings. Pro Schritt müssen  $n/4$  Schmetterlinge angewandt werden bei einer Iterationstiefe von  $\log_4 n = \frac{1}{2} \log_2 n$ , macht zusammen  $4.25n \log_2 n$  FLOPs.

Bemerkung: Für größere Einheiten, z.B.  $n = 8^t$ , werden die Ergebnisse noch besser.

Bemerkung: Viele Beweise und Ideen finden sich in Van Loan, Computational Frameworks for the FFT.

## 17 Aufgabe 17:

Schreiben Sie ein nicht-rekursives Programm `fft(n,y)` für die Radix-2-Version von Cooley-Tukey. Vergleichen Sie Resultat und Laufzeit für  $n = 1024$  mit der IMSL-Routine

`imsl_c_fft_complex()`.

Lösung:

Im Verzeichnis A17. Die Geschwindigkeiten sind vergleichbar, NAG ist sogar bei vorgegebenem Permutationsvektor und vorberechneten Gewichten  $\omega^k$  langsamer als die einfache Implementation der CT-FFT.

## 18 Aufgabe 18:

Konstruieren Sie mit Hilfe des chinesischen Restsatzes einen Algorithmus zur Berechnung der Faltung der Länge 4, der mit 5 Multiplikationen und 15 Additionen auskommt. Vorberechnungen auf einem der Faktoren werden nicht gezählt.

Lösung:

Eine Faltung entspricht der Multiplikation zweier Polynome modulo  $z^n - 1$ . Setze

$$\begin{aligned} p(z) &:= z^4 - 1 \\ p_1(z) &:= z^2 - 1 \\ p_2(z) &:= z^2 + 1 \\ q_1 &:= \frac{1}{2} \\ q_2 &:= -\frac{1}{2} \end{aligned}$$

Dann sind die Voraussetzungen einer alten Aufgabe erfüllt, und es gilt

$$(fg) \bmod p = (p_2 q_1 (fg) \bmod p_1 + p_1 q_2 (fg) \bmod p_2) \bmod p.$$

Eingesetzt:

$$\begin{aligned} (fg) \bmod p &= (z^2 - 1) \frac{1}{2} (((f_0 - f_2) + (f_1 - f_3)z)((g_0 - g_2) + (g_1 - g_3)z) \bmod (z^2 + 1)) \\ &\quad - (z^2 + 1) \frac{1}{2} (((f_0 + f_2) + (f_1 + f_3)z)((g_0 + g_2) + (g_1 + g_3)z) \bmod (z^2 - 1)) \end{aligned}$$

Die Faltung der Länge zwei kann dann mit 2 Multiplikationen und 4 Additionen realisiert werden. Die Multiplikation modulo  $z^2 + 1$  kann durch den

Algorithmus zur schnellen Multiplikation komplexer Zahlen mit 3 Multiplikationen und 3 Additionen realisiert werden. Insgesamt benötigt man damit 5 Multiplikationen und  $4 + 4 + 3 + 4 = 15$  Additionen.

Da der Algorithmus noch einmal benutzt wird, hier die genaue Rechenvorschrift:

$$\begin{aligned}
 s_0 &= -\frac{1}{2}(f_0 - f_2) & t_0 &= g_0 - g_2 \\
 s_1 &= -\frac{1}{2}(f_1 - f_3) & t_1 &= g_1 - g_3 \\
 s_2 &= -\frac{1}{2}(f_0 + f_2) & t_2 &= g_0 + g_2 \\
 s_3 &= -\frac{1}{2}(f_1 + f_3) & t_3 &= g_1 + g_3 \\
 & & m_0 &= s_4 t_4 \\
 & & m_1 &= s_5 t_5 \\
 & & t_6 &= m_0 + m_1 \\
 & & t_7 &= m_0 - m_1 \\
 s_8 &= s_2 + s_3 & t_8 &= t_2 + t_3 \\
 s_9 &= s_2 - s_3 \\
 & & m_2 &= s_2 t_8 \\
 & & m_3 &= s_8 t_3 \\
 & & m_4 &= s_9 t_2 \\
 & & t_{10} &= m_2 - m_3 \\
 & & t_{11} &= m_2 - m_4 \\
 & & t_{12} &= -t_6 + t_{10} \\
 & & t_{13} &= -t_7 + t_{11} \\
 & & t_{14} &= t_6 + t_{10} \\
 & & t_{15} &= t_7 + t_{11}
 \end{aligned}$$

Bemerkung:  $m_2$  geht in jedes Ergebnis einmal ein.

Bemerkung:  $t_8$  enthält die Summe aller  $f_k$ .

## 19 Aufgabe 19:

Geben Sie einen Algorithmus an, der die Fourier-Transformation der Länge  $n = 2^t$  für zwei reelle Vektoren in  $5n \log_2 n + 4n$  Flops ausführt.

Lösung:

Seien die Vektoren in  $a$  und  $b$  gegeben. Setze  $y_k := a_k + ib_k$ . Für die Fouriertransformation eines reellen Vektors  $a$  gilt:

$$\begin{aligned}
 \bar{\hat{a}}_{-j} &= \sum_{k=0}^{n-1} e^{2\pi i k j / n} a_k \\
 &= \hat{a}_j
 \end{aligned}$$

mit der Definition  $a_{-k} := a_{n-k}$ . Insbesondere gilt für  $y$ :

$$\hat{y}_j = \hat{a}_j + i\hat{b}_j$$

und

$$\bar{\hat{y}}_{-j} = \bar{\hat{a}}_{-j} - i\bar{\hat{b}}_{-j} = \hat{a}_j - i\hat{b}_j.$$

Damit ist für  $j \neq 0$   $\hat{a}_j = \frac{1}{2}(\hat{y}_j + \bar{\hat{y}}_{-j})$  und  $\hat{b}_j = \frac{1}{2}(\hat{y}_j - \bar{\hat{y}}_{-j})$ . Die Anzahl der Operationen ist  $4n+$  die Anzahl der Operationen zur Durchführung einer komplexen Fouriertransformation.

## 20 Aufgabe 20:

Die Sinus-Transformation der Länge  $n$  ist definiert durch

$$\hat{y}_k = \sum_{j=1}^{n-1} \sin(kj\pi/n)y_j, \quad k = 1, \dots, n-1.$$

- (a) Berechnen Sie die inverse Transformation.
- (b) Geben Sie einen Algorithmus an, der die Sinus-Transformation der Länge  $n = 2^t$  für reelle Vektoren mit  $\frac{5}{2}n \log_2 n + O(n)$  Flops berechnet.

Lösung:

- (a) Setze  $y_{n+j} := -y_j$ ,  $y_0 := 0$ . Es gilt:

$$\begin{aligned} \hat{y}_k &= \sum_{j=0}^{n-1} \sin(kj\pi/n)y_j \\ &= \frac{1}{2i} \sum_{j=0}^{2n-1} e^{ikj\pi/n}y_j \end{aligned}$$

Die Sinustransformation ist also eine Fouriertransformation auf dem Vektor  $y$ . Es gilt  $\hat{y}_{n+j} = -\hat{y}_j$ . Die inverse Fouriertransformation liefert die Formel

$$y_k = \frac{1}{n} \sum_{j=0}^{n-1} \sin(kj\pi/n)\hat{y}_j.$$

## 21 Aufgabe 21:

Leiten Sie einen Algorithmus zur Fourier-Transformation der Länge 5 her, der mit 5 Multiplikationen und 17 Additionen auskommt.

Lösung:

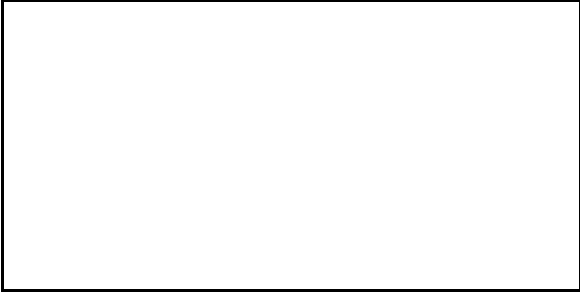
Die Matrix  $F_5$  der Fourier-Transformation der Länge 5 ist, nach Streichung der ersten Zeile und der ersten Spalte, isomorph zu der Gruppentafel der Gruppe  $M_5$ . Diese Gruppentafel ist, da 5 prim ist, nach Umordnung eine zyklische Faltung, denn  $M_5$  wird zum Beispiel vom Gruppenelement 2 erzeugt. Zur Anwendung von  $F_5$  auf einen Vektor  $y$  wird also zunächst eine zyklische Faltung der Länge 4 durchgeführt auf  $(y_1, y_2y_3, y_4)$ . Nach einer alten



Aufgabe benötigt dies 5 Multiplikationen und 15 Additionen. In diesem Algorithmus kommt das Ergebnis der ersten Multiplikation immer additiv vor. Wenn man daher dort auf das Ergebnis der ersten Multiplikation  $y_0$  aufaddiert, erhält man die korrekten Werte für  $(\hat{y}_k)$ ,  $k = 1 \dots 4$ . Zur Bestimmung von  $\hat{y}_0$  müssen alle Werte addiert werden. Im Verlauf der Faltung wird die Summe von  $y_1 \dots y_4$  berechnet, darauf muß nur noch  $y_0$  addiert werden.

## 22 Aufgabe 22:

Leiten Sie einen Algorithmus zur Lösung der Randwertaufgabe

$$\frac{\partial u}{\partial \nu} = 0$$


$$u = 0$$

$$u = 0$$

$$\frac{\partial u}{\partial \nu} = 0$$

auf einem  $n \times m$ -Gitter in  $O(nm \log_2(nm))$  Rechenoperationen her.

Lösung:

In der Vorlesung wurde bereits eine Lösung der eindimensionalen Aufgabe mit  $u = 0$  auf dem Rand hergeleitet. Wir leiten eine Lösung der eindimensionalen Aufgabe mit  $\frac{\partial u}{\partial \nu} = 0$  her. Die dabei auftretende Matrix  $A$  unterscheidet sich von den Dirichlet-Randbedingungen dadurch, daß in der ersten und letzten Zeile auf der Nebendiagonalen eine 2 statt einer 1 auftaucht.

Sei  $j$  fest und  $c_k := \cos(\pi k j / n)$ . Wir zeigen, daß  $c$  ein Eigenvektor von  $A$  ist. Es gilt

$$\begin{aligned} c_{k-1} + c_k + c_{k+1} &= \frac{e^{ikj\pi/n}}{2} (e^{-ikj\pi/n} - 2 + e^{ikj\pi/n}) + \\ &\quad \frac{e^{-ikj\pi/n}}{2} (e^{ikj\pi/n} - 2 + e^{-ikj\pi/n}) \\ &= \frac{e^{ikj\pi/n} + e^{-ikj\pi/n}}{2} (2 \sin(j\pi/n) - 2) \\ &= c_k (2 \sin(j\pi/n) - 2) \end{aligned}$$

In allen Zeilen außer der ersten und der letzten erfüllt  $c$  also die Eigenwertgleichung zum Eigenwert  $2 \sin(j\pi/n) - 2$ . Für  $k = 0$  gilt aber immer  $c_1 = c_{-1}$ , und damit  $2c_0 + 2c_1 = c_{-1} + 2c_0 + c_1 = (2 \sin(j\pi/n) - 2) c_0$ . Ebenso zeigt

man die Gleichung für die letzte Zeile. Wir haben damit ein vollständiges Eigenwertsystem von  $A$ . Die Matrix der Eigenvektoren ist die Matrix der Cosinustransformation. Damit kann die Lösung der Poissongleichung wie in der Vorlesung durch Aufspaltung von  $A$  berechnet werden.

## **23 Aufgabe 23:**

Schreiben Sie ein Programm `fft7(y)`, das die Fourier-Transformation der Länge 7 mit 8 Multiplikationen und 36 Additionen berechnet. Schreiben Sie damit eine Fourier-Transformation der Länge 28, die mit 36 Multiplikationen und 200 Additionen auskommt.

Lösung:  
`aufg28.c`.

## 24 Aufgabe 24:

Sei  $P$  die natürliche Darstellung von  $D_4$  auf einem 4 Gitter, und sei  $A$  eine  $(16, 16)$ -Matrix mit den Symmetrien von  $P$ . Zeigen Sie, daß  $A$  nach Satz IV.1.2 in je zwei Matrizen der Dimensionen 1, 3 und 4 zerfällt.

Lösung:

Nach Satz IV.1.2 ist zunächst die natürliche Darstellung  $P_n$  auszureduzieren. Wir lösen diese Aufgabe mit Orbits.

Ausreduzieren einer Darstellung bedeutet, daß wir eine Basis des  $\mathbb{R}^{16}$  angeben, bezüglich der die Darstellung eine Blockdiagonalgestalt hat. Auf der Blockdiagonalen stehen dann jeweils irreduzible Darstellungen.

Algebraisch ist dies eine Reduktion auf invariante Teilräume. Diese Teilräume suchen wir nicht im  $\mathbb{R}^{16}$ , sondern in anderen, einfach zu bestimmenden Teilräumen. Diese nennen wir Orbits. Wir betrachten folgende Numerierung unseres Quadrats:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Durch Drehungen und Spiegelungen werden die Punkte 1, 4, 13 und 16 ineinander überführt. Der Spann der Einheitsvektoren  $e_1, e_4, e_{13}$  und  $e_{16}$  bildet also einen invarianten Unterraum unter allen Matrizen der Darstellung  $P_n$ . Gleiches gilt für die Vektoren  $e_6, e_7, e_{10}$  und  $e_{11}$ . Die Struktur dieser Unterräume ist gleich.

Ebenso werden die Punkte 2, 3, 5, 8, 9, 12, 14 und 15 durch  $P_n$  ineinander überführt. Die zugehörigen Einheitsvektoren bilden wieder einen invarianten Unterraum, die Struktur ist aber jetzt anders (sogar die Dimension).

Man sieht leicht, daß es nur vier verschiedene Klassen von auf diese Weise gewonnenen invarianten Unterräumen gibt:

- Den Unterraum, der nur aus einem Punkt im Nullpunkt besteht (Dimension=1).
- Den Unterraum, der durch Drehung und Spiegelung eines Punktes mit 0 kleiner Winkel gegen die  $x$ -Achse kleiner 45 Grad entsteht (Dimension=8).
- Den Unterraum, der durch Drehung und Spiegelung eines Punktes auf der  $x$ -Achse entsteht (Dimension=4).
- Den Unterraum, der durch Drehung und Spiegelung eines Punktes auf der Diagonalen entsteht (Dimension=4).

Bemerkung: Falls die zugrundeliegende Gruppe  $D_n$  ist, so erhält man Dimension  $2n$  für Unterraum 2 und Dimension  $n$  für Unterräume 3 und 4.

Eine vollständige Liste von irreduziblen Darstellungen wurde bereits gegeben. Es sind dies:

$\rho_1(s^l r^k) = 1$ ,  $\rho_2(s^l r^k) = (-1)^l$ ,  $\rho_3(s^l r^k) = (-1)^k$  und  $\rho_4(s^l r^k) = (-1)^{k+l}$  (eindimensional) und mit einer vierten Einheitswurzel  $\omega$

$$\rho_5(r^k) = \begin{pmatrix} \omega^k & 0 \\ 0 & \bar{\omega}^k \end{pmatrix}, \quad \rho_5(sr^k) = \begin{pmatrix} 0 & \bar{\omega}^k \\ \omega^k & 0 \end{pmatrix}.$$

In unserem Beispiel haben wir zwei Unterräume der Klasse *II* und einen Unterraum der Klasse *IV*.

Es reicht nun, diese Unterräume auszureduzieren. Anschließend haben wir die Aufgabe gelöst, nicht nur für das  $4 \times 4$ -Gitter, sondern für *jede* Matrix mit den Symmetrien von  $D_4$ . Wir betrachten folgenden Vertreter der Klasse *II*:

$$\begin{array}{cc} 1 & 2 \\ 3 & 4 \end{array}$$

Wir bestimmen nun Vektoren, bezüglich derer die natürliche Darstellung  $P_n$  auf diesem Viereck in irreduzible Darstellungen zerfällt.

Wir betrachten  $\rho_1$ . Sei  $x$  ein Vektor mit  $P_n(s^l r^k)x = \rho_1(s^l r^k)x = x$ . Setze  $x_1 := 1$ , dann gilt sofort  $x_k = 1$  für  $k = 1 \dots 4$ .

Betrachte  $\rho_3$ . Für  $x_k := (-1)^k$  gilt  $P_n(s^l r^k)x = \rho_3(s^l r^k)x = -1^k x$ .

Betrachte  $\rho_5$ . Setze  $x_k := \omega^k$  und  $y_k := \bar{\omega}^k$ . Es gilt  $P_n(r^k)x = \omega^k x$ ,  $P_n(r^k)y = \bar{\omega}^k x$ ,  $P_n(sr^k)x = \bar{\omega}^k y$  und  $P_n(sr^k)y = \omega^k x$ .

Bezüglich der angegebenen Vektoren ist  $P_n$  die (ausreduzierte) Darstellung

$$\begin{pmatrix} \rho_1 & & & \\ & \rho_3 & & \\ & & \rho_5 & \\ & & & \rho_5 \end{pmatrix}.$$

Die Klasse *IV* macht etwas mehr Arbeit. Wir finden folgende Basisvektoren:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & & & 1 \\ 1 & & & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & & & 1 \\ & & & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & -1 & -1 \\ -1 & & & 1 \\ -1 & & & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & & & -1 \\ -1 & & & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

zu den Darstellung  $\rho_1$ ,  $\rho_2$ ,  $\rho_3$  und  $\rho_4$  und

$$\begin{pmatrix} \omega^3 & 1 & & \\ \omega^3 & & & 1 \\ \omega^2 & & & \omega \\ \omega^2 & \omega & & \omega \end{pmatrix}, \begin{pmatrix} \bar{\omega}^3 & 1 & & \\ \bar{\omega}^3 & & & \bar{\omega} \\ \bar{\omega}^2 & & & \bar{\omega} \\ \bar{\omega}^2 & \bar{\omega} & & \bar{\omega} \end{pmatrix}, \begin{pmatrix} -\omega^3 & 1 & & \\ \omega^3 & & & -1 \\ -\omega^2 & & & \omega \\ \omega^2 & -\omega & & \omega \end{pmatrix}, \begin{pmatrix} -\bar{\omega}^3 & 1 & & \\ \bar{\omega}^3 & & & -1 \\ -\bar{\omega}^2 & & & \bar{\omega} \\ \bar{\omega}^2 & -\bar{\omega} & & \bar{\omega} \end{pmatrix}$$

zur Darstellung  $\rho_5$  (zweimal). Damit hat unsere Klasse *IV* der Dimension 8 bezüglich dieser Basisvektoren die Darstellung

$$\begin{pmatrix} \rho_1 & & & & \\ & \rho_2 & & & \\ & & \rho_3 & & \\ & & & \rho_4 & \\ & & & & \rho_5 \\ & & & & & \rho_5 \end{pmatrix}.$$

Nun zurück zur Aufgabe. Unsere Diskretisierung hat zwei invariante Untergruppen des Typs *IV* und eine invariante Untergruppe des Typs *II*. Die zugehörige Darstellung  $P_n$  kann mit der obigen Rechnung reduziert werden zu

$$P_n = 3\rho_1 + 2\rho_2 + 3\rho_3 + 2\rho_4 + 4\rho_5.$$

Nach Satz IV.1.2 zerfällt  $A$  damit in zwei Matrizen der Dimension 3 ( $\rho_1, \rho_3$ ), zwei Matrizen der Dimension 2 ( $\rho_2, \rho_4$ ) und zwei Matrizen der Dimension 4 ( $\rho_5$ ).

## 25 Aufgabe 25:

Seien  $p, q \in \mathbb{C}$  und  $f(x) = x^3 + px + q$ .

- Bestimmen Sie eine Faltung  $A$  der Länge 3, so daß  $f$  das charakteristische Polynom von  $A$  ist.
- Berechnen Sie die Eigenwerte von  $A$  nach Satz IV.1.2.
- Geben Sie Formeln an für die Nullstellen von  $f$  (Cardanischer Formeln).

Lösung:

- Das charakteristische Polynom der Faltung

$$A = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$$

ist  $(a - \lambda)^3 + b^3 + c^3 - 3(a - \lambda)bc$ . Wir wählen also  $a = 0$ ,  $p = -3bc$  und  $q = -b^3 - c^3$ . Es gilt  $c = -\frac{p}{3b}$  und  $b^6 + qb^3 - 3p^3 = 0$  und damit

$$(b^3)_{1,2} = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + 3p^3}.$$

- (b) Sei  $X$  eine zyklische Faltung der Länge 3. Nach einem Satz der Vorlesung hat  $X$  die Symmetrien der Darstellung  $\rho(a^k) := P^k$  der Gruppe  $G = \langle 1, a, a^2 \rangle$  mit der Matrix

$$P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Nach einem weiteren Satz der Vorlesung kann man  $\rho$  ausreduzieren, also schreiben als direkte Summe von irreduziblen Darstellungen. Die irreduziblen Darstellungen von  $G$  sind gerade die Multiplikationen mit den dritten Einheitswurzeln.  $P$  muß also diagonalisierbar sein, in der Tat gilt mit einer einfachen dritten Einheitswurzeln  $\omega$

$$\Lambda = A^{-1}PA \text{ mit } A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \Lambda = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}.$$

$X$  hat die Symmetrien von  $\rho$ . Nach Vorlesung hat  $X$  damit bezüglich derselben Basis, bezüglich der  $P$  eine Diagonalmatrix ist, ebenfalls Diagonalgestalt. Tatsächlich errechnet man (mit MAPLE), daß eine allgemeine Faltungsmatrix der Dimension 3 mit den Koeffizienten  $(e, f, g)$  die Form

$$\begin{pmatrix} e + f + g & 0 & 0 \\ 0 & e + \omega f + \omega^2 g & 0 \\ 0 & 0 & e + \omega^2 f + \omega g \end{pmatrix}$$

hat. Insbesondere sind die gesuchten Eigenwerte  $a + b$ ,  $\omega a + \omega^2 b$  und  $\omega^2 a + \omega b$ .

- (c) Einsetzen von  $a$  und  $b$  in die obige Formel für die Eigenwerte liefert die Cardanischen Formeln.

## 26 Aufgabe 26:

Sei  $e_i$  der  $i$ -te Einheitsvektor in  $\mathbb{C}^n$ , und sei  $P = (e_2, \dots, e_{n-1}, e_n, e_1)$ .

Zeigen Sie: Die  $(n, n)$ -Matrix  $A$  ist genau dann eine Faltung, wenn  $P^m A = AP^m$  für ein  $m$  mit  $\text{ggT}(m, n) = 1$ .

Lösung:

Es gilt  $(PAP^t)_{i,j} = A_{i+1,j+1}$ . Die Addition wird modulo  $n$  durchgeführt. Damit ist  $A$  eine symmetrische Faltung, falls  $A = PAP^t$ . Sei nun  $P^m A (P^t)^m =$

$A$  und  $im+kn = 1$ . Es gilt  $A = P^m A(P^t)^m = P^{im} A(P^{im})^t = P^{im+kn} A(P^{im+kn})^t = PAP^t$  und  $A$  ist symmetrische Faltung.

## 27 Aufgabe 27:

$A$  sei eine zyklische Faltung der Länge  $n$  und  $n_d$  sei für jeden Teiler  $d$  von  $n$  der Grad des zugehörigen Kreisteilungspolynoms.

Geben Sie einen Algorithmus an, der das Gleichungssystem  $Ax = b$  (ohne Vorberechnungen!) mit  $n$  Divisionen und

$$N(n) = \sum_{d|n} \left( \frac{n_d^3}{3} + n_d^2 - \frac{n_d}{3} \right)$$

Multiplikationen löst.

Lösung:

In der Vorlesung wurde eine Zerlegung der Matrix  $A$  angegeben, so daß  $B^{-1}DB = A$  mit einer Blockdiagonalmatrix  $D$  und Matrizen  $B$  und  $B^{-1}$  mit ganzzahligen Einträgen. Zur Lösung von  $Ax = b$  muß mit  $B$  und  $B^{-1}$  multipliziert (durch Addition!) und das Gleichungssystem  $Dy = z$  gelöst werden. In  $D$  gibt es Untermatrizen der Dimension  $n_d$  für jeden Teiler  $d$  von  $n$ . Der Gesamtaufwand in Multiplikationen berechnet sich daher wie angegeben.

## 28 Aufgabe 28:

Sei  $A$  eine  $175 \times 175$ -Matrix, welche die Symmetrien des Weihnachtssterns (siehe Abbildung) hat. (D.h.: Ist  $P$  die Permutation der Punkte des Sterns, die von einer den Stern in sich überführenden Bewegung erzeugt wird, so ist  $P^tAP = A$ .)

Zeigen Sie: Bei der Anwendung von Satz IV.1.2 zerfällt  $A$  in 8 Matrizen der Dimensionen 23, 7, 12, 17, 19, 29, 29 und 29.

## 29 Aufgabe 29:

Seien  $A, B$  endliche Gruppen und  $G = A \otimes B$ . Sei  $\rho_1, \dots, \rho_m$  ein MIP für  $A$

und  $\sigma_1, \dots, \sigma_n$  ein MIP für  $B$ . Zeigen Sie: Die Abbildungen

$$\tau_{ik}(ab) = \rho_i(a) \otimes \sigma_k(b), \quad i = 1, \dots, m, \quad k = 1, \dots, n$$

bilden ein MIP für  $G$ .

Lösung:

- (a)  $\tau_{ik}$  ist eine Darstellung. Dies macht man sich sofort klar anhand der Formel

$$(AB) \otimes (CD) = (A \otimes C)(B \otimes D).$$

- (b) Es gilt für das auf den Charakteren definierte Skalarprodukt:

$$\begin{aligned} \langle \tau_{ik}, \tau_{jl} \rangle &= \frac{1}{|A||B|} \sum_{a \in A, b \in B} \text{tr}(\tau_{ik}(ab)) \text{tr}(\tau_{jl}) \\ &= \frac{1}{|A||B|} \sum_{a \in A, b \in B} \text{tr}(\rho_i(a)) \text{tr}(\sigma_k(b)) \text{tr}(\rho_j(a)) \text{tr}(\sigma_l(b)) \end{aligned}$$

unter Benutzung der Formel  $\text{tr}(A \otimes B) = \text{tr}(A)\text{tr}(B)$ . Die Orthogonalität folgt sofort aus der Orthonormalität von  $\rho$  und  $\sigma$ .

### 30 Aufgabe 30:

Sei  $z \in \mathbb{R}^n$  und  $S = (e_2, \dots, e_n, e_1)$  mit den Einheitsvektoren  $e_i \in \mathbb{R}^n$ . Sei  $X = (z, Sz, \dots, S^{n-1}z)$ . Zeigen Sie:  $X^*X$  ist Toeplitz-Matrix.

Lösung:

$X$  ist zyklische Faltung, ebenso  $X^*$ , das Produkt von zyklischen Faltungen ist wieder zyklische Faltung.

### 31 Aufgabe 31:

In der Vorlesung wurde der Algorithmus von Trench für allgemeine Toeplitz-Matrizen definiert.

- (a) In dem Originalartikel von Trench wird der Algorithmus nur für symmetrische Toeplitz-Matrizen definiert. Berechnen Sie für diesen Fall den Aufwand zur Lösung eines Gleichungssystems.
- (b) Für zyklische Toeplitz-Matrizen kann der Algorithmus vereinfacht werden, so daß nicht mehr  $O(n^2)$  Matrixelemente zwischengespeichert werden müssen. Beschreiben Sie den neuen Algorithmus und berechnen Sie den Aufwand zur Lösung eines Gleichungssystems.



Lösung:

- (a) Im Algorithmus werden die Matrizen  $A_k$  und  $A_{-k}$  definiert. Man sieht sofort, daß für symmetrische Matrizen  $A_{-k}$  durch Vertauschung von Spalten und Zeilen aus  $A_k$  hervorgeht.
- (b) Das Vorgehen für zyklische Matrizen ist nicht so einfach. Wir betrachten das Vorgehen für  $n = 1$ . Im normalen Algorithmus von Trench bleibt die erste Zeile unberührt. Im für zyklische Matrizen modifizierten Algorithmus addieren wir auch auf die erste Zeile ein Vielfaches der darüberliegenden Zeile. Dies ist natürlich die letzte Zeile der Matrix. Die Einträge dieser ersten Zeile sind bereits in den anderen Zeilen berechnet worden. Dadurch wird  $A_1$  wieder zyklisch, ebenso verfährt man mit  $A_{-1}$  und erhält, daß alle auftretenden Matrizen zyklisch sind. Insbesondere reichen  $O(n)$  Speicherplätze zur Speicherung der einzelnen Matrizen. Zusätzlich ist die letzte auftretende Matrix  $A_n$  eine Diagonalmatrix, so daß das Rückwärtseinsetzen entfällt.

## 32 Aufgabe 32:

In der Vorlesung wurde ein schneller Algorithmus zur Berechnung der  $LU$ -Zerlegung des Produkts zweier Matrizen mit kleinem Verschiebungsrang angegeben.

- (a) Berechnen Sie die  $LU$ -Zerlegung einer Toeplitz-Matrix.
- (b) Führen Sie den Algorithmus zur Multiplikation von zwei Matrizen mit kleinem Verschiebungsrang explizit mit zwei Toeplitz-Matrizen durch.
- (c) Berechnen Sie den Aufwand in Rechenoperationen.

Lösung:

- (a) Für eine Toeplitz-Matrix  $T$  sei  $T = L + D + U$  die  $LDU$ -Zerlegung. Es gilt für die  $(n, n)$ -Einheitsmatrix  $I$

$$T = LI + I(D + U) =: LI + IR.$$

- (b) Sei  $T_1 = L_1I + IR_1$  und  $T_2 = L_2I + IR_2$ . Damit gilt

$$T_1T_2 = (L_1L_2)I + I(R_1R_2) + L_1R_2 + R_1L_2.$$

Bis auf das letzte Produkt sind alle bereits in der richtigen Form. Dies muß noch in drei Einzelprodukte umgewandelt werden wie in der Vorlesung, wir erhalten eine  $LU$ -Zerlegung vom Grad 6.

- (c) Es sind 4 zyklische Faltungen der Länge  $n$  zu berechnen, macht  $4n \log n + O(n)$  Rechenoperationen.

### 33 Aufgabe 33:

Der Algorithmus von Morf berechnet die  $LU$ -Zerlegung der Inversen einer Matrix  $A$  mit Verschiebungsrang  $\alpha$ . Nehmen Sie an, daß bereits  $LU$ -Zerlegungen vom Grad  $\alpha$  der im Algorithmus auftretenden Matrizen  $A_{11}^{-1}$  und  $(A_{22} - A_{21}A_{11}^{-1}A_{12})^{-1}$  bekannt sind.

- (a) Wie groß ist der Grad der mit dem Algorithmus von Morf berechneten  $LU$ -Zerlegung?
- (b) Wie groß ist der Grad für eine Toeplitz-Matrix  $A$ ?
- (c) Geben Sie einen Algorithmus an, der den Grad der  $LU$ -Zerlegung mit  $O(n \log n)$  Operationen auf  $\alpha + 2$  reduziert.

Lösung:

- (a) Sei durch rekursive Anwendung  $C_{22}$  und  $A_{11}^{-1}$  bereits berechnet mit dem Grad  $\alpha$ . Dann hat  $C_{22}$  den Grad  $\alpha$ ,  $C_{11}$  hat den Grad  $\alpha + 81\alpha^5$ ,  $C_{12}$  hat wie  $C_{21}$  den Grad  $9\alpha^3$ . Begründung: Bei der Multiplikation von zwei  $LU$ -Zerlegungen ist der Grad 3 mal das Produkt der Grade der Einzelzerlegungen.
- (b) Durch den Algorithmus wird der Grad von 2 auf 2592 erhöht.
- (c) In der nächsten Aufgabe wird gezeigt, daß man zur Berechnung der  $LU$ -Zerlegung einer Matrix nur die ersten  $\alpha$  Zeilen der Matrix benötigt, falls die linke obere  $(\alpha, \alpha)$ -Teilmatrix invertierbar ist. Man sieht leicht, daß zur Berechnung der oberen  $\alpha$  Zeilen der Matrix  $LU$  für jedes Matrixelement maximal  $\alpha$  Summanden aufsummiert werden müssen, dies ergibt einen Aufwand von  $O(n)$  zur Berechnung der ersten  $\alpha$  Zeilen einer Matrix aus ihrer  $LU$ -Zerlegung. Mit dem Algorithmus der nächsten Aufgabe erhalten wir so sogar nur einen Aufwand von  $O(n)$ . Alternativ können die Einträge auch durch eine Faltung berechnet werden, in diesem Fall beträgt der Aufwand  $O(n \log n)$ .

## 34 Aufgabe 34:

(Programmieraufgabe, Abgabe: 3. Februar 1995)

Programmieren Sie folgende Prozeduren, die zur Implementation des Algorithmus von Morf benötigt werden.

- (a) Sei `ftrans((complex *)x, int n, int sign)` eine Prozedur, die für  $n = 2^m$  und  $sign = 1$  auf dem komplexen Vektor  $x$  eine Fouriertransformation der Länge  $n$  mit  $O(n \log n)$  Operationen ausführt. Für  $sign = -1$  werde die inverse Fouriertransformation durchgeführt. Schreiben Sie eine Prozedur `convol((complex *)x, (complex *) y, (complex *)z, n)`, die für beliebiges  $n$  die (nicht notwendig symmetrische) Faltung der Länge  $n$  der Vektoren  $x$  und  $y$  mit  $O(n \log n)$  Operationen berechnet und das Ergebnis auf  $z$  schreibt.
- (b) Sei  $A$  eine Matrix mit festem Verschiebungsrang  $\alpha$ . Es sei bekannt, daß für  $M = (e_2, \dots, e_n, 0)$  gilt: Die linke obere  $(\alpha, \alpha)$ -Teilmatrix von  $A - MAM^t$  ist invertierbar.  
Es stehe eine Prozedur `invert(matrix x, int n)` zur Inversion von  $(n, n)$ -Matrizen mit  $O(n^3)$  Rechenoperationen zur Verfügung. Schreiben Sie eine Prozedur  $A$ , die die  $LU$ -Zerlegung von  $A$  mit  $O(n)$  Operationen berechnet.

Lösung:

(nur b, Theoretischer Teil) Zur Berechnung der  $LU$ -Zerlegung einer Matrix reicht es nach Vorlesung, die Spalten der Matrix  $A - MAM^t$  nach einer Basis des Bildes von  $A - MAM^t$  der Länge  $\alpha$  zu entwickeln. Die Bedingung in der Aufgabe bedeutet, daß die ersten  $\alpha$  Spalten linear unabhängig sind. Nach Definition des Verschiebungsrangs sind diese Spalten dann eine Basis.

Seien  $x_k \in \mathbb{C}^\alpha$  jeweils die ersten  $\alpha$  Einträge der  $k$ -ten Spalte der Matrix  $A - MAM^t$ . Da die ersten  $x_k$  für  $k = 1 \dots \alpha$  eine Basis bilden, gilt  $\sum_{k=1}^{\alpha} \beta_{j,k} x_k = x_j$  und damit  $C\beta_j = x_j$  für die linke obere  $(\alpha, \alpha)$ -Teilmatrix. Dies Gleichungssystem ist nun für  $j = 1 \dots n$  zu lösen, der Aufwand beträgt  $O(n + \alpha^3)$ .

## 35 Aufgabe 35:

Seien  $x^k$  die Iterierten des Tschebyscheff-Verfahrens zur Lösung von  $x = Bx + c$ . Zeigen Sie:

$$\begin{aligned}x^1 &= Bx^0 + c, \\x^{k+1} &= \omega_k(Bx^k + c) + (1 - \omega_k)x^{k-1}, \quad k = 1, 2, \dots, \\ \omega_k &= 1 + T_{k-1}\left(\frac{1}{\rho}\right)/T_{k+1}\left(\frac{1}{\rho}\right).\end{aligned}$$

### 36 Aufgabe 36:

Sei  $A = D + L + R$ . Zeigen Sie, daß das SOR-Verfahren für  $Ax = b$  von der Form  $x^{k+1} = Bx^k + c$  ist mit

$$B = (D + \omega L)^{-1}((1 - \omega)D - \omega R) .$$

### 37 Aufgabe 37:

Zeigen Sie: Für die Zahlen  $\alpha_k, \beta_k$  des CG-Verfahrens gilt

$$\alpha_k = \frac{g^{kT} g^k}{d^{kT} A d^k} \quad , \quad \beta_k = \frac{g^{(k+1)T} g^{k+1}}{g^{kT} g^k}$$

mit  $g^k = Ax^k - b$ .

Lösung:

Lösungen dieses Zettels durch Nachrechnen.