WS 85/86

Literatur zur Vorlesung:

"Effiziente Algorithmen"

1. H.J. Nussbaumer: "Fast Fourier Transform and Convolution Algorithms", 2. Auflage
Springer-Verlag, 1982

2. T. Beth: Verfahren der schnellen Fourier-Transformation,
Teubner Studienbücher, Informatik

3. K. Mehlhorn: "Effiziente Algorithmen", Teubner-Studienbücher

4. Aho/Hocroft/Ullman: "The Design and Analysis of Computer Algorithms"
Addison-Wesley, 1974

5. Donald E. Knuth: "The Art of Computer Programming", Vol. 2,
Addison-Wesley Publishing Company, 1969

$3n^3 + O(n^2)$ reelle Multiplikationen

und $3n^3 + O(n^2)$ reelle Additionen

benötigt.

$n \neq 2^m$!

Aufgabe 4: ~~Schreiben~~ Erstellen Sie ein Unterprogramm fmult (b,n,x,y,z), welches die Zahlen

$$x_0 + x_1 b + \ldots + x_{n-1} b^{n-1} \quad , \quad 0 \le x_i < b \quad ,$$

und

$$y_0 + y_1 b + \ldots + y_{n-1} b^{n-1} \quad , \quad 0 \le y_i < b \quad ,$$

nach dem Verfahren von KARATSUBA multipliziert.

6,4
6,-8
-10,-8

2,0 -> 2
4,2
6,4
-8,6
-10,-8

-3,1
1,-3
-5,-3

a2,-10
B=-10
A=-8

a,b
if a=0 then b
else ggT(b, a mod b)

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Do., 31.10.85, 17^{00} Uhr, BK50

Aufgabe 5: Unter dem booleschen Produkt zweier boolescher (n,n) - Matrizen A, B versteht man die Matrix C mit

$$c_{ij} = \bigvee_{k=1}^{n} a_{ik} \wedge b_{kj} \quad ,$$

$a \cdot b = a + b$; ⌐

wobei die Verknüpfungen $\vee$, $\wedge$ durch

$\vee$	0	1
0	0	1
1	1	1

und

$\wedge$	0	1
0	0	0
1	0	1

erklärt sind.

Beschreiben Sie einen Algorithmus, der das boolesche Produkt zweier (n,n) - Matrizen mit $\mathcal{O}(n^{\log_2 7} \cdot (\log_2 n)^{\log_2 3})$ Bit-Operationen

V. Strassen Karatsuba Ring? subtrahieren

(Multiplikationen und Additionen) berechnet.

1, 0

Aufgabe 6: Zeigen Sie, daß die Anwendung einer (n,n) - Toeplitzmatrix A auf einen Vektor x mit $O(n^{\log_2 3})$, Operationen ausgeführt werden kann.

$\mathcal{O}(n \cdot \log n)$

Aufgabe 7: Für die Verschiebungsränge $\alpha_+(A)$, $\alpha_-(A)$ einer quadratischen Matrix A gilt

a) $\alpha = \alpha_+(A)$ (bzw. $\alpha = \alpha_-(A)$) ist die kleinste ganze Zahl, für welche

$$A = L_1 U_1 + L_2 U_2 + \ldots + L_\alpha U_\alpha$$

$$(\text{bzw. } A = U_1 L_1 + U_2 L_2 + \ldots + U_\alpha L_\alpha)$$

gilt mit unteren bzw. oberen Dreiecks-Toeplitzmatrizen L_i, U_i.

b) $|\alpha_+(A) - \alpha_-(A)| \leq 2$.

<u>Aufgabe 8:</u> (Abgabe 8.11.85, 9^{15}Uhr)

Erstellen Sie ein Unterprogramm fmamu (n,A,B,C) für die Strassen - Multiplikation.

Prof. Dr. F. Natterer

WS 85/86
Blatt 3

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Fr., 8.11.85, 9.15 Uhr, BK 50

Aufgabe 9: Sei e_i der i-te Einheitsvektor im $\mathbb{R}^n$, P die (n,n) - Matrix $(e_2,\ldots,e_{n-1}, e_n, e_1)$.

Man zeige: Die (n,n) - Matrix A ist genau dann eine zyklische Faltung, wenn es eine zu n teilerfremde natürliche Zahl m gibt mit $P^m A = A P^m$.

Aufgabe 10: Sei P wie in Aufgabe 9. Zeigen Sie, daß zwei (n,n) - Matrizen A_1, A_2, für die mit einer von n unabhängigen Konstanten r die Abschätzungen

$$\mathrm{rk}(PA_i - A_iP) \leq r \qquad , \ i = 1,2$$

gelten, mit $\mathcal{O}(n \log n)$ Rechenoperationen miteinander multipliziert werden können.

Aufgabe 11: Zeigen Sie, daß die zyklische Faltung der Länge 2 mit 2 Multiplikationen (, Multiplikationen mit Konstanten werden dabei nicht berücksichtigt,) und 6 Additionen ausgeführt werden kann.

Aufgabe 12: Erstellen Sie ein nicht-rekursives Programm zur schnellen Fourier - Transformation nach Cooley - Tukey für $n = 2^p$ und testen Sie es an dem Beispiel $n = 8$ und

$$x(0) = 2.0,\ x(1) = x(7) = -0.85355,$$

$$x(2) = x(4) = x(6) = 0.0,$$

$$x(3) = x(5) = -0.146446$$

Prof. Dr. F. Natterer

WS 85/86
Blatt 4

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Fr., 15.11.85, 9.15 Uhr

Aufgabe 13: Zeigen Sie, daß sich die Koeffizienten des Produkts zweier Polynome f,g in $F[z]/z^n - 1$ durch zyklische Faltung der Koeffizienten von f und g berechnen.

Aufgabe 14: Erstellen Sie ein Programm für den Bruun'schen Algorithmus im Falle $n = 8$, welches mit 3 reellen Multiplikationen auskommt.
(Hinweis: Die Multiplikation mit i wird natürlich nicht mitgezählt.) Abgabe: Fr., 22.11.85

Aufgabe 15: Für $n = 4^p$ kann man die Cooley-Tukey FFT auch so ausführen, daß man die Fourier-Transformation der Länge n auf 4 Transformationen der Länge $n/4$ zurückführt.
Zeigen Sie, daß man auf diese Weise mit

$$M(n) = \frac{3}{2} n \log_2 n + O(n)$$

$$A(n) = \frac{11}{4} n \log_2 n + O(n)$$

reellen Multiplikationen bzw. Additionen auskommt.

(Hinweis: Siehe Hinweis zu Aufgabe 14.)

Aufgabe 16: Lösen Sie mit Hilfe des euklidischen Algorithmus':

$10 \cdot 135 - 16 \cdot 84$

i) $135x + 84y = 6$ in $\mathbb{Z}$,

$11 \cdot 7 \cdot 3 \cdot 2 \cdot 5$

ii) $x \equiv 7 \mod 30$ $\quad$ $30 \cdot 77$

$7 \cdot 11 / 3 \cdot 10$ $\quad$ $x \equiv 0$ $\quad$ $x = \lambda 30 + 7$

$x \equiv 5 \mod 77$ in $\mathbb{Z}$, $\quad$ $x = \mu 77 + 5$

iii) $f \equiv 2z^2 + 7 \mod z^3 - 1$

$f \equiv z^3 + z + 1 \mod z^4 + 1$ in $\mathbb{R}[z]$.

$135 = 84 \cdot 1 + 51$
$84 = 51 \cdot 1 + 33$
$51 = 33 \cdot 1 + 18$
$33 = 18 \cdot 1 + 15$
$18 = 15 \cdot 1 + 3$ $\quad$ $3 = 18 - 15 = \cancel{\ldots}\, 33 - 33 + 2 \cdot 18$
$15 = 3 \cdot 1 + 0$

$= -3 \cdot 33 + 2 \cdot 51 = 5 \cdot 51 - 3 \cdot 84 = 5 \cdot 135 - 8 \cdot 84$

WS 85/86

Blatt 5

Vorlesung "Effiziente Algorithmen"

.85, 9.15 Uhr

$p_1, \ldots, p_r$ paarweise teilerfremde natürliche

$\cdot \ldots \cdot p_r$.

ß die modulo p eindeutig bestimmte Lösung

en

mod p_i , $i = 1, \ldots, r$,

$$\sum_{=1} \left(\frac{p}{p_i}\right)^{\varphi(p_i)} a_i$$

$\left(\frac{p}{p_i}\right)^{\varphi(p_i)}$ $\left(\frac{p}{p_i}\right)^{\varphi(p_i)} \equiv 1 \bmod p_i$ ✓

φ ist dabei die Euler'sche φ - Funktion.

lieses Resultat zu einer alternativen Lösung

ii).

Sie ein erzeugendes Element für die Gruppe

3, 9, 2, 6, 18, 4, 12, ~~11, 22, 16, 23, 21, 15, 14, 13~~, 1

11, 8, 24, 22, 16, 23, 19, 7, 21, 13, 14, 17, 1

Sie einen Algorithmus für die zyklische Faltung

cher mit 5 Multiplikationen auskommt. Vorberech-

ler Faktoren werden dabei nicht gezählt.

$= n_1 \cdot \ldots \cdot n_r$ mit paarweise teilerfremden

rphie

8, 1, 8

~~2455~~

$\oplus \ldots \oplus M_{n_r}$.

1, 2, 4, 5, 7, 8 → 1, 2, 8

3 · 4

2 · 7 : 14 4

$\to (\mathbb{Z}/p\mathbb{Z})^*$

Prof. Dr. F. Natterer

$s_0 = y_0 + i y_1,\ s_1 = y_0 - i y_1$

WS 85/86

Blatt 6

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Fr., 29.11.85, 9.15 Uhr

Aufgabe 21: ~~Geben~~ Berechnen Sie einen Algorithmus zur Fourier-Transformation der Länge 5 ~~an~~, welcher mit 5 Multiplikationen und 17 Additionen auskommt. (Vorberechnungen werden nicht gezählt.)

Aufgabe 22: Sei $\mathbb{F}$ ein Körper. Zeigen Sie, daß die Unterräume

$$V_1 = \mathrm{sp}\left\{\begin{pmatrix}1\\1\\1\end{pmatrix}\right\} \left(= \text{der von } \begin{pmatrix}1\\1\\1\end{pmatrix} \text{ aufgespannte Raum}\right) \quad \text{und}$$

$$V_2 = \mathrm{sp}\left\{\begin{pmatrix}1\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\end{pmatrix}\right\} \quad \text{des } \mathbb{F}^3 \text{ unter jeder zyklischen}$$

Faltung mit Elementen aus $\mathbb{F}^3$ invariant bleiben, und leiten Sie daraus einen Algorithmus zur zyklischen Faltung ab, welcher mit 4 Multiplikationen auskommt.

Aufgabe 23: Zeigen Sie die Invarianz der Unterräume

$$V_1 = \mathrm{sp}\left\{(1,1,1,1)^T\right\},\ V_2 = \mathrm{sp}\left\{(1,-1,1,-1)^T\right\},\ V_3 = \mathrm{sp}\left\{(1,0,-1,0)^T, (0,1,0,-1)^T\right\}$$

des $\mathbb{F}^4$ unter zyklischen Faltungen mit Elementen des $\mathbb{F}^4$, und leiten Sie daraus einen Algorithmus zur zyklischen Faltung ab, der mit 5 Multiplikationen auskommt.

Aufgabe 24: Bestätigen Sie folgende Tabelle für die Anzahl der ~~komplexen~~ vollen Rechenoperationen für die Fourier-Transformation der Länge n:

n	Mult.	Add.
120	288	2076
240	648	5016
420	1296	11352

$18 \cdot 7\ \ 7 + 5 \cdot 24$

180
126
306

320

80 . 6

480

~~30~~

676 · 3
2028

$M(24)A(5) + 5 \cdot A(24)$

$M(48)A(5) + 5\,A(48)$

$M(20)A(21) + 21\,A(20)$

648

15 · 26
300
90
390

$$\sum_{n=1}^{\infty} (1+z) n \cdot a_n \cdot z^{n-1} = \alpha \sum_{n=0}^{\infty} a_n z^n$$

$a_0 = 1$

$(z+1)^{\alpha}$

$\Downarrow$

$$h(z) := f_\alpha(z) \cdot \exp(-\alpha \log(z+1)) = 1$$

$$\Rightarrow h'(z) = f_\alpha' \cdot \exp(-\alpha \log(z+1))$$

$$+ f_\alpha (-1) \alpha \log'(1+z) \exp(-\alpha \log(z+1))$$

$$= \exp(-\alpha \log(z+1)) \cdot$$

$$\left(f_\alpha' - \alpha f_\alpha(z) \log'(1+z)\right)$$

$$\parallel$$

$$= \left(\frac{\alpha}{1+z} f_\alpha - \frac{\alpha}{1+z} f_\alpha(z)\right)$$

$\frac{1}{n} a \geq \frac{1}{n+1}\left(a + \frac{(-1)^{n+1}}{n+1}\right)$ $\qquad \ln 2$

$\frac{1}{n} a \geq \frac{(-1)^{n+1}}{(n+1)^2} \qquad a \geq \frac{(-1)^{n+1}}{(n+1)^2} n$

$s_0 = y_0 + i y_1, \; s_1 = y_0 - i y_1$

$\nu s_3 + \nu s_4 + \mu s_3 + \mu s_4 - \mu s_4 - \nu s_3$ $\qquad m_0 = \left(\frac{-ix_0 - x_1}{2}\right) s_0, \; m_1 = \left(\frac{ix_0 - x_1}{2}\right) s_1$

$\nu s_4 + \mu s_3$ $\qquad s_2 = i(m_0 - m_1) \;\Big|\; s_3 = m_0 + m_1$

$$= \frac{x_0 - ix_1}{2}(y_0 + iy_1) - \frac{-x_0 - ix_1}{2}(y_0 - iy_1) \;\Big|\; \frac{-ix_0 - x_1}{2}(y_0 + iy_1) + \left(\frac{ix_0 - x_1}{2}\right)(y_0 - iy_1)$$

$= x_0 y_0 + x_1 y_1$ $\qquad = x_0 y_1 - x_1 y_0$ ✓

$$\frac{x_0 + ix_1}{2} s_0, \; \frac{x_0 - ix_1}{2} s_1$$

Prof. Dr. F. Natterer WS 85/86

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Fr., 13.12.85, 9.15 Uhr

Aufgabe 29: Man gebe eine Liste sämtlicher irreduzibel nicht - äquivalenter Darstellungen von D_n für ungerades n an. Weisen Sie nach, daß die Darstellungen wirklich irreduzibel sind, und daß Ihre Liste vollständig ist.

Aufgabe 30: Man zeige, daß eine irreduzible Darstellung einer abelschen Gruppe den Grad 1 hat.

Aufgabe 31: Sei G eine Gruppe, H eine Untergruppe von G und ρ eine Darstellung von G in V.

i) Zeigen Sie, daß $\sigma := \mathrm{Rest}_H(\rho)$ (= die Restriktion von ρ auf H) eine Darstellung von H in V ist.

ii) Geben Sie ein Beispiel dafür an, daß σ für ein irreduzibles ρ reduzibel sein kann.

Aufgabe 32: Sei G eine endliche Gruppe und H ein Normalteiler von G vom Index r. $G = s_1 H \cup \ldots \cup s_r H$ sei die zugehörige Nebenklassenzerlegung von G. Dann gibt es zu jedem $g \in G$ eine Permutation $\pi(g) \in S_r$ mit $g s_\ell \in s_{\pi(g)(\ell)} H$.

$\left.\begin{array}{l} g s_\ell \in s_k H \\ g s_m \in s_k H \end{array}\right\}$ $\left.\begin{array}{l} s_k^{-1} g \in H s_\ell \\ s_k^{-1} g \in H s_m \end{array}\right\}$ $\left\{\begin{array}{l} = s_\ell H \\ = s_m H \end{array}\right.$

Zeigen Sie:

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

ii) Ist σ eine Darstellung von H in V und für $\ell = 1,\ldots,r$

$\rho_\ell : G \to Gl(V,V)$

$$\rho_\ell(g) := \sigma(s^{-1}_{\pi(g)\ell}\, g\, s_\ell) \quad , \quad g \in G$$, $\rho_k(s^\ell)(x) := e^{2\pi i k\ell/n} x$

so gilt $\rho_\ell(g_1 g_2) = \rho_{\pi(g_2)\ell}(g_1)\, \rho_\ell(g_2)$.

$\rho_k(s^\ell \cdot s^m)(x)$

$= \rho_k(s^{(\ell+m) \bmod n})(x)$

$g_1 s_\ell \in s_{\pi(g_1)(\ell)} H$

$g_2 s_\ell \in s_{\pi(g_2)(\ell)} H$

$g_1 g_2 s_\ell \in \underbrace{g_1 s_{\pi(g_2)(\ell)}}_{s_{\pi(g_1)\pi(g_2)(\ell)} H} H$

$\rho_\ell(g_1 g_2) = \sigma(s^{-1}_{\pi(g_1)\pi(g_2)(\ell)}\, g_1 g_2 s_\ell)$

$\rho_{\pi(g_2)(\ell)}(g_1) = \sigma(s^{-1}_{\pi(g_1)\pi(g_2(\ell))} g_1 s) \sigma(s^{-1}_{\pi(g_2)(\ell)}\, g_2 s_\ell)$

$= \sigma(s^{-1}_{\pi(g_1)\pi(g_2(\ell))}\, g_1 \underbrace{s_{\pi(g_2)(\ell)} s^{-1}_{\pi(g_2)(\ell)}}_{1} g_2 \cdot s_\ell)$

$= \sigma(s^{-1}_{\pi(g_1)\pi(g_2(\ell))}\, g_1 g_2 s_\ell)$

iii) Die Abbildung $\rho : G \to GL(V^r)$, die für $u = (u_1^*, \dots, u_r^*)^T \in V^r$ definiert ist durch

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

ist eine Darstellung von G in V^r.

(ρ heißt die von σ induzierte Darstellung.)

$\cancel{(\rho(g_1)\cdot\rho(g_2)\cdot u)_\ell} = \rho(g_1 g_2)_\ell$ $\qquad \pi(g_1 g_2)\cdot\pi(g_2 g_1)^{-1}$

$\cancel{\rho(g_1 g_2)_\ell = \rho_{\pi(g)^{-1}(\ell)}(g)\, u_{\pi(g)^{-1}(\ell)}}$

$(\rho(g_1 g_2)\cdot u)_\ell = \rho_{\pi(g_1 g_2)^{-1}(\ell)}(g_1 g_2)\, u_{\pi(g_1 g_2)^{-1}(\ell)}$

$= \rho_{\pi(g_2)\pi(g_1 g_2)^{-1}(\ell)}(g_1)\, \rho_{\pi(g_1 g_2)^{-1}(\ell)}(g_2)\, u_{\pi(g_1 g_2)^{-1}(\ell)}$

$\rho(g_1)\rho(g_2)\cdot u_\ell = \left(\rho(g_1)\left(\rho_{\pi(g_2)^{-1}(\ell)}(g_2)\, u_{\pi(g_2)^{-1}(\ell)}\right)\right)_\ell$

$\rho_{\pi(g_1^{-1})\ell}(g_1)\left(\rho_{\pi(g_2)^{-1}(\ell)}(g_2)\, u_{\pi(g_2)^{-1}(\ell)}\right)_{\pi(g_1)^{-1}(\ell)}$

$f(x)_\ell = f_\ell(x_\ell)$ $\qquad (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}$

Prof. Dr. F. Natterer WS 85/86

Blatt 9

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Fr., 20.12.85, 9.15 Uhr

Aufgabe 33:

i) Zeigen Sie: Ist ρ eine irreduzible Darstellung von G in V mit Charakter χ und $d = \dim V$, so gilt für $r, s \in G$

$$\frac{\chi(r)\chi(s)}{d} = \frac{1}{|G|} \sum_{t \in G} \chi(st^{-1}rt)$$

ii) Vervollständigen Sie den Beweis zu Satz 11.8.

Aufgabe 34: Sei ρ eine Darstellung der Gruppe G in V, M sei der Vektorraum der linearen Abbildungen von V, die die Symmetrien von ρ besitzen, und es gelte $\rho = c_1\rho_1 + \ldots + c_m\rho_m$ mit irreduziblen und paarweise inäquivalenten Darstellungen ρ_i.

Zeigen Sie, daß $\dim(M) = \sum_{i=1}^{m} c_i^2$ gilt. $\begin{pmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \\ a_2 & a_3 & a_1 \end{pmatrix}$

Aufgabe 35: Seien $p, q \in \mathbb{C}$ und $f(x) = x^3 + px + q$.

i) Bestimmen Sie eine zyklische Faltung A der Länge 3, so daß f das charakteristische Polynom von A ist.

ii) Berechnen Sie die Eigenwerte von A nach Satz 12.1.

iii) Geben Sie Formeln an für die Nullstellen von f (Cardanische Formeln).

Aufgabe 36: Sei A eine komplexe (n,n)-Matrix der Form

$$A = \begin{pmatrix} A_1 & A_2 \\ A_2 & A_1 \end{pmatrix}.$$

i) Geben Sie eine Gruppe G und eine Darstellung ρ von G in $\mathbb{C}^n$ an, so daß alle Matrizen A dieser Form die Symmetrien von ρ haben.

ii) Nehmen Sie die Ausreduktion von ρ vor und geben Sie die zugehörige direkte Zerlegung von $\mathbb{C}^n$ an.

iii) Bringen Sie A auf die Form wie in Satz 12.1.

iv) Geben Sie mit Hilfe von iii) einen Algorithmus zur Lösung von $Ax = b$ an, der mit $\frac{1}{12} n^3 + O(n^2)$ Multiplikationen und Additionen sowie n Divisionen auskommt. (Alle Operationen hierbei sind komplex.)

v) Vergleichen Sie Ihr Resultat mit dem Ergebnis des Faltungssatzes für die Fourier-Transformation der Länge 2, ausgeführt auf Blocks der Länge $n/2$.

Prof. Dr. F. Natterer

WS 85/86
Blatt 10

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Fr., 10.01.86, 9.15 Uhr

Aufgabe 37: 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~~ keine Vorberechnungen !) mit n Divisionen und

reg. Darst. der zykl. Gruppe

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

in den Kästchen mult.

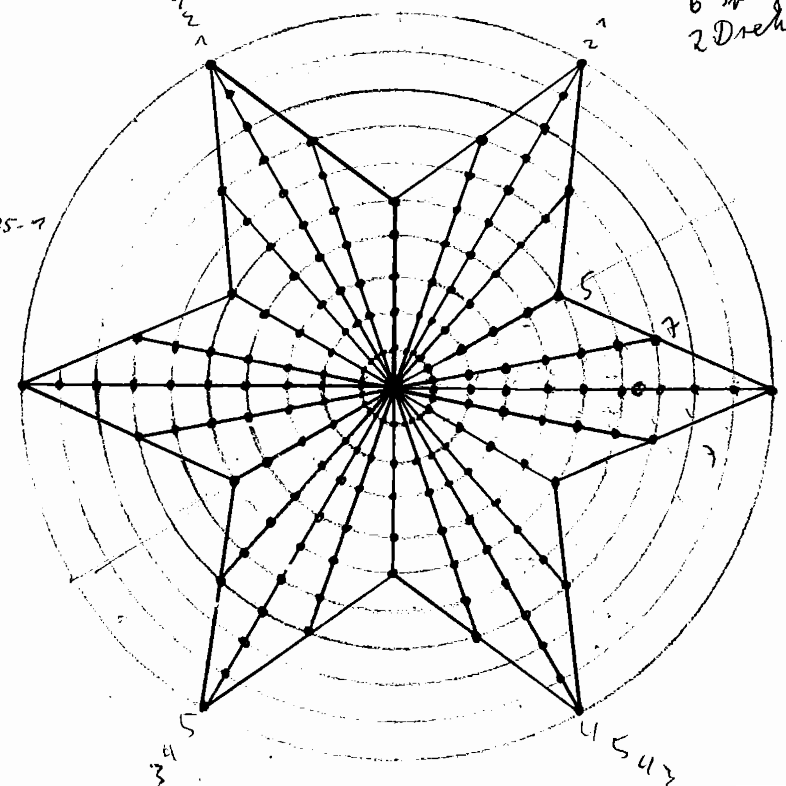
$(x+i)(x-i)$

Aufgabe 38: Sei ρ die natürliche Darstellung von D_4 auf einem 4×4 Gitter, und sei A eine 16×16 - Matrix mit den Symmetrien von ρ. Konstruieren Sie nach Satz 12.1 eine Orthonormalbasis von $\mathbb{C}^{16}$, so daß A bezüglich dieser Basis in je zwei Matrizen der Größe 1, 3 und 4 zerfällt.

Aufgabe 39: Sei A eine 175×175 Matrix, welche die Symmetrien des Weihnachtssterns (siehe Abb.) hat. (D.h.: Ist P die Permutation der Punkte des Sterns, welche von einer den Stern in sich überführenden Bewegung erzeugt wird, so ist $P^T A P = A$.)

6 Spiegelungen 12
6 Drehungen D_6
D_{10}

$22 \cdot 6 + 42$
$= 132 + 42 = 175 - 1$



$\frac{29 \cdot 6}{174}$

D_6

$6 \cdot 29$

$12 = 4 + 2 \cdot 4$
$20 = 4 + 4 \cdot 4$

O : 1
I : 7
II : 10
III : 5

$Z_{nat}(1) = 175.$
$Z_{nat}(r^k) = 1.$
$Z_{nat}(s) =$ Anzahl Symm. III.
$Z_{nat}(s r^{2k}) =$ Anzahl Symm. II

175

$\cancel{4 \cdot 29} =$ $29 \cdot 4$ / 116 / 59 / 175

Zeigen Sie, daß A bei der Anwendung von Satz 12.1 in 8 Matrizen der Dimensionen 23, 7, 12, 17, 29, 29, 29, 29 zerfällt.

30 42 59 29 · 3

Aufgabe 40: (Abgabe 17.01.86)

Erstellen Sie ein Programm, welches für die natürliche Darstellung ρ der Gruppe D_n auf einer gegen D_n invarianten Punktmenge die Ausreduktion vornimmt. Testen Sie Ihr Programm an dem Weihnachtsstern aus Aufgabe 39. $n = 2m, 2m+1$!

$1 \quad r \quad r^2 \quad r^3 \quad s \quad sr \quad sr^2 \quad sr^3$

$2\mathrm{I}+n_6 \quad 2\mathrm{II}+n_6 \quad 2\mathrm{II}+n_6 \quad 2\mathrm{III}+n_6$

$2u_2+n_0 \quad 2u_3+n_0 \quad 2u_2+n_0 \quad 2u_3+n_0$

ω^k

$(-\omega)^k$

$\omega^k + (-\omega)^k$

$= e^{2\pi i k/n} + e^{-2\pi i k/n}$

$= 2\cos(2\pi k/n)$

$r^k \quad sr^k$

$z(\rho_1) \quad 1 \quad 1$

$z(\rho_2) \quad 1 \quad -1$

n gerade $\begin{cases} z(\rho_3) & (-1)^k \quad (-1)^k \\ z(\rho_4) & (-1)^k \quad (-1)^{k+1} \end{cases}$

$z(\rho_5^h) \quad 2\cos(2\pi hk/n) \quad 0$

9820

9832

30-92

$(\hat{f}_3(\xi)) / \hat{f}_\varepsilon(\xi)$ $\quad x \to \frac{x}{\varepsilon^2}$

Prof. Dr. F. Natterer $\quad \hat{f}(2\xi) = 2^{-n}\hat{f}(\frac{\xi}{2})$ $\quad$ WS 85/86

$\hat{f}(2\xi) = e^{i\xi\xi}\hat{f}(\xi)$ $\quad$ Blatt 11

ε^{-2n}

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Fr., 17.01.86, 9.15 Uhr $\quad \int_{\mathbb{R}^n} f(\varepsilon\cdot x)e^{-ix\xi}dx$

$\int_{\mathbb{R}^n} f(\frac{x}{\varepsilon})e^{-ix\xi}dx$

Aufgabe 41: a) Seien $f,g \in \mathcal{S}(\mathbb{R}^n)$. Zeigen Sie:

i) Für $f_\varepsilon(x) := f(\varepsilon\cdot x)$, $0 \neq \varepsilon \in \mathbb{R}$, gilt $[\hat{f}_\varepsilon(\xi)] = \varepsilon^{-n}\,\hat{f}(\frac{\xi}{\varepsilon})$. e^{ε}

ii) Für $f_y(x) := f(x+y)$, $y \in \mathbb{R}^n$, gilt $\hat{f}_y(\xi) = e^{iy\xi}\,\hat{f}(\xi)$.

$\int f(x)e^{-ix\xi}$

iii) $\int\limits_{\mathbb{R}^n} f(x)\hat{g}(x)dx = \int\limits_{\mathbb{R}^n} \hat{f}(\xi)g(\xi)d\xi$ $\quad = \int f(x)e^{-i(x-y)\xi}$

iv) Ist α ein Multiindex, so gilt $(D^\alpha f)^\wedge(\xi) = i^{|\alpha|}\,\xi^\alpha\,\hat{f}(\xi)$.

v) Für $g(x) := x^\alpha f(x)$ gilt $\hat{g}(\xi) = i^{|\alpha|}\,D^\alpha\,\hat{f}(\xi)$. ✓

b) Bestimmen Sie einen Fixpunkt der Fourier-Transformation, d.h. ein $f \in \mathcal{S}(\mathbb{R}^n)$ mit $\hat{f} = f$. (e^{-x^2})

Aufgabe 42: Sei $F(\sigma) = \begin{cases} 1 & |\sigma| \leq b \\ 0 & \text{sonst} \end{cases}$ und $\hat{\gamma}(\sigma) = F(\sigma)|\sigma|$.

Berechnen Sie γ .

Aufgabe 43: Sei $f \in \mathcal{S}(\mathbb{R}^n)$ und $g = Rf$. Die Abbildung J^{n-1} auf $\mathcal{S}(\mathbb{R}^n)$ sei definiert durch $(J^{n-1}h)^\wedge(\xi) = |\xi|^{n-1}\hat{h}(\xi)$.

Zeigen Sie

$\text{II}: \hat{f}(\xi+\xi) = e^{i\xi\xi}\hat{f}(\xi)$

$$f = \frac{1}{2}(2\pi)^{1-n}\,J^{n-1}(R^* g) \ .$$

$\hat{f}(\xi+\xi) = \varepsilon^{-2}\hat{f}(\frac{\xi}{2})$

Aufgabe 44: Geben Sie für $n = 2$ einen Rekonstruktionsalgorithmus an, der auf der Inversionsformel aus Aufgabe 43 basiert, und bestimmen Sie die Anzahl der notwendigen Rechenoperationen.

$f(\xi)\hat{g}(\xi)$

$\hat{f}(\xi) = (2\pi)^{-n/2}\int_{\mathbb{R}^n} f(x)e^{-ix\xi}dx$ $\quad = \int_{\mathbb{R}^n} g(x)e^{-ix\xi}dx$

$\int_{\mathbb{R}^n} f(\frac{x}{\varepsilon})e^{-ix\xi}dx$ $\quad \int_{\mathbb{R}} \sim \int_{\mathbb{R}}$

$\int_{\mathbb{R}^n} f(x)e^{-ix\varepsilon\xi}dx\cdot\varepsilon^n$

$$\int_{\mathbb{R}^n} f_\varepsilon(x)\, e^{-i\xi x}\, dx \qquad \int_{\mathbb{R}^n} f(x)\, e^{-i\frac{\xi}{\varepsilon}\cdot x}\, dx$$

$$\parallel$$

$$\int_{\mathbb{R}^n} f(\varepsilon x)\, e^{-i\xi x}\, dx$$

$$\rightarrow x \rightarrow \frac{x}{\varepsilon} \qquad \varepsilon^{-n}$$

$$\varepsilon^{-n}\int_{\mathbb{R}^n} f(x)\, e^{-i\frac{\xi x}{\varepsilon}}\, dx \qquad \int_{\mathbb{R}^n} f(x)\, e^{-i\xi x}\, dx$$

$$\tilde{f}(x) = (2\pi)^{-n/2} \int_{\mathbb{R}^n} \hat{f}(\xi)\, e^{i\xi x}\, d\xi = f(x)$$

$$f(x) = c \int \hat{f}(\xi) e^{i\xi x} d\xi$$

$$= c \int_{|\xi| \le b} |\xi|\, e^{i\xi x}\, d\xi$$

$$f(x) = 2\pi^{-n/2} \int_0^\infty \int_{S^{n-1}} \sigma^{n-1} \hat{f}(\sigma w)\, e^{i\sigma w x}\, dw\, d\sigma$$

raus: $f(x) = \frac{1}{2}(2\pi)^{1-n}\, J^{n-1}\, R^* g$

$= \frac{1}{2}(2\pi)^{1-n}\, J^{n-1}$

Prof. Dr. F. Natterer WS 85

Blatt

$U a_i C_n$

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Fr., 24.01.86, 9.15 Uhr

abelsch ?

Aufgabe 45: Sei G_n eine Gruppe mit $|G_n| \leq cn$ und C_n als Untergruppe. NT ?
Zeigen Sie, daß man für $n = 2^k$ die Faltung auf G_n in $O(n \log n)$ Operationen durchführen kann. ✓

Aufgabe 46: Zeigen Sie, daß die Fourier-Transformation auf D_n und ihre Inverse für $n = 2^k$ in $\mathcal{O}(n \log n)$ Operationen durchgeführt werden kann. ✓

Aufgabe 47: Die (n,n)-Matrix A sei eine Faltung auf einer Gruppe G (d.h. A hat die Symmetrien der regulären Darstellung von G). Man zeige:

a) Das lineare System $Ax = b$ läßt sich in $\mathcal{O}(n^2)$ Operationen lösen, wenn ein vollständiges System irreduzibler Darstellungen von G zur Verfügung steht. ✓

b) Diese Anzahl reduziert sich auf $\mathcal{O}(n^{3/2})$, wenn dies für die Fourier-Transformation und ihre Inverse auf G der Fall ist.

c) Für $G = D_n$ und $n = 2^k$ kommt man mit $\mathcal{O}(n \log n)$ Operation aus.

Aufgabe 48: Sei G eine abelsche Gruppe. Man zeige, daß für die Fourier-Transformation und ihre Inverse auf G die gleiche Anzahl von Operationen benötigt wird.

s_i $a_1 s_1$

s_k $a_1 s_4$

$f(s_i s_k^{-1})$ $f(a_1 s_4 s_1 a_1^{-1})$

Prof. Dr. F. Natterer

$\hat{R}f$ ausdrücken in $\hat{\chi}_S, \hat{f}$; $(\hat{\chi}_S(\rho^{-1}))^{-1}$ inj, $\hat{Rf}$

$\hat{h}$ ausdrücken in $\hat{f}$, $\hat{Rf}$

Ws 85/86

Blatt 13

platt

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe/ Fr. 31.01.86, 9.15 Uhr

Aufgabe 49: Sei G das direkte Produkt der Gruppen $H_1, \ldots, H_r$.

a) Man zeige, daß die Fourier-Transformation auf G mit

$$|G| \sum_{i=1}^{r} |H_i|^{(1)?}$$

Operationen (eine Operation = eine komplexe Multiplikation + eine komplexe Addition) ausgeführt werden kann.

(Satz von Atkinson - Karpovski)

Tensor

b) Man zeige, daß die Hadamard - Walsh - Transformation der Länge $n = 2^r$ mit $2n \log_2 n$ Additionen ausgeführt werden kann.

Dimension des Raums

Aufgabe 50: Sei G eine (abelsche?) Gruppe und $S \subseteq G$. Die Radon-Transformation auf G (bezüglich S) ist für $f : G \to \mathbb{C}$ erklärt durch

$G = \{0,1\}$, $S = \{0,1\}$, $Rf = f(0)+f(1)$

$$Rf(y) = \sum_{x \in Sy} f(x) \quad .$$

$\widehat{h*g} = (\hat{h} \cdot \hat{g})$

$\hat{h} \cdot \hat{g} = \frac{1}{n^2}(h*g)$

Sei χ_S die charakteristische Funktion von S und

$$h(x) = \sum_{\rho \in \hat{G}} d_\rho \; \mathrm{tr}\,\big((\hat{\chi}_S(\rho^{-1}))^{-1} \rho(x^{-1}) \big)$$

$\sum_{t \in S} \rho(t)^{-1}$

$\sum_{\rho \in \hat{G}} d_\rho \, \mathrm{tr}\big((\sum_{t \in S} \rho(xt))^{-1} \big)$

$1, a, a^2, a^3 / \{1, a\}$

Man zeige die Inversionsformel

$\rho : G \to L(V)$, $\rho(x) : V \to V$, $1, a^2$, a, a^3

$\rho^{-1} : L(V) \to G$??? $(\rho(x))^{-1} : V \to V$

$\hat{f} = (\widehat{h * Rf}) = \hat{h} \cdot \hat{Rf}$

$$f = h * Rf \quad ,$$

$\in \hat{G}$???

$(\rho^{-1})(x) := \rho(x)^{-1}$

$(\rho^{-1})(xy) = \rho(xy)^{-1} = \rho(y)^{-1}\rho(x)^{-1} = \rho^{-1}(y)\,\rho^{-1}(x)$

welche immer dann gilt, wenn $\hat{\chi}_S(\rho^{-1})$ für jedes $\rho \in \hat{G}$ invertierbar ist.

keine Darstellung?

Aufgabe 51: Sei G das direkte Produkt von k Faktoren $C_2 = \{0,1\}$, und S bestehe aus den Elementen von G, welche genau eine positive Komponente haben. Man zeige mit Hilfe der Aufgaben 49 und 50:

$f : A \to B$, $g : B \to C$

a) Die Radon - Transformation R auf G (bez. S) ist genau dann invertierbar, wenn k ungerade ist. triv!

$f(g(x)) = x$, $f : A \to B'$ inj. surj., $g : B \to$ inj.

b) Ist k ungerade, so kann man R in $\mathcal{O}(k\,2^k)$ Operationen (eine Operation = eine Addition oder eine Multiplikation oder eine Division) invertieren.

$\hat{h} = h$; $(\hat{\chi}_S(\rho^{-1}))^{-1} = \hat{h}$

Nebenklassen / Tensor

<u>Aufgabe 52:</u> Sei G eine abelsche Gruppe, also das direkte Produkt zyklischer Gruppen der Ordnungen $p_1^{q_1},\dots,p_r^{q_r}$, mit Primzahlen $p_1,\dots,p_r$.

Man zeige, daß die Fourier-Transformation auf G in

$\mathcal{O}\left(|G| \sum_{i=1}^{r} q_i p_i\right)$ Operationen (eine Operation = eine komplexe Multiplikation + eine komplexe Addition) ausgeführt werden kann.

$p_i^{q_i}$ $|H_1|$

$C_{p_i^{q_i}}$

$H_1 \circ H_2 \leq |H_1| L(H_2) + |H_2| L(H_1)$

$\rho_{reg} = \Sigma\, d_i \rho_i$

ρ $a^{\Sigma d_i \rho_i} = \Pi\, a^{d_i \rho_i}$

$\hat{f}(\rho) = \sum_{t\in G} f(t)\rho(t)$

$Tr(A^{-1})$

$\hat{h}(\rho) = \sum_{t\in G} \left(\sum_{\mu\in\hat{G}} d_\mu Tr\left(\left(\sum_{s\in S} \mu(ts)\right)^{-1}\right)\rho(t)\right)$

$\hat{Rf}(\rho) = \sum_{t\in G} \left(\sum_{s\in S} f(st)\right)\rho(t)$

$\hat{h}\cdot\hat{Rf}(\rho) = \sum_{t\in G}\sum_{t'\in G}\sum_{\mu\in\hat{G}}\sum_{s\in S} d_\mu Tr\left(\left(\sum_{s\in S}\mu(ts)\right)^{-1}\right)\rho(t) f(st')\rho(t')$

$= \sum_{t\in G}\sum_{t'\in G}\left[\sum_{\mu\in\hat{G}}\sum_{s\in S} d_\mu Tr\left(\left(\sum_{s\in S}\mu(ts)\right)^{-1}\right) f(st')\right]\rho(tt')$

$) \; f(t) = \sum_{t'\in G}\sum_{\mu\in\hat{G}}\sum_{s\in S} d_\mu Tr.\, f(st')\rho(t')$

$|H| = p_1$

$L(G) \leq |H|\, L(G/H) + |G| + |G/H|\, L(H)$

$\{(a,b)\}_{a.3\; a.3}$

Prof. Dr. F. Natterer

WS 85/86

Blatt 14

Übungen zur Vorlesung "Effiziente Algorithmen"

Abgabe: Fr., 7.2.86, 9.15 Uhr

Aufgabe 53: Sei G das direkte Produkt der Gruppen $H_1, \dots, H_r$. Zeigen Sie, daß die inverse Fourier-Transformation auf G in $|G| \sum_{i=1}^{r} |H_i|$ Operationen (= 1 Mult. + 1 Add.) berechnet werden kann.

Aufgabe 54: P, Q seien konvexe Polygone mit je n Ecken. Für P, Q seien je eine BHR gegeben. Zeigen Sie, daß sich der Abstand von P, Q in $\mathcal{O}(\log n)$ Operationen berechnen läßt.

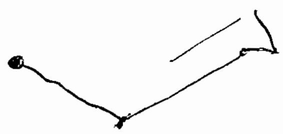
Aufgabe 55: Seien zwei konvexe Polygone P, Q mit je n Ecken gegeben. Zeigen Sie, daß man

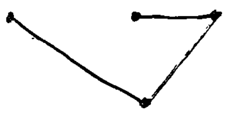
$$\max \{ |x - y| : x \in P \ , \ y \in Q \}$$

in $\mathcal{O}(n)$ Rechenoperationen bestimmen kann.

Aufgabe 56: Seien A, B Mengen in der Ebene mit n bzw. m Elementen. Zeigen Sie, daß man in $\mathcal{O}((n+m) \log(n+m))$ Operationen entscheiden kann, ob es eine Gerade gibt, die A und B trennt.

$O(n \log(n))$ T r





Effiziente Algorithmen

I Einleitung

1) Multiplikation zweier b-närer Darstellungen

$x = x_0 + b x_1 + \dots + b^{n-1} x_{n-1}$ $\qquad 0 \le x_i < b \quad b \in \mathbb{N}$ Basis

$y = y_0 + b y_1 + \dots + b^{n-1} y_{n-1}$

$z = x \cdot y$?

Schulmethode: $214 \cdot 713$

642
2140
~~1498~~
149100
152582

$214 \cdot 713$
642
214
1498
152582

dcl (x(0:n-1), y(0:n-1), z(0:2n-1), u, h) bin fixed

z = 0;

do k = 0 to n-1; /* k-te Stelle von y */

u = 0 ; /* Übertrag (engl. carry) */

do l = 0 to n-1; /* x · y_k und aufaddieren */

h = x(l) * y(k) + u + z(k+l);

z(l+k) = MOD(h, b); /* MOD(h,b) = Rest bei Division durch b

u = (h - z(l+k)) / b;

end;

z(n+k) = u $\qquad n^2$ (Mult + Add) $= O(n^2)$

end;

Effizientes Verfahren: Karatsuba 1962 (Knuth, sec 4.3.3)

$n = 2^p$, $m = n/2$

$x = X_0 + b^m X_1$, $X_0 = x_0 + x_1 b + \dots + x_{m-1} b^{m-1}$, $X_1 = x_m + x_{m+1} b + \dots + x_{n-1} b^{m-1}$

$y = Y_0 + b^m Y_1$ $\qquad Y_0 = \dots \qquad Y_1 = \dots$

$xy = X_0 Y_0 + b^m (X_0 Y_1 + Y_0 X_1) + b^n X_1 Y_1$

$= (1 + b^m) X_0 Y_0 - b^m (X_1 - X_0)(Y_1 - Y_0) + (b^m + b^n) X_1 Y_1$

$T(n)$ = # Operationen für $x \cdot y$, d.h. zwei Zahlen der Länge n.

$T(n) \leq 3\,T(\frac{n}{2}) + c\,n$, c unabh. von n

$T(1) = 1$

$T_p = T(2^p)$, $T_p \leq 3\,T_{p-1} + c\,2^p$, $T_0 = 1$

Lemma 1.1 $T_{p+1} \leq q\,T_p + r_p$, $p = 0, 1, \ldots$ $T_p, q, r_i \geq 0$

$$\Rightarrow T_p \leq q^p T_0 + \sum_{j=0}^{p-1} q^{p-1-j} r_j$$

Bew. trivial:

$$\Rightarrow T_p \leq 3^p + c \sum_{j=0}^{p-1} 3^{p-1-j}\, 2^{j+1} = 3^p \left(1 + c \sum_{j=0}^{p-1} \left(\tfrac{2}{3}\right)^{j+1}\right) \leq 3^p \left(1 + \tfrac{1}{3}\tfrac{c}{1-\frac{2}{3}}\right)$$

$$= c'\,3^p$$

$n = 2^p$

$$\Rightarrow T(n) \leq c'\,3^p = c'\,n^{\log_2 3 \approx 1.585} \qquad \left(p^{\log_q n} = n^{\log_q p}\right)$$

$$= ~~O(\ldots)~~ = O(n^{1.585})$$

Progr.:

```
FMULT: proc(n, x, y, z);
if n = 1 then Berechne z = x·y durch einf. Mult.;
      else begin; m = n/2
            X0 = (x0 ... x_{m-1}); X1 = (x_m, ... x_{n-1});
            y0 = ---           ; y1 =
        call FMULT (m, x0, y0, z0);
        call FMULT (m, x1, y1, z1);
        call FMULT (m, x1-x0, y1-y0, z01);
      Setze z zusammen aus z0, z1, z01;
    end;
end FMULT;
```

4.3 : $A - MAM^{t} = \sum_{j=1}^{\alpha} x^{j} (y^{j})^{t}$

$\Leftrightarrow A = \sum_{j=1}^{\alpha} L(x_j)\, V(y_j)$

$\sigma \left(\frac{f(x)}{g(x)} \right) = \sigma (f(x)) \cdot \sigma^{-1} (g(x))$

$\sigma \left(\frac{f(x)}{g(x)} \cdot \frac{h(x)}{p(x)} \right)$

$= \sigma (f(x)) \cdot \sigma (h(x)) \cdot \sigma (g(x))^{-1} \cdot \sigma (p(x))^{-1}$

$= \sigma \left(\frac{f}{g} \right) \cdot \sigma \left(\frac{h}{p} \right)$

$\sigma \left(\frac{f}{g} + \frac{h}{p} \right) = \sigma \left(\frac{fp + hg}{gp} \right)$

$= \sigma (fp + hg) \cdot \sigma (gp)^{-1}$

$= \sigma(f) \cancel{\sigma(p)} \cdot \sigma (g)^{-1} \cdot \cancel{\sigma(p)^{-1}} = \sigma \frac{f}{g}\, \sigma \frac{h}{p}$

25 · 25
150
25
225
208
17

§2. Einige Grundbegriffe der Informatik

1. Komplexitätsmaße

$+, -, \cdot, /$, if, transport,
(eigentlich: $\log_2$(Adressraum), aber Einheitszeitmaß $O(1)$).
$O(\log n)$

2. Stack: Stapel, Keller

nil, push, pop $k(1:\infty)$. top, tos. pop $|$ tos $= 0 \Rightarrow$ Fehler! tos $= 0$. LIFO/FIFO.

3. Rekursive Prozeduraufrufe.

siehe Gries, Compiler Construction for digital Computers, Wiley '71.

Stack enthält: aktuelle Pars, lokale Vars, Rücksprungadresse
Adressen

```
max: proc(n) returns(); recursive;
  if n=1 then return (x_1)
      else begin
            y=max(n-1);
            if y>x_n then return(y)
                     else return(x_n)
      end;
```

```
max: proc(n) returns();
top=0;
k(1)=n;
k(3)=Ende  / top+1=n, top+2=Result, top+3=Rück
Aufruf: if k(top+1)=1 then k(top+2)=x_1; goto top
        else
        top=top+3; k(top+1)=(top-2)
        k(top+3)=Marke;
        goto Aufruf;
        end;
Marke: top=top-3; k(top+2)=max(k(top+5), x_{k(top+1)})
       goto k(top+3).
Ende: return(k(2)).
```

Kapitel II:

§3 Matmult und -inversion

§3. Strassen-Algorithmus. (Lit.: V. Strassen, Gaussian Elimination is not optimal, Num. Mathematik 13, 354-356 (1969)).

Ziel: Multiplikation zweier (n,n)-Mat. in $O(n^{\log_2 7})$ Operationen.

$A, B \in \mathbb{R}^{n\times n}$, n gerade. $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$, $B =$, $C = A\times B$.

Lemma 3.1: $C_{11} = I + IV - V + VII$, $C_{22} = I + III - II + VI$,
$C_{21} = II + IV$, $C_{12} = III + V$,

$I = (A_{11}+A_{22})(B_{11}+B_{22})$, $II = (A_{21}+A_{22})B_{11}$, $III = (A_{11})(B_{12}-B_{22})$, $IV = A_{22}(-B_{11}+B_{21})$,
$V = (A_{11}+A_{12})B_{22}$, $VI = (-A_{11}+A_{21})(B_{11}+B_{12})$, $VII = (A_{12}-A_{22})(B_{21}+B_{22})$.

7 Mult. statt 8, 18 Add. statt 4!

$$C_{11} = \cancel{A_{11}B_{11}} + A_{12}B_{11} + \underline{A_{11}B_{22}} + \cancel{A_{22}B_{22}} - A_{22}B_{11} + A_{22}B_{21} \underline{- A_{11}B_{22}} \cancel{+ A_{12}B_{22}} \cancel{+ A_{12}B_{21}}$$
$$- A_{22}B_{21} + A_{12}B_{22} - A_{22}B_{22}$$

Algorithmus: $n = m \cdot 2^p$.

$M_p = \#$ ~~Mult. von 2~~ $\#$ Mult. für Mult. von 2^p-Matrizen.
$A_p = \#$ Add. "

$M_{p+1} = 7 M_p$, $M_0 = m^3$
$A_{p+1} = 7 A_p + 18 \cdot (m \cdot 2^p)^2$, $A_0 = m^2 (m-1)$.
Auflösung nach Lemma 1.1: $M_p = 7^p \cdot m^3$; $A_p = 7^p \cdot m + 18 m^2 \overbrace{\sum_{l=0}^{p-1} 2^{2l} 7^{p-1-l}}^{} \leq 7^{p-1} \frac{1}{1-\frac{4}{7}}$.

$$\Rightarrow A_p = O(7^p \cdot m^3),$$

$M(n) = \#$ Mult für $(n,n) = n^{\log_2 7}$
$A(n) = \#$ Add " " $= O(n^{\log_2 7})$.

Satz 3.2: Zwei (n,n)-Matrizen können in $O(n^{\log_2 7})$ Operationen mult. werden.

Bemerkung: $M(n) \leq 7 n^{\log_2 7}$, $A(n) \leq 42\, n^{\log_2 7}$.

Strassen-Multiplikation mit $n = 2^k \cdot m$

$M(n) = 7^k \cdot m^3$

$A(n) = 7^k \cdot m^3 + 5m^2\, 7^k - 6(m\, 2^k)^2$

Optimale Bestimmung von m:

$m = 1$: $M(n) = 7^k$, $A(n) = 6 \cdot 7^k - 6n^2$. $(7^k = n^{\log_2 7})$.
$m = n$: $M(n) = n^3$, $A(n) = n^3 - n^2$

Für welche m bringt Halbierung Vorteil?

Schulmethode: $2m^3 - m^2$ Rechenops; Strassen: $7\left(2\left(\frac{m}{2}\right)^3 - \left(\frac{m}{2}\right)^2\right) + 18\left(\frac{m}{2}\right)^2$ Rechenops + Schulmeth.

Schul schlechter $\Leftrightarrow \frac{m^3}{4} > \frac{15 m^2}{4} \Leftrightarrow \underline{m > 15}$.

~~FMAMV(n,A,B,C)~~
FMAMV: proc(n,A,B,C);
if $n < 16$ Then Schulmethode;
Else if n gerade then Halbierung und rek. Aufruf;
Else
$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$, $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$; mit A_{11}, B_{11} $(n-1)$-Matr.
Rest Zeilenvektoren
rek. $\rightarrow$
$C = \begin{pmatrix} A_{11}B_{11} + A_{12}B_{21}, & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21}, & A_{21}B_{12} + A_{22}B_{22} \end{pmatrix}$. Rest nach Schulmethode $O(n^2)$.
end;

Lemma 3.2: $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ invertierbar, $A^{-1} = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$.

C kann i.a. berechnet werden als:

$\mathrm{I} = A_{11}^{-1}$, $\mathrm{II} = A_{21}\mathrm{I}$, $\mathrm{III} = \mathrm{I}A_{12}$, $\mathrm{IV} = A_{21}\mathrm{III}$, $\mathrm{V} = \mathrm{IV} - A_{22}$; $\mathrm{VI} = \mathrm{V}^{-1}$, $\mathrm{VII} = \mathrm{III} \cdot C_{21}$

$C_{12} = \mathrm{III} \cdot \mathrm{VI}$, $C_{21} = \mathrm{VI} \cdot \mathrm{II}$, $C_{11} = \mathrm{I} - \mathrm{VII}$, $C_{22} = -\mathrm{VI}$.

2 Inversionen, 6 Mult., 2 Add.

Rechenop. für rek. Berechnung von A^{-1}: $(n = 2^k \cdot m)$

$\left.\begin{array}{l} \delta_k = \delta(n) \\ \mu_k = \mu(n) \\ \alpha_k = \alpha(n) \end{array}\right\} = \#$ Divisionen, Mult., Add.

$\delta_{k+1} = 2\delta_k$; $\delta_0 = m$;
$\mu_{k+1} = 2\mu_k + 6M_k$ (Strassen!); $\mu_0 = m^3$
$\alpha_{k+1} = 2\alpha_k + 6A_k + 2(2^k \cdot m)^2$, $\alpha_0 = O(m^3)$ (!)

$\Rightarrow \delta_k = 2^k \cdot m = n$
$\mu_k = 2^k \mu_0 + 6 \sum_{l=0}^{k-1} M_l\, 2^{k-1-l} = \left(\frac{6}{5} 7^k - \frac{1}{5} 2^k\right) m^3$
$\alpha_k \le \frac{6}{5}(m^3 + 5m^2)\, 7^k$

$D(n) = n$, $M(n) = \frac{6}{5} n^{\log_2 7}$, $A(n) \le \frac{36}{5} n^{\log_2 7}$

Mehlhorn

§4 Toeplitz-Matrizen:

$T = \begin{pmatrix} t_0 & t_{-1} & \cdots & t_{-n+1} \\ t_1 & \ddots & & \vdots \\ \vdots & & \ddots & t_{-1} \\ t_{n-1} & \cdots & t_1 & t_0 \end{pmatrix}$ ist Toeplitz-Matrix, entsteht aus 1. Zeile durch sukzessive Rechts-shifts.

$M = \begin{pmatrix} 0 & & 0 \\ 1 & \ddots & \\ 0 & 1 & 0 \end{pmatrix}$. Def 4.1: A (n,n) Matrix. $\alpha_+(A) = \operatorname{rk}(A - MAM^t)$ = „+“-Verschiebungsrang

$MA = \begin{pmatrix} 0 & \cdots & 0 \\ a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{n-1\,1} & \cdots & a_{n-1\,n} \end{pmatrix}$, $AM^t = \begin{pmatrix} 0 & a_{11} & \cdots & a_{1\,n-1} \\ \vdots & \vdots & & \vdots \\ 0 & a_{1n} & \cdots & a_{n\,n-1} \end{pmatrix}$. $\alpha_-(A) = \operatorname{rk}(A - M^tAM)$ = „−“-Verschiebungsrang.

$MAM^t = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & a_{11} \cdots & a_{1\,n-1} \\ 0 & a_{n-1\,1} & a_{n-1\,n-1} \end{pmatrix}$ $\quad T - MTM^t = \begin{pmatrix} t_0 & \cdots & t_{-n+1} \\ \vdots & 0 & \\ t_{n-1} & & \end{pmatrix}$, $T - M^tTM = \begin{pmatrix} 0 & & t_{-n+1} \\ & & \vdots \\ t_{n-1} & \cdots & t_0 \end{pmatrix}$

Bem. $\alpha_+(T) \le 2$, $\alpha_-(T) \le 2$.

Lemma 4.2: Sei A invertierbar $\Rightarrow \alpha_+(A) = \alpha_-(A^{-1})$.

(a) $\operatorname{rk}(I - AB) = \operatorname{rk}(I - BA)$; $(A, B \in n \times n)$

Bew: $\overset{m:=}{\operatorname{rk}}(I - AB) \ge \operatorname{rk}(I - BA)$:

$\exists\, x_1 \dots x_{n-m}$, l. u., $(I - AB)x_i = 0$, $i = 1 \dots n-m$.

Bx_i l. u., denn sonst wäre $ABx_i = x_i$ l. a.

$B(I - AB)x_i = 0 \Rightarrow (I - BA)\underbrace{Bx_i}_{\text{l. u.}} = 0 \Rightarrow \operatorname{rk}(I - AB) \ge \operatorname{rk}(I - BA)$ □

(b) $\alpha_+(A) = \operatorname{rk}(I - MAM^t) = \operatorname{rk}((I - MAM^tA^{-1})A)$
$= \operatorname{rk}(I - MAM^tA^{-1})$
$= \operatorname{rk}(I - M^tA^{-1}MA) = \operatorname{rk}(A^{-1} - M^tA^{-1}M)$ □ $= \alpha_-(A^{-1})$

~~Lemma 4.3~~:

Def Sei $x = \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix}$, $L(x) = \begin{pmatrix} x_0 & & 0 \\ \vdots & \ddots & \\ x_{n-1} & \cdots & x_0 \end{pmatrix}$, $U(x) = L^t(x)$. $(L(x))_{kl} = \begin{cases} x_{k-l} & k \ge l \\ 0 & \text{sonst} \end{cases}$.

$(U(x))_{kl} = \begin{cases} x_{l-k} & l \ge k \\ 0 & \text{sonst} \end{cases}$.

Lemma 4.3: $x^j, y^j \in \mathbb{R}^n$. Dann ist äq:

(a) $A - MAM^t = \sum_{j=1}^{\alpha} x^j (y^j)^t$

(b) $A = \sum_{j=1}^{\alpha} L(x_j) U(y_j)$

$b \Rightarrow a$: $A_{kl} = \sum_{j=1}^{\alpha} \sum_{i=1}^{n} L(x_j)_{ki} U(y_j)_{il} = \sum_{j=1}^{\alpha} \sum_{i=1}^{n} x^j_{k-i} y^j_{l-i}$. $(x_i = 0$ für $i < 0)$

$A - MAM^t = a_{k,l} - a_{k-1,l-1} = \sum_{j=1}^{\alpha} \sum_{i=1}^{n} (x^j_{k-i} y^j_{l-i} - x^j_{k-i+1} y^j_{l-i+1}) = \sum_{j=1}^{\alpha} x^j_{k-1} y^j_{l-1} = \sum_{j=1}^{\alpha} (x^j y^{jt})_{k,l}$

$a \Rightarrow b$: $A - MAM^t = 0 \Rightarrow A = 0$, d. h. Gleichungen nur trivial lösbar.

1 Lösung in $b \Rightarrow a$ $\Rightarrow$ eindeutige bzg. $A = 0$.

Frank Wübbeling -5-

$\alpha_+(A) = rk(A - MAM^t)$; $\alpha_-(A^{-1}) = \alpha_+(A)$

~~$A = \sum_{i=1}^{\alpha_+(A)} L(x^i)U(y^i)$, $A = \sum_{i=1}^{\alpha_-(A)}$~~

Lemma 4.4: Es gibt Vektoren x^i, y^i $(\tilde{x}^j, \tilde{y}^j)$ sod.

$$A = \sum_{i=1}^{\alpha_+(A)} L(x^i)U(y^i), \quad A = \sum_{i=1}^{\alpha_-(A)} U(\tilde{y}^i)L(\tilde{x}^i).$$

Bew.: (a) $rk(A) = \alpha \Rightarrow A = \sum_{i=1}^{\alpha} x^i y^{it}$.

$x^1 \dots x^\alpha$ l. u. Spalten von $A = (a_1 \dots a_n)$.

$\Rightarrow a^i = \sum_{j=1}^{\alpha} y_j^i x^j$, $i = 1 \dots n$. $a_{ki} = \sum_{j=1}^{\alpha} (x_j y^{jt})_{ki}$

(b) Lemma 4.3: $A - MAM^t = \sum_{j=1}^{\alpha} x^j y^{jt} \Rightarrow A = \sum_{i=1}^{\alpha} L(x^j)U(y^j)$.

Bem.: LU bzw. UL-Zerlegung erfordert $O(n)$ Ops, α_+, α_- konstant.

Satz 4.5: A invertierbar $\Rightarrow A^{-1} = \sum_{j=1}^{\alpha_-(A)} L^j U^j$ mit unteren bzw. oberen Δ-Toeplitz-Matrizen L^j, U^j

Bew.: $\alpha_+(A) = \alpha_-(A^{-1})$, siehe Lemma 4.4.

Lemma: Sei T Toeplitz-Matrix, $x \in \mathbb{R}^n$. Dann kann man Tx in $O(n \cdot \log n)$ Operationen berechnen
(Idee)

Bew.: Siehe Teil III.

Kor.: A invertierbar mit Verschrang $\alpha_+(A)$. Dann kann $A^{-1}x$ in $O(n \cdot \log n)$ Ops berechnet werden, falls LU- bzw. UL-Zerlegung bekannt ist.

Lemma 4.6: Matrizen A, B mit $+,-$ Versch. $\le \alpha_0$ lassen sich mit $O(n \cdot \log(n))$ Operationen multiplizieren.

Bew. i) $L(x)L(y)$: $L(x) = \begin{pmatrix} x_0 & & 0 \\ \vdots & \ddots & \\ x_{n-1} & \cdots & x_0 \end{pmatrix}$, $L(z)$: $z_i = \sum_{k=0}^{n-1} x_k y_{i-k}$, $y_i = 0$ für $i < 0$ (Faltung von $x y$). $O(n \cdot \log n)$.

ii) $UL = \sum_{i=1}^{3} L^i U^i$; L^i, U^i Toeplitz-Matrizen.

$$(U, \tilde{L}) = \left(\begin{array}{cccc|cccc} u_0 & \cdots & & u_{n-1} & 0 & \cdots & & 0 \\ & u_0 & \cdots & u_{n-2} & u_{n-1} & & & \vdots \\ 0 & & \ddots & \vdots & \vdots & & & \\ & & & u_0 & u_1 & \cdots & u_{n-1} & 0 \end{array}\right), \quad \begin{pmatrix} L \\ \tilde{U} \end{pmatrix} = \begin{pmatrix} l_0 & 0 & \cdots & 0 \\ l_1 & l_0 & & \vdots \\ & & & 0 \\ l_{n-1} & l_{n-2} & \cdots & l_0 \\ \hline 0 & l_{n-1} & \cdots & l_1 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & l_{n-1} \end{pmatrix}$$

$T = (U, \tilde{L}) \begin{pmatrix} L \\ \tilde{U} \end{pmatrix} = UL + \tilde{L}\tilde{U}$. $T_{k,l}$ = Funktion von $k - l$, T Toeplitz $\Rightarrow T = L^1U^1 + L^2U^2$ (Lemma 4.4)
$\Rightarrow UL = L^1U^1 + L^2U^2 - \tilde{L}\tilde{U}$

iii) $A = \sum_{i=1}^{\alpha_+(A)} L^i U^i$, $B = \sum_{j=1}^{\alpha_+(B)} \tilde{L}^j \tilde{U}^j$

$$AB = \sum_{i,j} L^i \underbrace{U^i \tilde{L}^j}_{= \sum_{k=1}^{3} L^k U^k \ O(n \log n) \text{ nach ii)}} \tilde{U}^j = \sum_{i,j,k} \overbrace{L^i L^k}^{L^{ik}} \overbrace{U^k \tilde{U}^j}^{U^{jk}} \text{ in } O(\log n \cdot n) = \sum_{i,k,j} L^{ik} U^{kj}. \ 3\alpha_0^2 \text{ Summanden} \Rightarrow O(n \cdot \log n)$$

Algorithmus von Morf; Bitmead, Anderson zur Inversion von Matrizen mit kleinem Versch.-rang

INVERT proc $(n, \alpha_0, A, x^1, y_1 \ldots x^{\alpha_0}, y^{\alpha_0})$

/* $C = A^{-1} = \sum_{j=1}^{\alpha_0} L(x^j)\, U(y^j)$ */ $(\alpha_+(A) \le \alpha_0)$

1. $n = 1$: $L = A^{-1}$, $U = I$

2. n gerade, $m = n/2$: $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ $\}n$, $\underbrace{\phantom{A_{11}}}_{m}$

$C_{22} = (A_{22} - A_{21} A_{11}^{-1} A_{12})^{-1}$, $C_{11} = A_{11}^{-1} + A_{11}^{-1} A_{12} A_{12} C_{22} A_{21} A_{11}^{-1}$,

$C_{12} = -A_{11}^{-1} A_{12} C_{22}$, $C_{21} = -C_{22} A_{21} A_{11}^{-1}$

Es gilt: $\alpha_+(A_{11}) \le \alpha_0$; $\alpha_+(A_{22} - A_{21} A_{11}^{-1} A_{12}) \le \alpha_0$,

$\alpha_+(A_{12}), \alpha_+(A_{21}) \le \alpha_0 + 1$;

$\alpha_+(A_{22}) \le \alpha_0 + 2$.

Bew. (i): $A = \sum_{j=1}^{\alpha_0} L^j U^j$, $L^j = \begin{pmatrix} L_{11}^j & 0 \\ L_{21}^j & L_{22}^j \end{pmatrix}$, alle Toeplitz, $U^j = \begin{pmatrix} U_{11}^j & U_{12}^j \\ 0 & U_{22}^j \end{pmatrix}$.

$$A = \sum_{j=1}^{\alpha_0} \begin{pmatrix} L_{11}^j U_{11}^j & L_{11}^j U_{12}^j \\ L_{21}^j U_{11}^j & L_{21}^j U_{12}^j + L_{22}^j U_{22}^j \end{pmatrix} \Rightarrow A_{11} = \sum_{j=1}^{\alpha_0} L_{11}^j U_{11}^j \Rightarrow \alpha_+(A_{11}) \le \alpha_0.$$

(ii) $\alpha_-(A^{-1}) \le \alpha_0$, $\alpha_-(C_{22}) \le \alpha_0$ wie i) mit UL-Zerlegung $\Rightarrow \alpha_+(C_{22}^{-1}) \le \alpha_0$.

(iii) $A_{12} = \sum_{j=1}^{\alpha_0} L_{11}^j \underbrace{U_{12}^j}_{L_1^j + U_1^j} = \underbrace{\sum_{j=1}^{\alpha_0} L_{11}^j L_1^j}_{L\,T} + \sum_{j=1}^{\alpha_0} L_{11}^j U_1^j \overset{?}{\Rightarrow} \alpha_+(A_{12}) \le \alpha_0 + 1$.

3. Berechne A_{11}^{-1}, C_{22} rekursiv. Produkte durch schnelle Mult. nach 4.6.

$M(n) = \#\mathrm{Op}$ für Länge n.

$M(n) \le 2 M(\frac{n}{2}) + c \cdot n \log n \Rightarrow M(n) = \Theta(n \cdot (\log_2 n)^2)$.

Teil III Fourier-Transformationen und Faltungen

§5. Diskrete Fourier-Transformation.

$$\hat{y}_k = \sum_{j=0}^{n-1} e^{-2\pi i kj/n} \; ; \; y_k = \sum_{j=0}^{n-1} e^{2\pi i kj/n} \hat{y}_k .$$

(Orthogonalität von e^{ix}: $\frac{1}{n}\sum_{j=0}^{n-1} e^{2\pi i jk/n} = \begin{cases} 1 & k = 0, \pm n, \pm 2n \dots \\ 0 & \text{sonst} \end{cases}$.

$$\Rightarrow \hat{y} = \frac{1}{n} W_n y \quad W_n = \begin{pmatrix} 1 & \dots & 1 \\ 1 & w \dots & w^{n-1} \\ 1 & w^2 \dots & w^{2n-2} \\ \vdots & & \end{pmatrix} \; (W_n)_{jk} = w^{j\cdot k} . \; w^n = w \Rightarrow w^k = w^{k \bmod n} .$$

$$W_n W_n^* = \frac{1}{n} \cdot I .$$

Zyklische Faltung: $x = \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix}, y = \begin{pmatrix} y_0 \\ \vdots \\ y_{n-1} \end{pmatrix}$. $z = x * y$: $z_k = \sum_{j=0}^{n-1} x_{k-j} y_j$; Indizes mod n

$$\Rightarrow z = X y . \; X = \begin{pmatrix} x_0 & x_{n-1} & \dots & x_1 \\ x_1 & x_0 & \dots & x_2 \\ x_2 & x_1 & \dots & x_3 \\ \vdots & & & \\ x_{n-1} & x_n & \dots & x_0 \end{pmatrix}$$

Faltungssatz: $(x * y)^\wedge_k = n \hat{x}_k \hat{y}_k$

Phasensatz: $(Tx)_k = x_{k+1}$, $T\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_{n-1} \\ x_0 \end{pmatrix} \Rightarrow$

$$(Tx)^\wedge = e^{2\pi i k/n} \hat{x}_k$$

§6. FFT nach Cooley / Tukey.

1. Divide & conquer. $n = 2^k$. ($\frac{1}{n}$ weggelassen).

$$\hat{y}_k = \sum_{j=0}^{n-1} e^{-2\pi i kj/n} y_j = \sum_{l=0}^{m-1} e^{-2\pi i lk/m} y_{2l} + \left(\sum_{l=0}^{m-1} e^{-2\pi i lk/m}\right) e^{-2\pi i k/n} y_{2l+1}$$

$$\hat{y}_{k+m} = \sum_{l=0}^{m-1} e^{-2\pi i kl/m} y_{2l} - e^{-2\pi i k/n} \sum_{l=0}^{m-1} e^{-2\pi i kl/m} y_{2l+1}$$

$$\Rightarrow \hat{y}_k = \hat{g}_k + w^k \hat{u}_k , \; \hat{y}_{k+m} = \hat{g}_k - w^k \hat{u}_k .$$

$$M(n) = 2 M\left(\frac{n}{2}\right) + \frac{n}{2}, \; A(n) = 2 A\left(\frac{n}{2}\right) + n, \; M(1) = A(1) = 0 .$$

$$\Rightarrow M(n) = \frac{1}{2} n \cdot \log_2 n, \; A(n) = n \cdot \log_2 n .$$

Matrix-Darstellung der FFT ($n = 8 = 2^3$)

$$W_8 = \begin{pmatrix} 1 & \dots & 1 & & & & & 1 \\ 1 & w & w^2 & w^3 & w^4 & w^5 & w^6 & w^7 \\ 1 & w^2 & w^4 & w^6 & 1 & w^2 & w^4 & w^6 \\ 1 & w^3 & w^6 & w & w^4 & w^7 & w^2 & w^5 \\ 1 & w^4 & 1 & w^4 & 1 & w^4 & 1 & w^4 \\ 1 & w^5 & w^2 & w^7 & w^4 & w & w^6 & w^3 \\ 1 & w^6 & w^4 & w^2 & 1 & w^6 & w^4 & w^2 \\ 1 & w^7 & w^6 & w^5 & w^4 & w^3 & w^2 & w \end{pmatrix} \; P_8 : \begin{matrix} 01234567 \\ 02461357 \end{matrix} \downarrow = \begin{pmatrix} e_0^t \\ e_2^t \\ e_4^t \\ e_6^t \\ e_1^t \\ e_3^t \\ e_5^t \\ e_7^t \end{pmatrix}$$

$\tilde{W}_8 = W_8 P_8$. $P_8 = (e_0, e_2, e_4, e_6, e_1, e_3, e_5, e_7)$

$$\boxed{D_4 = \begin{pmatrix} 1 & & & 0 \\ & w & & \\ & & w^2 & \\ 0 & & & w^3 \end{pmatrix}}$$

$$\tilde{W}_8 = \begin{pmatrix} W_4 & D_4 W_4 \\ W_4 & -D_4 W_4 \end{pmatrix} \; w^4 = -1 . \Rightarrow \tilde{W}_8 = \begin{pmatrix} E_4 & E_4 \\ E_4 & -E_4 \end{pmatrix} \begin{pmatrix} E_4 & 0 \\ 0 & D_4 \end{pmatrix} \begin{pmatrix} W_4 & 0 \\ 0 & W_4 \end{pmatrix};$$

E_4 = 4-reihige Einheitsmatrix

$P_4 = (e_0, e_2, e_1, e_3)$. $\tilde{W}_4 = W_4 P_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & t^2 & t & t^3 \\ 1 & 1 & t^2 & t^2 \\ 1 & t^2 & t^3 & t \end{pmatrix} = \begin{pmatrix} W_2 & D_2 W_2 \\ W_2 & -D_2 W_2 \end{pmatrix}$, $D_2 = \begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix}$, $t^2 = -1$.

$$\tilde{\tilde{W}}_8 = W_8 P_8 \begin{pmatrix} P_4 & 0 \\ 0 & P_4 \end{pmatrix} \Rightarrow \tilde{\tilde{W}}_8 = \begin{pmatrix} E_4 & E_4 \\ E_4 & -E_4 \end{pmatrix} \begin{pmatrix} E_4 & 0 \\ 0 & D_4 \end{pmatrix} \begin{pmatrix} E_2 & E_2 & & \\ E_2 & -E_2 & & \\ & & E_2 & E_2 \\ & & E_2 & -E_2 \end{pmatrix} \begin{pmatrix} E_2 & & & \\ & D_2 & & \\ & & E_2 & \\ & & & D_2 \end{pmatrix} \begin{pmatrix} w_2 & & & \\ & w_2 & & \\ & & w_2 & \\ & & & w_2 \end{pmatrix}$$

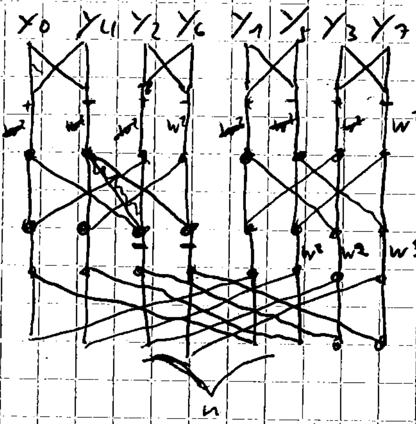
Ausführung der Permutation: 0 1 2 3 4 5 6 7
0 2 4 6 1 3 5 7
0 4 2 6 1 5 3 7

$s = (s_2, s_1, s_0)_2$ 0, 1, 0

$\tilde{s} = (s_1, s_0, s_2)_2$ 0, 0, 1

$\tilde{\tilde{s}}_2 = (s_0, s_1, s_2)_2$

Schaltbild für FFT, n = 8



$\bowtie$ Boulderdash - Schmetterling

s_0, s_1, s_2, s_3

00000	0000	0	0
10001	1000	8	1
0010	0100	4	2
0011	1100	12	3
0100	0010	2	4
0101	1010	10	5
0110	0110	6	6
0111	1110	14	7
1000	0001	1	8
1001	1001	9	9
1010	0101	5	10
1011	1101	13	11
1100	0011	3	12
1101	1011	11	13
1110	0111	7	14
1111	1111	15	15

1, 3, 5, 7
4, 5, 6, 7

~~x_0 y_4~~ | y_2 y_6 | y_1 y_5 |

0 1 | 2, 3 | 4 5 | 6 7
0, 2 | 1, 3 | 4, 6 | 5, 7
0, 4 | 1, 5 | 2, 6 | 3, 7

1012

~~usw. mit~~

~~(7, 8), (11, 12), (15)~~
(2, 3) (6, 7) (10, 11) (14, 15) mit (1, w)
(4, 5, 6, 7) (12, 13, 14, 15) mit (1, w, w^2, w^3) } alles in!

original in 8: (2, 6); (3, 7)
(1, 5, 3, 7)

original in 16: (4, 12) (6, 14) (5, 13) (7, 15)
(2, 10, 6, 14) (3, 11, 7, 15)
(1, 9, 5, 13, 3, 11, 7, 15)
8 -4 8 -10 8 -4 8
0001|1001|0101|1101|0011|1011|0111|1111
0000

0010|1010|0110|1110

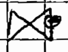
$\S 6$

1. Cooley - Tukey FFT: $n = 2^p$, $m = \frac{n}{2}$ durch Dezimierung in der Zeit

$$\hat{y}_k = \sum_{j=0}^{n-1} w^{jk} y_j, \quad w = e^{-2\pi i/n}. \Rightarrow \hat{y}_k = g_k + w^k \cdot u_k, \quad \hat{y}_{k+m} = g_k - \underset{\substack{\uparrow \\ \text{Drehfaktoren}}}{w^k} u_k$$

$$\begin{matrix} g_k \\ u_k \end{matrix} = \sum_{j=0}^{m-1} (w^2)^{jk} \begin{matrix} y_{2j} \\ y_{2j+1} \end{matrix}$$

2 Matrixdarstellung

3 Schaltbild: 

4 Dezimierung in der Frequenz:

$$\hat{y}_k = \sum_{j=0}^{n-1} w^{jk} y_j = \sum_{j=0}^{m-1} w^{jk} y_j + \sum_{j=m}^{n-1} w^{jk} y_j = \sum_{j=0}^{m-1} w^{jk} y_j + \sum_{j=0}^{m-1} w^{(j+\frac{n}{2})k} y_{m+j}$$

$$\underbrace{w^{k\cdot m}}_{(-1)^k} \sum_{j=0}^{m-1} w^{jk} y_{m+j}$$

$$\boxed{\begin{aligned} \hat{y}_{2k} &= \sum_{j=0}^{m-1} (w^2)^{jk} (y_j + y_{j+m}) \\ \hat{y}_{2k+1} &= \sum_{j=0}^{m-1} (w^2)^{jk} w^j (y_j - y_{m+j}) \end{aligned}}$$

$$= \sum_{j=0}^{m-1} w^{jk} (y_j + (-1)^k y_{j+m})$$

5) Polynomiale Interpolation (Beth)

z-Transformation: $y_0 \dots y_{n-1} \Rightarrow f(z) = \sum_{j=0}^{n-1} y_j z^j$, dem Vektor wird ein Polynom zugeordnet.

Fourier-Transformation: $\hat{y}_k = f(z_k)$, $z_k = e^{-2\pi i k/n}$, $k = 0 \dots n-1$.

$f \equiv g \mod p \Leftrightarrow f = g + q \cdot p$

Regeln 1) $f_i \equiv g_i \mod p_i \Rightarrow f_1 + f_2 \equiv g_1 + g_2$, $f_1 f_2 \equiv g_1 g_2$ jeweils mod p.

2) $p_1 | p \Rightarrow p = q p_1$; $f \equiv g \mod p \Rightarrow f \equiv g \mod p_1$ $f \mod p_1 = (f \mod p) \mod p_1$

$\hat{y}_k = f(z_k)$, $k = 0 \dots n-1$. z_k Nullstellen von $z^n - 1$

$f(z) \mod z - z_k$: $f(z) = f(z_k) + (z - z_k) p(z) \equiv f(z_k) \mod (z - z_k)$

0. Stufe: $f(z) \mod z^n - 1$: $y_0 + \dots + y_{n-1} z^{n-1}$

1. Stufe: $z^n - 1 = (z^m - 1)(z^m + 1)$ $f(z) \mod z^m - 1$ | $f(z) \mod z^m + 1$

$$= (y_0 + y_{\frac{n}{2}}) + (y_1 + y_{m+1}) z + \dots + (y_{m-1} + y_{n-1}) z^{m-1} \quad (y_0 - y_m) + (y_1 - y_{m+1}) z + \dots + (y_{m-1} - y_{n-1}) z^{m-1}$$

2. Stufe: $(z^{n/4} - 1)(z^{n/4} + 1)$, $(z^{n/2} + 1) = (z^{n/4} - i)(z^{n/4} + i)$

$f(z) \mod z^{n/4} - 1$: $(y_0 + y_{\frac{n}{2}} + y_{\frac{n}{4}} + y_{\frac{3n}{4}}) \dots$ $f(z) \mod z^{n/4} + 1$ / $f(z) \mod z^{n/4} - i$ / $f(z) \mod z^{n/4} + i$

letzte Stufe: $\underset{\substack{\parallel \\ f(z_k)}}{f(z) \mod z - z_k}$, $k = 0 \dots n-1$.

$n=8$:

$$z^8-1$$
$$z^4-1 \qquad z^4+1$$
$$z^2-1 \quad z^2+1 \quad z^2-i \quad z^2+i$$
$$(z-1)\ (z+1)\ (z-i)\ (z+i)\ \ z-z_1\ \ z-z_5\ \ z-z_3\ \ z-z_7$$
$$z-z_0 \quad z-z_4 \quad z-z_2 \quad z-z_6$$

$$z^8-1$$
$$z^4+1 \qquad z^4-1$$
$$z^2-i \quad z^2+i \quad z^2+1 \quad z^2-1$$
$$7\ 3\ 5\ 1\ 6\ 2\ 4\ 0$$

reduce : proc (n, p, w, q);

/* $p = \sum_{k=0}^{n-1} a_k z^k \bmod z^{n/2} - w = q$ */

do $k = 0$ to $\frac{n}{2} - 1$

$\quad q_k = a_k + w\, a_{k+\frac{n}{2}}$

end;

$7\,3\,5\,1\,6\,2\,4\,0$

$$z^n - w^m = \left(z^n - w^{m/2}\right)\left(z^n + w^{m/2}\right)$$

6) Reelle FFT nach Brunn : $n = 16$

$$z^{16}-1$$
$$(z^4+a z^2+1)\left(z^2-\sqrt{2-a}\,z+1\right)\left(z^2+\sqrt{2-a}\,z+1\right)$$
$$z^8-1 \qquad z^8+1$$
$$z^4-1 \quad z^4+1 \quad z^4-\sqrt{2}z^2+1 \quad z^4+\sqrt{2}z^2+1$$
$$z^2-1 \quad z^2+1 \quad z^2-\sqrt{2}z+1 \quad z^2+\sqrt{2}z+1 \quad z^2-\sqrt{2+\sqrt{2}}\,z+1 \quad z^2+\sqrt{2+\sqrt{2}}\,z+1 \quad z^2-\sqrt{2-\sqrt{2}}\,z+1 \quad z^2+\sqrt{2-\sqrt{2}}\,z+1$$
$$a_0+a_1 z \quad b_0+b_1 z \qquad\qquad c_0+c_1 z$$
$$z_0, z_8 \quad z_4, z_{12} \quad z_2, z_{10} \quad z_6, z_{14}$$

$f \bmod z-z_0 : a_0 + a_1 z_0$, $f \bmod z - z_1 : a_0 + a_1 z_4$

$f \bmod z_j : c_0 + c_1 z_j$
$f \bmod z_k : c_0 + c_1 z_k$.

§ 7 Der chinesische Restsatz.

R Ring (mit 1) 1) abelsche Gruppe, additiv
2) Multiplikation $(a+b)c = ac+bc$, $c(a+b) = ca+cb$, assoz., $1a = a1 = a$;

Beisp.: 1) $\mathbb{Z}$, 2) $\mathbb{K}[x]$, 3) Matrizen.

Teilbarkeit: $b \mid a \Leftrightarrow$ ~~[illegible]~~ $a = r \cdot b$. $a \equiv b \bmod p \Leftrightarrow p \mid a-b$.

Restklassenring R/p.

p prim $\Leftrightarrow$ 1) $p = ab \Rightarrow a$ oder b Einheit, 2) p keine Einheit.

R_1, R_2. $R := R_1 \oplus R_2$ ($R = R_1 \times R_2$, $(a,b) + (a',b') = (a+a', b+b')$, Produkt genauso

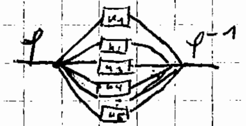
Satz 7.5: R eukl. Ring, $p_1 \dots p_m \in R$ paarweise teilerfremd $\Rightarrow$ ($p = \prod p_i$)

$R/(p) \cong R/(p_1) \oplus \dots \oplus R/(p_m)$.

Bew: $\varphi: R/(p) \to R/(p_1) \oplus \dots \oplus R/p_m$, $\varphi(a) := (a_1 \dots a_m)$, $a_i = a \bmod p_i$. φ bijektiv (CRT)

$\varphi(ab) = (a_1 b_1, \dots, a_m b_m)$, denn $ab \bmod p_i = (a \bmod p_i \cdot b \bmod p_i) \bmod p_i$.

Beisp. 3: Modulare Arithmetik: $R = \mathbb{Z}$. Rechne in $\mathbb{Z}_n$, $n \gg 1$, $n = \prod_{i=1}^{r} n_i$.


Rechenwerke rechnen mod n_k.

4: $p = p_1 p_2$, $(p_1, p_2) = 1$. $a \equiv a_i \bmod p_i$. $a = \frac{p}{p_1} x_1 a_1 + \frac{p}{p_2} x_2 a_2$, $p = p_1 p_2$.

$\Leftrightarrow a = p_2 x_1 a_1 + p_1 x_2 a_2$, $p_2 x_1 + p_1 x_2 \equiv 1 \bmod p$.

§8. Aus der Gruppentheorie

Sei G endliche Gruppe, multiplikativ und nicht notw. abelsch. $|G| =$ Ordnung $G =: n$.

H Untergruppe in G, $|H| = m$, $m \mid n$. Aequivalenzrelation in G, $s \sim t \Leftrightarrow t^{-1}s \in H \Leftrightarrow s \in tH$

$s_1 \dots s_r$ Repräsentantensystem, $\underbrace{s_1 H}_{m} \cup \dots \cup \underbrace{s_r H}_{m} = G$. (Links-)Nebenklassen, d.h. $n = m \cdot r$

Nebenklassen bilden Gruppe (Faktorgruppe G/H) $\Leftrightarrow$ H NT in G, d.h. $tHt^{-1} = H \;\forall t \in G$

$\Leftrightarrow H$ invariant bzgl. inneren Automorphismen. $sH\,tH := stH$. Neutrales El. ist H.

$a \in G$. Ordnung von $a := \inf\{m \geq 1 : a^m = 1\}$. $\{1, a, \dots, a^{m-1}\} =: C_m$ ist zyklische Gruppe der Ordn.

$a^k \cdot a^l = a^{k+l \bmod m} \Rightarrow C_m \cong \mathbb{Z}/m\mathbb{Z}$ (additiv).

Sei G abelsch, $a_1 \dots a_r$ Elemente der Ordnung $m_1 \dots m_r$, paarw. teilerfremd

$\Rightarrow a = \prod a_i$ hat die Ordnung $m = \prod m_i$. ($a^m = 1$, $a^q = 1 \underset{q \leq m}{\Rightarrow} q \mid m \Rightarrow q \mid m_1 \Rightarrow a^q = a_1^q (a_2 \dots a_r)^q$ (teilerfremd) usw. durch Ind.

<u>Direktes Produkt von Gruppen</u>

A, B Gruppen. $G := A \odot B$ ($A \times B$). $A \odot B = A \times B$, $(a,b) \cdot (a',b') = (aa', bb')$.

$\Rightarrow \{(a,1)\} \subset G$ ist isomorph zu A, $(a,1) \leftrightarrow a \Rightarrow A$ Untergruppe von $A \odot B$, und

A sogar NT in $A \odot B$. Vereinfachung der Schreibweise: $ab = ba = (a,b)$.

1) $g \in G \Rightarrow g = ab$, 2) $ab = ba$.

z.B. $C_{n_1} \odot C_{n_2} = C_n$, $n = n_1 n_2$. $a_1^{n_1} = a_2^{n_2} = 1 \Rightarrow a = a_1 a_2$ hat Ordnung n.

$M_n = \{a \in \mathbb{Z} : 1 \leq a \leq n : (a,n) = 1\}$, Multiplikation mod n. $|M_n| = \varphi(n)$.

M_n ist Gruppe $\Leftrightarrow ax \equiv 1 \bmod n \;\forall a \in M_n \Leftrightarrow$ CRT. ($(a,n) = 1$).

$r \geq 2$

p prim: $\varphi(p) = p-1$. $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

Beh: $M_n \cong C_{\varphi(n)}$ für $p \neq 2$. Bew: $n = p^r$. $2 \cdot 2$: Es gibt in M_n ein Element der Ordnung $p^{r-1}(p-1)$. ~~Da~~: Es gibt ein a_1 mit $a_1^{p^{r-1}} \neq 1$, denn sonst hätte $x^{p^{r-1}} = 1$ $p^{r-1}(p-1)$ Lösungen $\not\downarrow$, denn Polynom hat grad p^{r-1}, und a_2^{p-1} hat Lsg., denn sonst hätte $x^{p-1} = 1$ $(p^{r-1})(p-1)$ Lsg.

$b_1 = a_1^{p-1}$, $b_2 = a_2^{p^{r-1}}$, $b_1^{p^{r-1}} = 1$, $b_2^{p-1} = 1$.

Denn: $b_1^m = 1, m < p^{r-1} \Rightarrow m \mid p^{r-1} \not\downarrow$. $b = b_1 b_2 \Rightarrow$ Ordnung $(b) = p^{r-1} \cdot (p-1)$.

$G \rhd N_1 \rhd N_2 \rhd \ldots \rhd N_r = E = \{1\}$ heißt Normalreihe. Faktoren der Normalreihe sind G/N_1, G/N_2

Def. G auflösbar $\Leftrightarrow$ G hat Normalreihe mit abelschen Faktoren.

7.1 $C_n \cong C_{n_1} \odot C_{n_2}$. $C_{n_1} = \{1, a_1 .. a_1^{n_1-1}\}$, $C_{n_2} = \{1, a_2 .. a_2^{n_2-1}\}$, $C_n = \{1, a .. a^{n-1}\}$, $a_1 = a^{n_2}$, $a_2 = a^{n_1}$

$C_{n_1} \odot C_{n_2} = \{a_1^k a_2^l : k \bmod n_1, l \bmod n_2\}$. $kn_2 + ln_1 = 1 \Rightarrow a_1^k a_2^l = a^{kn_2 + ln_1} = a$

Satz 7.2: p prim $\Rightarrow M_{p^r} \cong \begin{cases} C_{(p-1)p^{r-1}}, p>2, r \geq 1 \\ C_2 \odot C_{2^{r-2}} \end{cases}$. (Hasse, Number Theory, Ch. 4.5).

Suche erzeugendes Element von $M_{p^r} = \{1, a .. a^{(p-1)(p^{r-1})-1}\}$

$r = 1$: a primitive Wurzel mod p. Für $p < 10.000$ bei Abramowitz-Stegun / Handbook of Math. Tab. 864-865

3	5	7	11	13	17	19	23
2	2	3	2	2	3	2	5

Bsp: $p = 5, r = 1$, $M_5 = \{1, 2, 3, 4, 5\}$. $a = 2$: zykl.

2) $p = 3, r = 2$: $M_9 = \{1, 2, 4, 5, 7, 8\}$ Ordnung $6 = (p-1)p^{r-1}$. $\boxed{a = 5}$

§9. Schnelle Faltungen nach Winograd.

Winograd, On Computing the Discrete Fourier Transform, Mathematics of Computation 32, 175-199 (1978).

3 Hilfsmittel: CRT, direkte Produkte von Gruppen, Transposition.

(a) $z^n - 1 = p_1 p_2$. $\mathbb{C}[z]/_{z^n-1} \cong \mathbb{C}[z]/p_1 \oplus \mathbb{C}[z]/p_2$

Bemerkung: $fg = p_2 q_1 (fg) \bmod p_1 + p_1 q_2 (fg) \bmod p_2$, $p_2 q_1 + p_1 q_2 = 1$.

$n=2$: $(z^2-1)=\underset{p_1}{(z-1)}\underset{p_2}{(z+1)}$. $\underset{a_1}{(z+1)\frac{1}{2}}+\underset{a_2}{(z-1)\frac{-1}{2}}=1$

$f=x_0+x_1z,\ g=y_0+y_1z.\ fg=w_0+w_1z,\ \mathrm{mod}\,(z^2-1)$ $\quad w_0=x_0y_0+x_1y_1$, $w_1=x_0y_1+x_1y_0$.

$(fg)\ \mathrm{mod}\ p_1=(fg)(1)=f(1)g(1)=(x_0+x_1)(y_0+y_1)$.

$(fg)\ \mathrm{mod}\ p_2=(fg)(-1)=f(-1)g(-1)=(x_0-x_1)(y_0-y_1)$.

$$fg=(z+1)\frac{x_0+x_1}{2}(y_0+y_1)-(z-1)\frac{x_0-x_1}{2}(y_0-y_1)$$

Alg: $s_1=y_0+y_1,\ s_2=y_0-y_1,\ m_1=\frac{x_0+x_1}{2},\ m_2=\frac{x_0-x_1}{2}$. m_i vorberechnet!

4 Additionen, 2 Multiplikationen.

$n=3$: $(z^3-1)=(z-1)(z^2+z+1)$.

$$(z^2+z+1)=(z-1)(z+2)\ \text{Rest}\ 3\Rightarrow \underset{a_1}{\tfrac{1}{3}(z^2+z+1)}+\underset{a_2}{\left(-\tfrac{z+2}{3}\right)}(z-1)=1.$$

$(fg)\ \mathrm{mod}\,(z-1)=\underset{m_0'}{(x_0+x_1+x_2)(y_0+y_1+y_2)}$; $f=x_0+x_1z+x_2z^2$, $g=y_0+y_1z+y_2z^2$, $fg=w_0+w_1z+\dots$

$f\ \mathrm{mod}\ z^2+z+1=(x_0-x_2)+(x_1-x_2)z$, $g\ \mathrm{mod}\ z^2+z+1=(y_0-y_2)+(y_1-y_2)z$.

$fg\ \mathrm{mod}\ z^2+z+1=\underset{m_1'}{(x_0-x_2)(y_0-y_2)}-\underset{m_2'}{(x_1-x_2)(y_1-y_2)}+\{(x_0-x_2)(y_1-y_2)+(x_1-x_2)(y_0-y_2)-(x_1-x_2)(y_1-y_2)\}$

$\{\}=(x_0-x_2)(y_0-y_2)+(x_0-x_1)(y_1-y_0)+(x_1-x_2)(y_0-y_1)=\underset{m_1'}{(x_0-x_2)(y_0-y_2)}+\underset{-m_3'}{(x_0-x_1)(y_1-y_0)}$

$=m_1'-m_2'+\{m_1'-m_3'\}z$.

$$fg\ \mathrm{mod}\,(z^3-1)=(z^2+z+1)\tfrac{1}{3}fg\ \mathrm{mod}(z-1)+(z-1)\left(-\tfrac{z+2}{3}\right)fg\ \mathrm{mod}\,(z^2+z+1).$$

$$=(z^2+z+1)\frac{m_0'}{3}-(z-1)(z+2)\left\{\frac{m_1'-m_2'}{3}+\frac{m_1'-m_3'}{3}z\right\},\ m_i=\frac{m_i'}{3}.$$

$$=\{m_0+2m_1-2m_2-m_1+m_3\}+\{m_0-m_1+m_2+2m_1-2m_3\}z+\{m_0-m_1+m_2-m_1+m_3\}z^2$$

Alg: $s_0=(y_0+y_1+y_2),\ s_1=y_0-y_2,\ s_2=y_1-y_2,\ s_3=y_0-y_1$.

$m_0=\frac{(x_0+x_1+x_2)}{3}s_0,\ m_1=\frac{(x_0-x_2)}{3}s_1,\ m_2=\frac{(x_1-x_2)}{3}s_2,\ m_3=\frac{(x_0-x_1)}{3}s_3$.

$w_0=m_0+\underbrace{m_1-2m_2}_{-m_2-m_2}+m_3,\ w_1=m_0+m_1+m_2-2m_3,\ w_2=m_0-2m_1+m_2+m_3$.

4 Mult., 17 Add.

(b) Direkte Produkte. $G=A\odot B;\ A,B\trianglelefteq G$. $G=\{\overset{e=1}{g_1}\dots g_n\}$. $\mathcal{G}_{ik}=g_ig_k$, Gruppentafel

$\mathcal{G}$ kann beschrieben werden durch Permutationen $\quad\begin{matrix} g_1 & \dots & g_n \\ g_{i1} & \dots & g_{in} \\ g_{in1} & \dots & g_{inn}\end{matrix}$ $\quad i_1\dots i_n$ Perm. von $1\dots$

$\mathfrak{A}$, $\mathfrak{B}$ Gruppentafel von $A=\{a_1\dots a_p\}$, $B=\{b_1\dots b_q\}$.

$G=\{a_1b_1,\dots,a_1b_q,\ a_2b_1\dots a_2b_q\ \dots\ a_pb_1\dots a_pb_q\}$, lexikographische Anordnung

$$\mathcal{G}=\begin{array}{c|c|c} & a_1b_1\ \dots\ a_1b_q & a_2b_1\ \dots\ a_2b_q \\ \hline \begin{matrix}a_1b_1\\ \vdots\\ a_1b_q\end{matrix} & a_1^2\mathfrak{B} & a_1a_2\mathfrak{B} \\ \hline \begin{matrix}a_2b_1\\ \vdots\\ a_2b_q\end{matrix} & a_2a_1\mathfrak{B} & a_2^2\mathfrak{B} \end{array}\ \dots$$

Die Gruppentafel $a_ia_j\mathfrak{B}$ ist isomorph zu $\mathfrak{B}$.
(d.h. $\mathfrak{B}$ hat gleiche Perm. wie $a_ia_j\mathfrak{B}$)
Ergibt zu $\mathfrak{B}$ isomorphe Gruppentafeln $\mathfrak{B}$, in der Anordnung der Gruppentafel $\mathfrak{A}$.

$$F_n = \begin{matrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & x_2 & \cdots & x_0 \\ x_2 & x_3 & \cdots & x_1 \\ \vdots \\ x_{n-1} & x_0 & \cdots & x_{n-2} \end{matrix}$$

Gruppentafel von $\mathbb{Z}/n\mathbb{Z}$: $\begin{pmatrix} 0 & \cdots & n-1 \\ \vdots & & \vdots \\ n-1 & 0 \cdots & n-2 \end{pmatrix}$

$n = p \cdot q,\ (p,q) = 1.\ C_n = C_p \odot C_q \ldots \{1, a^p \ldots a^{p(q-1)}\}$

$\{1, a \ldots a^{n-1}\}\ \{1, a^q \ldots a^{q(p-1)}\}$

Indices lexikographisch geordnet:

$$\begin{array}{c|cccccc} & 1 & a^p & \ldots & a^{p(q-1)} & a & a^{q+1} \ldots \\ \hline 1 \\ a^p \\ \vdots \\ a^{p(q-1)} \\ a^q \\ a^{q+p} \\ \vdots \end{array}$$

$$F_n' = P^t F_n P = \begin{pmatrix} X_0 & \cdots & X_{p-1} \\ X_{p-1} & X_0 & \cdots & X_{p-2} \\ \\ \end{pmatrix}$$

X_j Faltung der Länge q, angeordnet als Faltung der Länge p.

$$F_n' \begin{pmatrix} y_0 \\ \vdots \\ y_{n-1} \end{pmatrix}_{u_j} = F_n' \begin{pmatrix} u_0 \\ \vdots \\ u_{p-1} \end{pmatrix} = \begin{pmatrix} X_0 u_0 + \ldots + X_{p-1} u_{p-1} \\ X_{p-1} u_0 + \ldots + X_{p-2} u_{p-1} \\ \\ X_1 u_0 + \ldots + X_0 u_{p-1} \end{pmatrix} \quad \text{in } F!$$

(u_j mit Länge q)

Faltung der Länge n = Faltung der Länge p mit Mult. $\hat{=}$ Faltung der Länge q, 1 Add $\hat{=}$ q Add.

$M(n) =:$ Anzahl Mult / $A(n)$: Anzahl Add für Faltung der Länge n über Körper F. in F.

$$M(n) = M(p)\, M(q),\ A(n) = M(p)\, A(q) + A(p) \cdot q.$$

14.15-77: Übungen! s.t.

$n = 6 = 2 \cdot 3 = 3 \cdot 2.\ C_6 = C_2 \odot C_3 = C_3 \odot C_2$. a 6. Einheitswurzel, $a = e^{\pi i/3}$

$C_2 = \{1, a^3\} = \{0,3\}$, $C_3 = \{1, a^2, a^4\} = \{1,2,4\}$

Gruppentafel:

⊕	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

⊕	0	2	4	3	5	1
0	0	2	4	3	5	1
2	2	4	0	5	1	3
4	4	0	2	1	3	5
3	3	5	1	0	2	4
5	5	1	3	2	4	0
1	1	3	5	4	0	2

oder auch

⊕	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	6	4	1
5	5	2	6	3	1	4

03, 25, 41

Rechenops: $C_2 \odot C_3$:

$A(6) = M(2) A(3) + 3 A(2)$

$C_3 \odot C_2$

$A(6) = M(3) A(2) + 2 A(3)$

n	$M(n)$	$A(n)$	
2	2	4	
3	4	(17)	auf 10 reduzierbar
HA: 4			
6	8	(46) (50)	nicht eindeutig

(c) Transposition

Auswertung von t Bilinearformen, $\sum_{i=1}^{s} \sum_{j=1}^{r} a_{ijk} x_i y_j,\ k = 1 \ldots t.$

Alg. mit m Multiplikationen, ohne Operationen auf x: ($\alpha, \beta \in \mathbb{Z}!$, γ, f)

$$\sum_{\ell=1}^{m} \gamma_{\ell k} \frac{1}{f_\ell} \left(\sum_{i=1}^{s} \alpha_{\ell i} x_i\right) \left(\sum_{j=1}^{r} \beta_{\ell j} y_j\right) = \sum_{i=1}^{s} \sum_{j=1}^{r} a_{ijk} x_i y_j$$

Transponierte Bilinearform: $\sum_{k=1}^{t} \sum_{j=1}^{r} a_{ijk} z_k y_j$ für $i = 1 \ldots s$.

$$\sum_{k=1}^{t} z_k \sum_{i=1}^{s} \sum_{j=1}^{r} a_{ijk} x_i y_j = \sum_{i=1}^{s} x_i \sum_{k=1}^{t} \sum_{j=1}^{r} a_{ijk} z_k y_j$$

$$= \sum_{k=1}^{t} z_k \sum_{\ell=1}^{m} \gamma_{\ell k} \left(\frac{1}{f_\ell} \sum_{i=1}^{s} \alpha_{\ell i} x_i\right) \left(\sum_{j=1}^{r} \beta_{\ell j} y_j\right) = \sum_{i=1}^{s} x_i \sum_{\ell=1}^{m} \alpha_{\ell i} \left(\frac{1}{f_\ell} \sum_{k=1}^{t} \gamma_{\ell k} z_k\right) \left(\sum_{j=1}^{r} \beta_{\ell j} y_j\right)$$

$$\Rightarrow \sum_{k=1}^{t}\sum_{j=1}^{r} a_{ijk} z_k y_j = \sum_{l=1}^{m} \alpha_{li}\left(\frac{1}{f_l}\sum_{k=1}^{t}\gamma_{lk} z_k\right)\left(\sum_{j=1}^{r}\beta_{lj} y_j\right)$$

$$w_k = \sum_{i=0}^{n-1} x_i \underset{\text{mod } n!}{y_{k-i}} = \sum_{l=1}^{m} \gamma_{lk}\left(\frac{1}{f_l}\sum_{i=1}^{s}\alpha_{li} x_i\right)\left(\sum_{j=1}^{r}\beta_{lj} y_j\right)$$

$$w_i' = \sum_{k=0}^{n-1} z_k y_{k+i} = \sum_{l=1}^{m} \alpha_{li}\left(\frac{1}{f_l}\sum_{k=1}^{n-1}\gamma_{lk} z_k\right)\left(\sum_{j=1}^{n-1}\beta_{ij} y_j\right)$$

~~n=3~~ ~~Beisp~~:

(a) CRT $\begin{pmatrix} w_0 \\ w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} x_0 & x_2 & x_1 \\ x_1 & x_0 & x_2 \\ x_2 & x_1 & x_0 \end{pmatrix}\begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix}$

$s_0 = y_0+y_1+y_2 \qquad m_0 = \frac{x_0+x_1+x_2}{3} s_0 \qquad w_0 = m_0+m_1-2m_2+m_3$

$s_1 = y_0-y_2 \qquad m_1 = \frac{x_0-x_2}{3} s_1 \qquad w_1 = m_0+m_1+m_2-2m_3$

$s_2 = y_1-y_2 \qquad m_2 = \frac{x_1-x_2}{3} s_2 \qquad w_2 = m_0-2m_1+m_2+m_3$

$s_3 = y_0-y_1 \qquad m_3 = \frac{x_0-x_1}{3} s_3$

(b) die Produkte

(c) Transposition.

$$w_k = \sum_{i=0}^{n-1} x_i y_{k-i} = \sum_{l=1}^{m} \gamma_{lk}\left(\frac{1}{f_l}\sum_{i=0}^{n-1}\alpha_{li} x_i\right)\left(\sum_{j=0}^{n-1}\beta_{lj} y_j\right),\ k=0..n-1$$

$$\Rightarrow w_i' = \sum_{k=0}^{n-1} z_k y_{k-i} = \sum_{l=1}^{m} \alpha_{li}\left(\frac{1}{f_l}\sum_{k=0}^{n-1}\gamma_{lk} z_k\right)\left(\sum_{j=0}^{n-1}\beta_{lj} y_j\right),\ i=0..n-1.$$

Schema:

γ	α	β	
1 1 1	1 1 1 ·	1 1 1	m_0
1 1 -2	1 0 -1 ·	1 0 -1	m_1
-2 1 1	0 1 -1 ·	0 1 -1	m_2
1 -2 1	1 -1 0 ·	1 -1 0	m_3
$w_0\ w_1\ w_2$ ~~$m_0\ m_1\ m_2$~~ m_3	$(x_0\ x_1\ x_2)$	$(y_0\ y_1\ y_2)$	
12 Add.	nicht gezählt!	5 Add.	

$f_l = 3$

Transposition:

1 1 1	1 1 1	1 1 1
1 0 -1	1 1 -2	1 0 -1
0 1 -1	-2 1 1	0 1 -1
1 -1 0	1 -2 1	1 -1 0
$w_0'\ w_1'\ w_2'$	$z_0\ z_1\ z_2$	$y_0\ y_1\ y_2$
6 Add.	nicht gezählt!	5 Add.

$\Rightarrow$ 5 Mult., 11 Add.

Transponierter Alg: $s_0 .. s_3$ wie oben.

$m_0 = \frac{z_0+z_1+z_2}{3} s_0 \qquad w_0' = m_0+m_1+m_3$

$m_1 = \frac{z_0+z_1-2z_2}{3} s_1 \qquad w_1' = m_0+m_2-m_3$

$m_2 = \frac{-2z_0+z_1+z_2}{3} s_2 \qquad w_2' = m_0-m_1-m_2$

$m_3 = \frac{z_0-2z_1+z_2}{3} s_3$

$n=6:\ C_6 = C_2 \cdot C_3$

n	M(n)	A(n)
2	2	4
3	4	11
4	5	15
5	8 (10)	(31)
6	8	34
1	1	0

| Mult. nicht optimal

Satz 9.1: Sei F Körper der Charakteristik 0, ~~falls~~ ($\Leftrightarrow n \cdot 1 \neq 0\ \forall n$) und P sei (Winograd / sein Primkörper ($\Leftrightarrow$ Körper der erzeugt ist von $\{n \cdot 1 : n \in \mathbb{N}\}$), d. h. $\mathbb{Q}$.
Toom)
1968 Sei k die Anzahl der Teiler $\leq n$ von n. Dann kann man die zyklische Faltung der Länge n über F mit $(2n-k)$ Multiplikationen berechnen. Dabei werden Vorberechnungen auf einem der Faktoren nicht gezählt.

Beweis: 1) Kreisteilungspolynome: $\Phi_d(x)$: $x^n-1=\prod_{d|n}\Phi_d(x)$. (rekursive Def.).

$\Phi_1=x-1$, $\Phi_2=x+1$, $\Phi_3=x^2+x+1$, $\Phi_4=x^2+1$, $\Phi_5=x^4+x^3+x^2+x+1$.

Eig: i) Φ_d „ganzzahlig" (Koeff. sind Vielfache der 1).

ii) Φ_d irreduzibel (weil Char $F=0$)

iii) $(\Phi_d, \Phi_{d'})=1$ für $d\neq d'$.

$\Rightarrow x^n-1=p_1\cdots p_k$, $k=\#$ Teiler $\leq n$, ganzzahlig, irred., paarweise teilerfremd

2) $f, g\in F[z]$, Grad k bzw. l.

fg ist mit $k+l+1$ Mult. berechenbar

(Mult. mit festen Faktoren aus $\underset{\uparrow}{P}^{\text{Primkörper}}$ werden nicht gezählt)

Alg: Wähle $k+l+1$ versch. Elemente aus P, $a_0\cdots a_{k+l}$.

(1) $f(a_i)g(a_i)$: ($k+l+1$ Mult.)

(2) $fg=\sum w_i (fg)(a_i)$, $w_i=\dfrac{\prod_{j\neq i}(z-a_j)}{\prod_{j\neq i}(a_i-a_j)}$.

3) CRT: $(fg)\bmod \overbrace{p_1\cdots p_k}^{x^n-1}=p_1q_1\, fg \underset{\uparrow}{\bmod}\, P_2+P_2q_2\, fg\bmod p_1$
$\quad p_1\cdot P_2 \qquad\qquad f\bmod P_2\cdot g\bmod P_2=2(\text{grad}(P_2)-1)+1$ Mult.

$M(p)=\#$Mult. von $fg \bmod p$, $p\in P[z]$

$M(p_1\cdots p_k)=\underbrace{M(p_2\cdots p_k)}_{M(p_2)+M(p_3\cdots p_k)}+M(p_1)=\sum_{i=1}^{k}M(p_i)=\sum_{i=1}^{k}(2\,\text{grad}\,p_i-1)=2n-k$

$fg \bmod x^n-1$: $2n-k$ Mult. $+$? Anzahl von Mult mit Elementen aus P.

Gehe über nach $\frac{a}{b}$ und schiebe die Mult. auf die g.

§10. FFT nach Winograd:

$$W_n=\begin{pmatrix}1 & \cdots & 1\\ \vdots & \boxed{w^{kl\bmod n}_{k,l=1..n-1}} & \\ 1 & & \end{pmatrix}, \quad w=e^{-2\pi i/n}.$$

n prim $\Rightarrow$ hier steht Gruppentafel von M_n.
n nicht prim $\Rightarrow$ nach Weglassen ~~der~~ zu n nicht teilerfremden Zeilen und Spalten steht hier M_n

$p\neq 2$, $n=p^r$: $M_n\cong C_{(p-1)p^{r-1}}$. Nach Zeilen-, Spaltenumordnung: W_n durch Faltung berechnen. (Rader 1968)

Beisp.: $n=7$: $M_7\cong C_6=\{1,a,a^2,a^3,a^4,a^5\}$. erz. Element ist 3. $\Rightarrow C_6=\{1,3,2,6,4,5\}$

$$W_7\to W_7':\quad \begin{array}{c|ccccccc} & 0 & 1 & 3 & 2 & 6 & 4 & 5\\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 0 & 1 & 3 & 2 & 6 & 4 & 5\\ 3 & 0 & 3 & 2 & 6 & 4 & 5 & 1\\ 2 & 0 & 2 & 6 & 4 & 5 & 1 & 3\\ 6 & 0 & 6 & 4 & 5 & 1 & 3 & 2\\ 4 & 0 & 4 & 5 & 1 & 3 & 2 & 6\\ 5 & 0 & 5 & 1 & 3 & 2 & 6 & 4\end{array}$$

w^n!
zykl. Faltung der Länge 6. + Schulmethode für 1. Spalte, Zeile.
8 Mult. + (34+17) Add.

FFT für Primzahlpotenzen: $n=p^r, p\neq 2$. $n=9=3^2$

$M_9=\{1,2,4,5,7,8\}\cong C_6$. $a=5$ ist erz. Element von $M_9=\{1,a\,..\,a^5\}=\{1,5,7,8,4,2\}$.

W_9':

	0	3	6	1	5	7	8	4	2	
0	1	1	1	1	1	1	1	1	1	← Fourier-Transf. der Länge 3.
3	1	1	1	w^3	w^6	w^3	w^6	w^3	w^6	
6	1	1	1	w^6	w^3	w^6	w^3	w^6	w^3	
1	1	w^3	w^6	w	w^5	w^7	w^8	w^4	w^2	zykl. Faltung der Länge 6
5	1	w^6	w^3	w^5	w^7	w^8	w^4	w^2	w	
7	1	w^3	w^6	w^7	w^8	w^4	w^2	w	w^5	
8	1	w^6	w^3	w^8	w^4	w^2	w	w^5	w^7	
4	1	w^3	w^6	w^4	w^2	w	w^5	w^7	w^8	
2	1	w^6	w^3	w^2	w	w^5	w^7	w^8	w^4	

$n=2^r$: $n=8=2^3$: $M_{2^r}\cong C_2\times C_{2^{r-2}}$ $(r\geq 2)$. $\Rightarrow M_8\cong C_2\times C_2$. $C_2=\{1,a\}=\{1,b\}$, $a^2=b^2=(ab)^2=1$.

		(1)	(3)	(5)	(7)
		1	a	b	c
1	1	1	a	b	c
3	a	a	1	c	b
5	b	b	c	1	a
7	c	c	b	a	1

Klein'sche Vierergruppe. $M_8=\{1,3,5,7\}$.

vgl. Cooley-Tukey! →

	0	2	4	6	1	3	5	7
0								
2								
4								
6								
1								
3								
5								
7								

Tabelle von FFT's kleiner Länge:

n	# Mult	# Add.	Bem.
2	0	2	—
3	2	6	$M_3\cong C_2$
4	0	8	$M_4\cong C_2$
5	5	17	Üb.
7	8	36	$M_7\cong C_6$
9	10	45	$M_9\cong C_6$
16	10	74	$M_{16}\cong C_2\times C_4$
8	2	26	$M_8\cong C_2\times C_2$

$n=3$: $W_3=\begin{pmatrix}1&1&1\\1&\boxed{w\;\;w^2}\\1&\boxed{w^2\;\;w}\end{pmatrix}$. $M_3\cong C_2$ $\quad w=e^{2\pi i/3}$, $w^2=e^{4\pi i/3}=\bar w$ $=e^{-2\pi i/3}$.

zykl. Faltung Länge 2

$\begin{pmatrix}w_0\\w_1\\w_2\end{pmatrix}=W_3\begin{pmatrix}y_0\\y_1\\y_2\end{pmatrix}$, $\begin{pmatrix}w_1-w_0\\w_2-w_0\end{pmatrix}=\begin{pmatrix}0&w-1&w^2-1\\0&w^2-1&w-1\end{pmatrix}\begin{pmatrix}y_0\\y_1\\y_2\end{pmatrix}$

$w_1-w_0=\underbrace{\frac12(w+w^2-2)}_{\text{reell!}}(y_1+y_2)\overset{(+?)}{+}\overbrace{\frac12(w-w^2)}^{\text{imaginär}}F_1(y_1-y_2)$

$w_2-w_0=\underbrace{\frac12(w+w^2-2)}_{\text{reell!}}(y_1+y_2)\overset{(-?)}{-}\underbrace{\frac12(w-w^2)}_{\text{imaginär!}}(y_1-y_2)$

Alg: $s_1=y_1+y_2$; $s_2=y_1-y_2$; $w_0=s_1+y_0$

$m_1=\frac12(w+w^2-2)s_1$, $m_2=\frac12(w-w^2)s_2$.

$s_3=m_1+w_0$, $w_1=s_3-m_2$, $w_2=s_3+m_2$

$n=7$: $\begin{pmatrix}w_1-w_0\\ \vdots\\ w_5-w_0\end{pmatrix}=\left(0\,\middle|\,\begin{matrix}F_3&\tilde F_3\\ \tilde F_3&F_3\end{matrix}\right)\begin{pmatrix}y_0\\y_1\\y_3\\y_2\\y_4\\y_6\\y_5\end{pmatrix}$

$W_4=\begin{pmatrix}1&1&1&1\\1&i&-1&-i\\1&-1&1&-1\\1&-i&-1&i\end{pmatrix}$ $W_4'=\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&i&-i\\1&-1&-i&i\end{pmatrix}$ 4 Add. in Spalte 3, 4 berechnen $+\,4$ weitere

1. Faltung der Länge 6: 8 Mult, 34 Add.
2. $y_1+y_3+y_2$, $y_4+y_6+y_5$ wird bei $F_3, \hat F_3$ gebildet.
3. Σy_i wird bei Blockfaltung F_2 berechnet.
4. Faltung der Länge 3 enthält $w_k=m_0s_0+\dots$. $w_k+w_0=(m_0s_0+w_0)+\dots$

Satz 10.1: Alle von w abhängigen Multiplikationen in der Tabelle sind entweder Multiplikationen mit reellen oder rein imag. Zahlen.

Bew.: $n=p$ prim^{*2}: $M_p\cong C_{p-1}=\{1,a\,..\,a^{p-2}\}$, a erz. Element.

CRT: $f=w^{a^0}z^0+w^{a^1}z^1+\dots+w^{a^k}z^k+\dots+w^{a^{p-2}}z^{p-2}$. $g=y_{a^0}z^0+y_{a^1}z^1+\dots+y_{a^k}z^k+\dots+y_{a^{p-2}}z^{p-2}$ $\quad z^{\frac{p-1}{2}}$

$fg \bmod z^{p-1}-1$. $z^{p-1}=\underbrace{(z^{p-1/2}-1)}_{p_1}\underbrace{(z^{p-1/2}+1)}_{p_2}$. $f\bmod z^{(p-1)/2}-1=(\underbrace{w^{a^0}+w^{a^{p-1/2}}}_{=w+w^{-1}})z^0+\dots(\underbrace{w^{a^{\frac{p-1}{2}-1}}+w^{a^{p}}}_{=w^{a^{\frac{p-1}{2}-1}}+w^{-a^{\dots}}})$ $\quad w^a+w^{-a}$

$a^{p-1}=1$. $a^{\frac{p-1}{2}}=-1$. Form lautet: $w^\alpha+w^{-\alpha}$, und $\overline{w^\alpha}=\bar w^\alpha=w^{-\alpha}$.

$\Rightarrow f\bmod z^{(p-1)/2}-1$ hat reelle Koeff., $f\bmod p_2$ hat rein imaginäre Koeff..

$fg\bmod z^{\frac{p-1}{2}}-1$ erfordert nur rein reelle bzw. für $fg\bmod z^{\frac{p-1}{2}}+1$ rein imag. Mult. $fg\bmod z^{p-1}-1$ erfordert keine Mult.

§ 10. Winograd FFT. (a) $M_{p^r} \cong C_{(p-1)p^{r-1}} \cong C_2 \otimes C_{2^{r-2}} (p=7)$

(b) $n = n_1 n_2$. $M_n \cong M_{n_1} \otimes M_{n_2}$. $W_n = (w^{kl}), w = e^{-2\pi i/n}$.

$k \in M_n \to (k_1, k_2) \in M_{n_1} \times M_{n_2}, k \to (k \bmod n_1; k \bmod n_2)$. („Ring"-Isom.)

(*) CRT: $n_1 m_1 + n_2 m_2 = 1$, $k = n_1 m_1 k_2 + n_2 m_2 k_1 \pmod n$. $kl = n_1 m_1 (kl \bmod n_2) + n_2 m_2 (kl \bmod n_1)$.
$= n_1 m_1 k_2 l_2 + n_2 m_2 k_1 l_1$

$w^{kl} = w^{n_1 m_1 k_2 l_2 + n_2 m_2 k_1 l_1} = \underbrace{(w^{n_1 m_1})}_{w_2}{}^{k_2 l_2} \cdot \underbrace{(w^{n_2 m_2})}_{w_1}{}^{k_1 l_1} = w_1^{k_1 l_1} \cdot w_2^{k_2 l_2}$

w^k prim. n-te EW $\Leftrightarrow (n,k) = 1$.

Satz 10.2 w_1, w_2 sind prim. n_1- bzw. n_2. EW.

Bew.: $w_1^{n_1} = w^{n_2 m_2 n_1} = w^{n \cdot m_2} = 1$. $w_1 = e^{2\pi i n_2 m_2 / n} = e^{2\pi i m_2 / n_1}$. $(m_2, n_1) = 1$, (*).

$W_n(w)$ wie üblich. $W_{n_1}(w_1) \otimes W_{n_2}(w_2) = W_n(w)$ Tensorprodukt.

Ordne die Elemente von $\mathbb{Z}_n$, $\{0, 1 .. n-1\}$ lexikographisch gemäß $k \to (k_1, k_2)$, d.h. $(0,0) \cdot (0, n_2-1), (1,0) \cdot (1, n_2-1)$ usw.

Bezeichne die umgeordnete Matrix mit W_n'. $W_n'(w) = \begin{pmatrix} w_1^0 W_{n_2}(w_2) & \cdots & \\ \vdots & w_1^1 W_{n_2}(w_2) & w_1^{n_1-1} W_{n_2}(w_2) \\ & w_1^{n_1-1} W_{n_2}(w_2) & w_1 \; W_{n_2}(w_2) \end{pmatrix}$.

$\Rightarrow W_n$ zerfällt in $n_2 \times n_2$-Blöcke, welche DFT's der Länge n_2 sind, angeordnet als DFT der Länge n_1. (Verfahren von Good-Thomas, 1958), Primfaktor-FFT.

Aufg. 24: n	$A(n)$	
288	120	2016
648	240	4512
1296	420	11736

Beisp.: $n = 6 = 3 \cdot 2$ (n_1, n_2), $n_1 - n_2 = 1$: $n_1 + 2n_2 = 1 \bmod 6$. $w_1 = w^{n_2 m_2} = e^{-\frac{4\pi i}{3}}$, $w_2 = w^{n_1 m_1} = e^{-\pi i} = -1$.

k	(k_1, k_2)
0	(0,0)
1	(1,1)
2	(2,0)
3	(0,1)
4	(1,0)
5	(2,1)

Ordnung: 0/3/4/1/2/5.

$W_{n_1}(w_1) = \begin{pmatrix} w_1^0 & w_1^0 & w_1^0 \\ w_1^0 & w_1 & w_1^2 \\ w_1^0 & w_1^2 & w_1 \end{pmatrix}$. Bei Änderung von w_1 erhält man Permutation von ~~[illegible]~~ Spalten.

$W_{n_2}(w_2) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

$$W_6' = \begin{pmatrix} w_1^0 W_2 & w_1^0 W_2 & w_1^0 W_2 \\ w_1^0 W_2 & w_1^1 W_2 & w_1^2 W_2 \\ w_1^0 W_2 & w_1^2 W_2 & w_1^1 W_2 \end{pmatrix} \cdot \begin{pmatrix} u_0 \\ \vdots \\ u_5 \end{pmatrix} = W_6 \begin{pmatrix} Y_0 \\ \vdots \\ Y_5 \end{pmatrix} \overset{=}{\begin{pmatrix} u_0 \\ u_3 \\ u_4 \\ u_1 \\ u_2 \\ u_5 \end{pmatrix}} \begin{pmatrix} U_0 \\ U_1 \\ U_2 \end{pmatrix} = W_6' \overbrace{\begin{pmatrix} Y_0 \\ Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} Y_0 \\ Y_3 \\ Y_4 \\ Y_1 \\ Y_2 \\ Y_5 \end{pmatrix}}^{=}$$

Alg.: $S_1 = Y_1 + Y_2$, $S_2 = Y_1 - Y_2$, $S_3 = Y_0 + S_1$. $M_1 = (\cos\frac{2\pi}{3} - 1) W_2 S_1$. $M_2 = (i \sin\frac{2\pi}{3}) W_2 S_2$.

$M_0 = W_2 S_3$, $S_4 = M_0 + M_1$. $U_0 = M_0$, $U_1 = S_4 + M_2$, $U_2 = S_4 - M_2$.

$\Rightarrow$ 3 Faltungen mit W_2, $c W_2 S_i = c \begin{pmatrix} s_1 + s_2 \\ s_1 - s_2 \end{pmatrix} = \begin{pmatrix} c s_1 + c s_2 \\ c s_1 - c s_2 \end{pmatrix}$,

wobei bei W_2 die Multiplikation mit w_2^0, w_2^1 zählen.

Satz 10.3: $M(n)$ = Anzahl der Mult. für DFT der Länge n einschließlich der Mult. mit w^0.

$A(n) = \#$ Add. für DFT der Länge $n \Rightarrow M(n) \le M(n_1) M(n_2)$, $A(n) \le M(n_1) A(n_2) + n_2 A(n_1)$.

Bem.

n	$M(n)$	$A(n)$
2	2 ↖ rein reell oder kompl. 2 reell/unabh.	2 ↖ komplexe!
3	3	6
4	4	8
5	6	17
7	9	36
8	8	26
9	11	45
16	18	74
6	$3 \cdot 2 = 6$	$3 \cdot 2 + 2 \cdot 6 = 18$
28	$4 \cdot 9 = 36$	$4 \cdot 36 + 7 \cdot 8 = 200$

$3 \cdot 2$
$4 \cdot 7$ Schulmeth.: 784 Mult, 756 Add.

Teil IV: Symmetrie

§ 11. Darstellung endlicher Gruppen. (Literatur: Serre, Lineare Darstellung endl. Gruppen, Vieweg 1972. Stiefel-Fässler, gruppenth. Meth. und ihre Anwendungen. Teubner 1979. Müller, Darstellungstheorie endl. Gruppen 1980)

Def 11.1: Sei G endl. Gruppe, V Vektorraum über $\mathbb{C}$, $\dim V = d$, $GL(V)$ Gruppe der invertierbaren linearen Abb. $V \to V$.

1) Ein Hom.: $\rho: G \to GL(V)$ heißt Darstellung von G in V. ($\rho(s\cdot t) = \rho(s)\cdot\rho(t)$)

2) Grad $(\rho) = d$. Die Darstellung heißt treu, wenn ρ Isomorphismus ist.

3) $\rho, \rho': G \to V, V'$ heißen aequivalent falls ex. $\tau \in GL(V, V')$: $\rho' = \tau\rho\tau^{-1} \Leftrightarrow \rho'(s) = \tau\rho(s)\tau^{-1}$

Es gilt: $\rho(1) = 1$, $\rho(s^{-1}) = \rho(s)^{-1}$.

Beisp.: 1) $\rho(s) = 1 \;\forall s \in G$. ρ heißt Einheitsdarstellung.

2) reguläre Darstellung ρ_{reg}: $V = sp\{\underset{\text{e.u.}}{e_t} : t \in G\}$. $\rho_{reg}(s)(e_t) := (e_{s\cdot t})$ treu.

Matrizenschreibweise von ρ_{reg}: Bezeichne Elemente von G mit $1..n$. $v = \sum_{i=1}^{n} v_i e_i$, $v \in V$, $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$.

$\rho_{reg}(s)(v) = \sum_{i=1}^{n} v_i\, e_{s\cdot i} \underset{j = s\cdot i}{=} \sum_{j=1}^{n} v_{s^{-1}j}\, e_j \Rightarrow \rho(s)\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} v_{s^{-1}1} \\ \vdots \\ v_{s^{-1}n} \end{pmatrix} = P(s)(v)$, $P(s) = \begin{pmatrix} e^t_{s^{-1}1} \\ \vdots \\ e^t_{s^{-1}n} \end{pmatrix} = (e_{s\cdot 1} \dots e_{s\cdot n})$.

Grad $(\rho_{reg}) = |G|$.

3) $G = C_n$, ω n-te EW, $G = \{1, a .. a^{n-1}\}$. $\rho(a^k) := \omega^k$ Darstellung in $\mathbb{C}$ vom Grad 1.

Treu wenn ω primitive n-te Einheitswurzel.

ρ_{reg}: $P(a) = (e_2 .. e_n, e_1)$. (s. Aufg. 9).

4) $G = S_n$ = symm. Gruppe der Perm. von n Elementen.

(a) <u>Alternierende Darstellung</u>: $\rho_{alt}(s) = \begin{cases} 1 & s \text{ gerade} \\ -1 & \text{sonst} \end{cases}$ über $\mathbb{C}$, nicht treu für $n > 2$.

(b) <u>Natürliche Darstellung</u>: $V = sp\{e_1 .. e_n\}$. Sei $\pi \in S_n$, $v = \sum_{i=1}^{n} v_i e_i$. $\rho_{nat}(\pi)(v) = \sum_{i=1}^{n} v_i e_{\pi(i)}$, $P(\pi) = (e_{\pi(1)} .. e_{\pi(n)})$

5) $G = D_n$ = Diedergruppe = Gruppe der Drehungen und Spiegelungen in $\mathbb{R}^2$, die ein reg. n-Eck invariant lassen.

D_n: r = Rot. um Winkel $\frac{2\pi}{n}$. s = Spiegelung an einer festen Winkelhalb. $\Rightarrow$

$D_n = \{ s^l r^k : s^2 = 1, r^n = 1, srs = r^{-1} (sr = r^{-1}s)\}$, also kein direktes Produkt.

Darstellungen von D_n, n gerade:

ρ	$\rho(r^k)$		$\rho(s\cdot r^k)$	Grad
ρ_1	1		1	1
ρ_2	1	nicht eind.	-1	1
ρ_3	$(-1)^k$	$\Leftrightarrow$ Kennung.	$(-1)^k$	1
ρ_4	$(-1)^k$		$(-1)^{k+1}$	1
ρ_5^h	$\begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix}^{h\cdot k}$		$\begin{pmatrix} 0 & w^{-1} \\ w & 0 \end{pmatrix}^{kh}$	2

$\omega = e^{2\pi i/n}$, $0 < h < \frac{n}{2}$

Es gilt: ρ_5^{n-h} ist äq. zu ρ_5^h:

$\rho_5^{n-h} = \begin{pmatrix} w^{-1} & 0 \\ 0 & w \end{pmatrix}^{hk} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\tau} \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix}^{hk} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\tau^{-1}}$

Def 11.2: Darstellung ρ von G in V reduzibel $:\Leftrightarrow$ Es gibt einen echten Unterraum V_1 $(\{0\}\neq V_1\neq V)$ mit $\rho(s)(V_1)\subset V_1\ \forall s\in G$, d.h. V_1 invariant bzgl. ρ, V_1 inv. Unterraum von ρ.

Andernfalls heißt ρ irreduzibel.

Beisp.: 1) Einheitsdarstellung irred $\Leftrightarrow$ Grad $=1$. 2) Grad $\rho=1\Rightarrow\rho$ irreduzibel.

3) ρ_{reg} reduzibel für Grad $\rho_{reg}>1$. $V_1:=sp\left\{\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}\right\}$.

ρ reduzibel, $V=sp\{v_1..v_n\}$, $V_1=sp\{v_1..v_m\}$, $m<n$. $R(s)$ Matrix von $\rho(s)$ bez. $v_1\dots v_n$.

$$R(s)=\begin{array}{cc} & m \\ m & \begin{pmatrix}R_{11}(s) & R_{12}(s)\\ 0 & R_{22}(s)\end{pmatrix}\end{array},\quad R(s)R(t)=\begin{pmatrix}R_{11}(s)R_{11}(t) & \sim\\ 0 & R_{22}(s)R_{22}(t)\end{pmatrix}=\begin{pmatrix}R_{11}(st) & \sim\\ 0 & R_{22}(st)\end{pmatrix}$$

$\Rightarrow R_{11}$ def. Darstellung von G in V_1

R_{22} def. Darstellung vom Grade $n-m$

Def 11.3: $V=\bigoplus_{i=1}^{r}V_i$, ρ_i seien Darstellungen einer Gruppe G in V_i. Dann heißt die Darstellung $\rho(s)(v)=\sum_{i=1}^{r}\rho_i(s)(v_i)$, $v=\sum_{i=1}^{r}v_i$, $v_i\in V_i$, die direkte Summe $\rho=\rho_1+\dots+\rho_r$ von $\rho_1\dots\rho_r$.

Seien v_{ij}, $j=1..n_i$, Basis von V_i. Dann hat V die Basis $\{v_{11}..v_{1n_1}, v_{21}..v_{2n_2},..v_{r1}..v_{rn_r}\}$.

Bezüglich dieser Basis nimmt ρ die Form an: $R(s)=\begin{pmatrix}R_1(s) & 0 & 0\\ 0 & R_2(s) & 0\\ 0 & 0 & R_r(s)\end{pmatrix}$.

Satz 11.1: Jede Darstellung ist direkte Summe irreduzibler Darstellungen.

Bew.: 1) ρ ist bez. eines geeigneten inneren Produkts $\langle,\rangle$ in V unitär, d.h. $\langle\rho(s)u,\rho(s)v\rangle=\langle u,v\rangle$ für alle $s\in G$:

$\rho(s)$ habe Matrix $R(s)$ bez. einer Basis $\mathcal{B}$. $\langle u,v\rangle:=\frac{1}{|G|}\sum_{t\in G}(R(t)u)^t\overline{(R(t)v)}$

$$\langle R(s)u,R(s)v\rangle=\frac{1}{|G|}\sum_{t\in G}(\underbrace{R(t)R(s)}_{R(t\cdot s)}u)^t\overline{(\underbrace{R(t)R(s)}_{R(t\cdot s)}v)}=\frac{1}{|G|}\sum_{t'\in G}(R(t')u)^t\overline{(R(t')v)}=\langle u,v\rangle.$$

2) Jede unitäre Darstellung ist direkte Summe irred. Darstellungen:

ρ irreduzibel: $\checkmark$. ρ reduzibel: $\exists V_1\subset V$, $\{0\}\neq V_1\neq V$: $\rho(V_1)\subset V_1$. $V_2:=V_1^{\perp}$ bzgl. $\langle,\rangle$.

Sei $u\in V_1$, $v\in V_2$. $\langle\rho(s)v,u\rangle=\langle\rho(s)v,\rho(s)\rho(s^{-1})u\rangle=\langle\underbrace{v}_{\in V_2=V_1^{\perp}},\underbrace{\rho(s^{-1})u}_{\in V_1}\rangle=0\Rightarrow\rho(s)v\in V_1^{\perp}=V_2$,

V_2 invariant unter ρ.

Bzgl. geeigneter Basis hat $\rho(s)$ die Darstellung: $\begin{pmatrix}R_{11}(s) & 0\\ 0 & R_{22}(s)\end{pmatrix}$, $\rho=\rho_1+\rho_2$. Induktion $\square$.

~~Beisp~~. Kor.: Man kann annehmen, daß ρ unitär ist mit $\rho^*(s)=\rho(s^{-1})$.

Bem.: Die Herstellung der direkten Zerlegung in irred. Darstellungen heißt Ausreduktion

Beisp.: Ausreduktion von ρ_{reg} für $G=C_n$. $V_i=sp\left\{\begin{smallmatrix}\omega_i^{1}\\ \vdots\\ \omega_i^{n-1}\end{smallmatrix}\right\}$, $\omega_i:=e^{2\pi i/n}$. $P\begin{pmatrix}v_0\\ \vdots\\ v_{n-1}\end{pmatrix}=\begin{pmatrix}v_{n-1}\\ v_0\\ \vdots\\ v_{n-2}\end{pmatrix}$

$$P\begin{pmatrix}1\\ \vdots\\ \omega_i^{n-1}\end{pmatrix}=\begin{pmatrix}\omega_i^{n-1}\\ \omega_i^{0}\\ \vdots\\ \omega_i^{n-2}\end{pmatrix}=\omega_i^{-1}\begin{pmatrix}\omega_i\\ \vdots\\ \omega_i^{n-1}\end{pmatrix}\Rightarrow PV_i\subset V_i,\ P_{reg}(a^k)=P^k,\ P^kV_i\subseteq V_i,\ k=0..n-1.$$

$\Rightarrow V_i$ inv. Unterraum von ρ_{reg}. $C_n=\{1,a..a^{n-1}\}$, $v_i\in V_i$. $\rho_{reg}(a)v_i=\omega^{-1}v_i$.

$\rho_i(a^k)=\omega_i^{-k}$, Grad $=1$. $\rho=\rho_1+\dots+\rho_n$.

Satz 11.2 (Lemma von Schur): Seien ρ_i irreducible Darstellungen von $G \to V_i$, $i=1,2$. Sei $\tau: V_1 \to V_2$ linear und $\tau\rho_1(s)=\rho_2(s)\tau \ \forall s \in G$.

(a) ρ_1, ρ_2 nicht aequivalent $\Rightarrow \tau = 0$.

(b) $\rho_1=\rho_2 \Rightarrow \tau=\lambda, \lambda \in \mathbb{C} \Leftrightarrow \tau x = \lambda x \ \forall x \in V_1$.

Bew.: (a) $W_1 := \{x \in V_1 : \tau(x)=0\} = \tau^{-1}(0)$

W_1 invariant unter ρ_1: $x \in W_1 \Rightarrow \tau\rho_1(s)(x) = \rho_2(s)\underbrace{\tau x}_{0} = 0 \Rightarrow \rho_1(s)x \in W_1$.

Da ρ_1 irreducibel ist $W_1=\{0\}$ oder $W_1=V_1$. $W_1=\{0\} \overset{???}{\Rightarrow} \tau$ invertierbar $\Rightarrow \rho_2 = \tau\rho_1(s)\tau^{-1}$ ↯
Nebenbetrachtung: τ surj. $\Rightarrow \tau = 0$.

(b) $\rho_1=\rho_2 \Rightarrow \tau: V_1 \to V_1$. $\exists \lambda \in \mathbb{C}, x \in V_1, x \neq 0: \tau x = \lambda x$, $\tau' = \tau - \lambda$.

$W_1' = \{x \in V_1 : \tau' x = 0\}$, $\tau'\rho_1(s) = \rho_2(s)\tau' \overset{(a)}{\Rightarrow} W_1' = \{0\}$ ↯ ($x \in W_1'$) oder $W_1' = V_1 \Rightarrow \tau' = 0 \Rightarrow \tau = \lambda$

Satz 11.3: ρ_i irred. Darstellungen von G in V_i, $\tau: V_1 \to V_2$ linear, $\tau' = \frac{1}{|G|}\sum_{t\in G}\rho_2(t^{-1})\tau\rho_1(t)$

(a) ρ_1, ρ_2 nicht äq. $\Rightarrow \tau' = 0$.

(b) $\rho_1=\rho_2 \Rightarrow \tau' = \frac{1}{d}\,Tr(\tau)$, d = Grad ρ_1 = dim V_1, $Tr(\tau)$ = Spur$(\tau) = \sum_{i=1}^{d} R_{ii}$; $R = (R_{k\ell})$ Matrix zu τ.

Bew.: Sei $s \in G$. $\rho_2(s)\tau' = \frac{1}{|G|}\sum_{t\in G}\rho_2(s)\rho_2(t^{-1})\tau\rho_1(t) = \frac{1}{|G|}\sum_{t'\in G}\rho_2(t')\tau\underbrace{\rho_1(t'^{-1}s)}_{\rho_1(t'^{-1})\rho_1(s)}$

$= \left(\frac{1}{|G|}\sum_{t\in G}\rho_2(t)\tau\rho_1(t^{-1})\right)\rho_1(s) = \tau'\rho_1(s)$.

(a) $\tau' = 0$ nach 11.2 (a), (b) $\tau' = \lambda$ nach 11.2 (b), $Tr(\tau') = \lambda d$, $Tr(\tau') = \frac{1}{|G|}\sum_{t\in G} Tr(\rho_1(t)^{-1}\tau\rho_1(t))$

$= \frac{1}{|G|}\sum_{t\in G} Tr(\tau) = Tr(\tau) \Rightarrow \lambda = \frac{1}{d}\,Tr(\tau)$.

Satz 11.4: ρ_i irred. Darst. von G in V_i, $i=1,2$. $R^i(s)$ Matrix zu $\rho_i(s)$.

(a) $\rho_{1,2}$ nicht aequivalent $\Rightarrow \frac{1}{|G|}\sum_{t\in G} R^1_{k\ell}(t^{-1})R^2_{k'\ell'}(t) = 0 \ \forall k, \ell, k', \ell'$.

(b) $\rho_1 = \rho_2 \Rightarrow \frac{1}{|G|}\sum_{t\in G} R^1_{k\ell}(t^{-1})R^1_{k'\ell'}(t) = \frac{1}{d}\,\delta_{k+i\ell,\,k'+i\ell'}$ (i imag)

Beisp.: D_n, n gerade: ρ_1, ρ_2
$\{s^s r^k : s=0,1,\ r=0..n-1\}$ $R_1 = 1$, $R^2 = \pm 1$ $\begin{matrix}\ell=0\\ \ell=1\end{matrix}$

$\frac{1}{2n}\left(\sum_{k=0}^{n-1} 1\cdot 1 + \sum_{k=0}^{n-1} 1\cdot(-1)\right) = 0$. ρ_1, ρ_5^h: $\frac{1}{2n}\left\{\sum_{k=0}^{n-1} 1\cdot\begin{pmatrix}\omega^{-hk} & 0\\ 0 & \omega^{hk}\end{pmatrix} + \sum_{k=0}^{n-1}\begin{pmatrix}0 & \omega^{hk}\\ \omega^{-hk} & 0\end{pmatrix}\right\} = 0$.

$R_2 = R^h = \begin{pmatrix}\omega^{-hk} & 0\\ 0 & \omega^{hk}\end{pmatrix} (s=0)$ bzw. $\begin{pmatrix}0 & \omega^{hk}\\ \omega^{-hk} & 0\end{pmatrix} (s=1)$. ρ_5^h, ρ_5^h: $(1,1)$: $\frac{1}{2n}\left(\sum_{k=0}^{n-1}\omega^{hk}\omega^{-hk}\right) = \frac{1}{2} = \frac{1}{d}$.

Def 11.4: ρ Darstellung von G in V. Dann heißt $\chi: G \to \mathbb{C}$, $\chi(s) := Tr(\rho(s))$, $s \in G$

der Charakter von ρ.

Eigenschaften: 1) Äquivalente Darstellungen haben den gleichen Charakter.

2) $d = \chi(1)$, d = Grad von ρ. 3) $\chi(a^{-1}sa) = \chi(s)$. 4) $\rho = \rho_1 + \dots + \rho_n$, direkte Summe

$\Rightarrow \chi = \chi_1 + \dots + \chi_n$. 5) $\overline{\chi}(s) = \chi(s^{-1})$ (OE ρ unitär bzgl. geeigneter Basis).

6) Führe auf den Charakteren von $G \to \mathbb{C}$ inneres Produkt ein: $(\varphi, \psi) := \frac{1}{|G|}\sum_{t\in G}\varphi(t)\overline{\psi(t)}$. Für zwei irred. Charaktere,

d. h. Charaktere irred. Darstellungen χ, χ' gilt: $(\chi,\chi')=1$, falls χ,χ' aequivalent, 0 sonst.

Bew. zu 6): $\chi_i = Tr(\rho_i) = \sum_{k=1}^{d_i} R^i_{kk}$, d_i Grad von ρ_i. 11.4 $\Rightarrow (\chi_1,\chi_2) = \frac{1}{|G|}\sum_{t\in G}\chi_1(t)\chi_2(t^{-1})$

$$= \frac{1}{|G|}\sum_{k=1}^{d_1}\sum_{l=1}^{d_2}\sum_{t\in G} R^1_{kk}(t)\, R^2_{ll}(t^{-1}) = \begin{cases}0 & \rho_1,\rho_2 \text{ nicht äq.}\\ 1 & \text{sonst}\end{cases}$$

$$\text{und } \sum_{k=1}^{d_1} \underbrace{\frac{1}{|G|}\sum_{t\in G} R^1_{kk}(t)\, R^1_{kk}(t^{-1})}_{=1/d_1} = 1 \text{ sonst.}$$

Direkte Summe: $\rho = \rho_1' + \dots + \rho_r'$.

Fasse äq. Darstellungen zusammen. $\rho = c_1\rho_1' + c_2\rho_2' + \dots + c_m\rho_m'$.

(c_1: gibt an wie oft ρ_1' in ρ vorkommt oder äquivalent vorkommt!)

$\Rightarrow \rho = \sum c_i\rho_i$, ρ_i paarw. inaequivalent (auf neuer Basis!!!). Matrix: $\begin{pmatrix} \overbrace{\boxed{\rho_1}\ \boxed{\rho_1}\ \boxed{\rho_1}}^{c_1}\ \overbrace{\boxed{\rho_2}\ \boxed{\rho_2}}^{c_2}\ \boxed{\rho_3} & \text{usw.}\end{pmatrix}$.

Satz 11.5: Jede Darstellung läßt sich (bis auf Reihenfolge) eindeutig als direkte Summe paarweise inaequivalenter irred. Darstellungen schreiben.

Sind χ und χ_i die Charaktere von ρ, ρ_i, so gilt $c_i = (\chi,\chi_i)$.

Bew.: 11.1 $\Rightarrow \rho = \rho_1' + \dots + \rho_r'$, ρ_i' irred. $(\chi,\chi_i) = \frac{1}{|G|}\sum_{t\in G}\chi(t)\overline{\chi_i(t)}$ $\quad \chi,\chi_i : G \to \mathbb{C}$, $\chi_\rho(t) = sp(Mat(\rho(t)))$

$(\chi,\chi_i) = \sum_{k=1}^{r}(\underset{\text{Char. von }\rho_k'}{\chi_k'}, \chi_i) = \#(\rho_k' \text{ aequivalent zu } \rho_i)$

unabhängig von der Zerlegung!

Satz 11.6: Darstellungen mit gleichen Charakteren sind aequivalent.

Bew.: ρ, ρ' Darstellungen mit gemeinsamen Charakter χ. $\rho = \sum_{i=1}^m c_i\rho_i$, $\rho' = \sum_{i=1}^m c_i'\rho_i$, ρ_i paarw. irred.

$c_i = (\chi,\chi_i) = c_i'$.

Satz 11.7: Sei χ_{reg} der Charakter der regulären Darstellung von G.

1) $\chi_{reg}(s) = \begin{cases}|G| & s=1\\ 0 & \text{sonst}\end{cases}$ 2) Jede irreduzible Darstellung ist in der regulären Darstellung so oft enthalten, wie es ihr Grad angibt $\Leftrightarrow \rho_{reg} = \sum d_i\rho_i$, $d_i = $ Grad ρ_i, ρ_i irred.

3) Sei $d_i = $ Grad (ρ_i), ρ_i irred. paarw. inäq. Darstellungen, $i=1..m$.

$|G| = \sum_{i=1}^m d_i^2$.

Bew.: $\rho_{reg}(s)(e^t) = e_{st}$. Matrix: $(e_{s1} \dots e_{sm})$, Diag. unbesetzt für $s\neq 1 \Rightarrow$ Beh.

2) $\chi_i = Tr(\rho_i)$. $(\varphi,\chi_i) = \frac{1}{|G|}\sum_{t\in G}\varphi(t)\chi_i(t^{-1}) = \frac{1}{|G|}\chi_i(1) = d_i = $ Grad (ρ_i).

3) $|G| = \varphi(1) = \sum_{i=1}^{m} d_i \underbrace{Tr(\rho_i(1))}_{d_i}$.

Beisp.: $\chi_5^h = Tr\,\rho_5^h$. $\chi_5^h(r^k) = \omega^{-kh} + \omega^{kh} = 2\cos(2\pi kh/n)$, $\omega = e^{2\pi i/n}$. $\chi_5^h(sr^k) = 0$.

χ_5^h irreduzibel? $(\chi_5^h,\chi_5^h) = \frac{1}{2n}\sum_{k=0}^{n-1}\chi_5^h(r^k)\chi_5^h(r^{-k}) = \frac{1}{2n}\sum 4\cos^2(2\pi kh/n) = \underset{h>0,\ h\neq n/2}{1}$ (?).

$h=0$: $(\chi_5^0,\chi_5^0) = 2 \Rightarrow$ nicht irred.

vollständig: $\sum_{i=1} d_i^2 + \sum_{0<h<\frac{n}{2}}(d_5^h)^2 = 4 + (\frac{n}{2}-1)\cdot 4 = 2n = |D_n|$.

G Gruppe. $a \sim b \Leftrightarrow \exists s : a = s b s^{-1}$, $a, b, s \in G$.

Aequivalenzklassen $A_1 - A_k$ bzgl. „$\sim$“, $1 \in A_1$, $g_i = |A_i|$. $h : G \to \mathbb{C}$ heißt Klassenfkt., wenn $h|A_i$ konstant, $i = 1..k$. Beispiel für Klassenfunktion: $\chi_j = \mathrm{Tr}\, \rho_j$, ρ_j Darstellungen von G.

11.8 Satz: $\rho_1 \dots \rho_N$ vollständige Liste inaequivalenter irreduzibler Darstellungen von G.

a) $N = K$. b) Jede Klassenfunktion ist Linearkombination der Charaktere.

c) $\chi_j(A_i) := \sqrt{\frac{g_i}{g}}\, \chi_j(s)$, $s \in A_i$. Die χ_j bilden bzgl. $(u,v) = \sum_{i=1}^{k} u(A_i)\overline{v(A_i)}$ ein ONS.

Bew.: a) $N \leq K$. $(\chi_j, \chi_k) = \sum_{i=1}^{k} \sqrt{\frac{g_i}{g}}\, \chi_j(A_i) \overline{\sqrt{\frac{g_i}{g}}\, \chi_k(A_i)} = \frac{1}{g} \sum_{\substack{i=1 \\ s_i \in A_i}}^{k} g_i\, \chi_j(s_i)\, \overline{\chi_k}(s_i)$

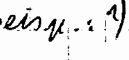
$$= \frac{1}{g} \sum_{i=1}^{k} \sum_{s \in A_i} \chi_j(s)\, \overline{\chi_k}(s) = \frac{1}{g} \sum_{s \in G} \chi_j(s)\, \chi_k(s^{-1}) = \begin{cases} 1 & j = k \\ 0 & \text{sonst} \end{cases}$$ ON-Eig. für Char.!

b, c): ohne Bew.

§ 12. Operatoren mit Symmetrien

Def 12.1 G Gruppe, ρ Darstellung von G in V, $\alpha: V \to V$ linear.

α hat die Symmetrien von ρ, falls $\alpha\rho(s) = \rho(s)\alpha \;\forall s \in G$.

Beisp.: 1)  Symmetrieachse, unter Belastung: Diskretisiere, numeriere die Punkte 1 .. 26.

a_{ik} = Kraft, die in Knoten i bei Auslenkung des Knoten k um 1 Einheit auftritt.

Bei Auslenkung $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ tritt Kraft $\left(A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right)_i$ im Knoten i auf.

Problem: $b = Ax$ gegeben, x gesucht.

P vertausche symmetrisch gelegene Knoten, $APx = Pb = PAx$, d.h. $AP = PA$, $P^2 = 1$.

$G = C_2 = \{1, -1\}$, $\rho(1) = I$, $\rho(-1) = P$. $V = \mathbb{C}^n$.

2) $\begin{matrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{matrix}$ A wie in 1), $G = D_4$. Jedes $s \in D_4$ führt zu Perm. $\pi(s)$ der Knoten 1 .. 9.

$P_\pi = \begin{pmatrix} e_{\pi_1}^t \\ \vdots \\ e_{\pi_n}^t \end{pmatrix}$, $P_\pi \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\pi_1} \\ \vdots \\ x_{\pi_n} \end{pmatrix}$. $\rho: s \to \pi(s) \to P_{\pi(s)}$, ρ Darst. vom Grad $n = 9$.

$A P_{\pi(s)} = P_{\pi(s)} A$, $s \in D_4$.

3) A zykl. Faltung der Länge n. Aufg. 9: $AP = PA$, $P = (e_2 \dots e_n, e_1)$.

$\Rightarrow AP^k = P^k A$. $G = C_n$, $\rho(e^k) = P^k$. A zykl. Falt. $\Leftrightarrow$ A hat Symm. von ρ.

Satz 12.1: G Gruppe, ρ Darstellung von G in $V = \mathbb{C}^n$, $\alpha: V \to V$ linear und besitze die Symm. von ρ.

Stiefel! $V = V_1 \oplus \dots \oplus V_r$, $\rho = \rho_1 + \dots + \rho_r$, $\rho_\ell^{(s)}: V_\ell \to V_\ell$, $\rho_\ell = \sum_{j=1}^{s_\ell} c_{\ell j} \sigma_\ell^j$, σ_ℓ^j irreduzible Darstellungen mit $\sigma_\ell^j, \sigma_k^i$ paarweise inäquivalent für ~~[illegible]~~ $\ell \neq k$.

(a) Bezüglich einer Basis in V in welcher zuerst eine Basis von V_1, dann eine von V_2 usw. steht, wird α durch eine Matrix A der Form $A = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_r \end{pmatrix}$, A_ℓ: $d_\ell \times d_\ell$-Matrizen, $d_\ell = \text{Grad}\,\rho_\ell = \dim V_\ell$ dargestellt.

(b) Sei $\sigma_{\ell j} = \sigma_\ell$, unabhängig von j, d.h. $\rho_\ell = c_\ell \sigma_\ell$, $c_\ell = \sum_j c_{\ell j}$, ($\rho = \sum c_i \sigma_i$, σ_i irred. und paarw. inäqu.)

Dann gibt es Basen in V_ℓ, so daß bzgl. einer Anordnung wie in a),

$A_\ell = \underbrace{\begin{pmatrix} B_\ell & & 0 \\ & \ddots & \\ 0 & & B_\ell \end{pmatrix}}_{d_\ell = \text{Grad}(\sigma_\ell)}$, $B_\ell \in \mathbb{C}^{c_\ell \times c_\ell}$.

Beweis: (a) Bez. Basis der genannten Art besitzt ρ die Gestalt $R = \begin{pmatrix} R_1 & & \\ & \ddots & \\ & & R_r \end{pmatrix}$, $R_\ell \in \mathbb{C}^{d_\ell \times d_\ell}$, R_ℓ Darst. von ρ_ℓ.

Bzgl. der gleichen Basis besitze α die Matrix $A = \begin{pmatrix} A_{11} & \cdots & A_{1r} \\ \vdots & & \\ A_{r1} & \cdots & A_{rr} \end{pmatrix}$. $A_{k\ell} \in \mathbb{C}^{d_k \times d_\ell}$.

$\rho(s)\alpha = \alpha\rho(s) \Leftrightarrow R(s)A = AR(s) \Leftrightarrow$ (*) $R_k(s)A_{k\ell} = A_{k\ell}R_\ell(s)$. ($R_\ell$ irred. $\Rightarrow A_{k\ell} = 0$ ($k \neq \ell$), Lemma v. Schur).

Bezüglich geeigneter Basis in V_ℓ: $R_\ell = \begin{pmatrix} S_\ell^1 & & 0 \\ & \ddots & \\ 0 & & S_\ell^{s_\ell} \end{pmatrix}$ ($c_{\ell j}$-mal), S_ℓ^j Matrix zu $\sigma_{\ell j}$, $\text{grad}\,\sigma_{\ell j} = f_{\ell j} \Rightarrow S_\ell^j \in \mathbb{C}^{f_{\ell j} \times f_{\ell j}}$, $d_\ell = \sum c_{\ell j} f_{\ell j}$.

$A_{k\ell} = \begin{pmatrix} A_{k\ell}^{11} & \cdots & A_{k\ell}^{1 s_\ell} \\ \vdots & & \\ A_{k\ell}^{s_k 1} & \cdots & A_{k\ell}^{s_k s_\ell} \end{pmatrix}$, $\underbrace{\begin{pmatrix} S_k^j & & 0 \\ & \ddots & \\ 0 & & S_k^j \end{pmatrix}}_{c_{kj}} A_{k\ell}^{ji} = A_{k\ell}^{ji} \underbrace{\begin{pmatrix} S_\ell^i & & 0 \\ & \ddots & \\ 0 & & S_\ell^i \end{pmatrix}}_{c_{\ell i}}$. Schur's Lemma $\Rightarrow A_{k\ell}^{ji} = 0$, $k \neq \ell$, weil $\sigma_k^j, \sigma_\ell^i$ irred. und inäquivalent. $\Rightarrow$ a)

b) $\rho_\ell = c_\ell \sigma_\ell$. $V_\ell = V_\ell^1 \oplus \ldots \oplus V_\ell^{c_\ell}$, $\dim V_\ell^j = \text{Grad}\,\sigma_\ell = f_\ell$, $d_\ell = c_\ell \cdot f_\ell$.

$\Rightarrow R_\ell^{(s)} = \underbrace{\begin{pmatrix} S_\ell & & 0 \\ & \ddots & \\ 0 & & S_\ell \end{pmatrix}}_{c_\ell \text{ mal}}$, $S_\ell \in \mathbb{C}^{f_\ell \times f_\ell}$.

(*) für $k = \ell$: $S_\ell^{(s)} A_{\ell\ell}^{ji} = A_{\ell\ell}^{ji} S_\ell(s)$ $\forall s \in G$.

Satz 11.1 $\Rightarrow A_{\ell\ell}^{ji} = \alpha_{ji,\ell} I_\ell$, I_ℓ: $f_\ell \times f_\ell$ - Einheitsmatrix. Vgl (3 4 !!!)

$\Rightarrow A_{\ell\ell} = \begin{pmatrix} \alpha_{11,\ell} I_\ell & \ldots & \alpha_{1c_\ell,\ell} I_\ell \\ \vdots & & \vdots \\ \alpha_{c_\ell 1,\ell} I_\ell & \ldots & \alpha_{c_\ell c_\ell,\ell} I_\ell \end{pmatrix}$ bzgl. folgender Basis: $V_\ell^1 : v_{\ell,1}^1 \ldots v_{\ell,f_\ell}^1 \ldots V_\ell^{c_\ell} : v_{\ell,1}^{c_\ell} \ldots v_{\ell,f_\ell}^{c_\ell}$.

zeilenweise Anordnung. σ_ℓ hat bzgl. dieser Basen in V_ℓ^j dieselbe Darstellung S_ℓ.

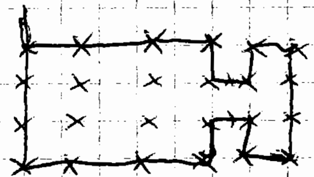
Umordnung: Spaltenweise Anordnung. $v_{\ell 1}^1, v_{\ell 1}^2 \ldots v_{\ell 1}^{c_\ell}, v_{\ell 2}^1, v_{\ell 2}^2 \ldots v_{\ell 2}^{c_\ell}$ usw.

$\Rightarrow A_{\ell\ell} = \underbrace{\begin{pmatrix} B_\ell & & 0 \\ & \ddots & \\ 0 & & B_\ell \end{pmatrix}}_{f_\ell}$, $B_\ell \in \mathbb{C}^{c_\ell \times c_\ell}$. Beisp.: $c_\ell = 3$, $f_\ell = 2$.

$$\begin{pmatrix} \alpha_{11} & 0 & \alpha_{12} & 0 & \alpha_{13} & 0 \\ 0 & \alpha_{11} & 0 & \alpha_{12} & 0 & \alpha_{13} \\ \alpha_{21} & 0 & \alpha_{22} & 0 & \alpha_{23} & 0 \\ 0 & \alpha_{21} & 0 & \alpha_{22} & 0 & \alpha_{23} \\ \alpha_{31} & 0 & \alpha_{32} & 0 & \alpha_{33} & 0 \\ 0 & \alpha_{31} & 0 & \alpha_{32} & 0 & \alpha_{33} \end{pmatrix} \to \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & & 0 & \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & & & \\ \alpha_{31} & \alpha_{32} & \alpha_{33} & & & \\ & & & \alpha_{11} & \alpha_{12} & \alpha_{13} \\ & 0 & & \alpha_{21} & \alpha_{22} & \alpha_{23} \\ & & & \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix}$$

$\square$ (?)

Beisp. zu Satz 12.1 (a)

1)  $G=\{1,-1\}$, $\rho(1)=I_{26\times 26}$, $\rho(-1)=P=\begin{pmatrix}0 & Q^t\\ \underset{\uparrow}{Q} & 0\end{pmatrix}$

Permutation

Irr. Darstellungen von G: $\rho_1(\pm 1)=1$, $\rho_2(\pm1)=\pm 1$ ist Liste der irred. Darst.

Ausreduktion: $\rho=c_1\rho_1+c_2\rho_2$; $c_j=(z,z_j)$, z = Char. von ρ, z_j = Char. von ρ_j.

$=\frac{1}{2}\{z(1)\cdot z_j(1)+z(-1)\cdot z_j(-1)\}=\frac{n}{2}$

$\Rightarrow \rho=\frac{n}{2}\rho_1+\frac{n}{2}\rho_2$. $\underset{PV_1=V_1}{V_1=(I+P)C^n}$. $\underset{PV_2=-V_2}{V_2=(I-P)C^n}$.

Spalten

Basis in V_1: $\begin{pmatrix}I\\Q\end{pmatrix}$. Die weiteren Spalten von $I+P$ sind $\begin{pmatrix}Q^t\\I\end{pmatrix}=\begin{pmatrix}I\\Q\end{pmatrix}Q^t$.

in V_2: $\begin{pmatrix}I\\-Q\end{pmatrix}$, besser $\begin{pmatrix}Q^t\\-I\end{pmatrix}$. Basis von $V=C^n$: $\begin{pmatrix}I & Q^t\\Q & -I\end{pmatrix}$, $SS^t=2I$.

Spalten

Nach Satz 12.1: Bzgl. der Basis S nimmt A (= Matrix mit Symm. von ρ) die Form an: $\begin{pmatrix}A_1 & 0\\0 & A_2\end{pmatrix}$. $S^{-1}AS$

$\uparrow A=\begin{pmatrix}A_{11} & A_{12}\\A_{21} & A_{22}\end{pmatrix}$, $PA=AP$.

$\begin{pmatrix}0 & Q^t\\Q & 0\end{pmatrix}\begin{pmatrix}A_{11} & A_{12}\\A_{21} & A_{22}\end{pmatrix}=\begin{pmatrix}A_{11} & A_{12}\\A_{21} & A_{22}\end{pmatrix}\begin{pmatrix}0 & Q^t\\Q & 0\end{pmatrix}\Rightarrow\begin{pmatrix}Q^tA_{21} & Q^tA_{22}\\Q^tA_{11} & QA_{12}\end{pmatrix}=\begin{pmatrix}A_{12}Q & A_{11}Q^t\\A_{22}Q & A_{21}Q^t\end{pmatrix}$.

$Q^t=Q^t=Q^{-1}$. $S^{-1}AS=\frac{1}{2}\begin{pmatrix}I & Q^t\\Q & -I\end{pmatrix}\begin{pmatrix}A_{11} & A_{12}\\A_{21} & A_{22}\end{pmatrix}\begin{pmatrix}I & Q^t\\Q & -I\end{pmatrix}=\begin{pmatrix}A_{11}+A_{12}Q & 0\\0 & A_{22}-QA_{12}\end{pmatrix}$

$Ax=b\underset{x=Sy}{\Leftrightarrow}S^{-1}ASy=S^{-1}b=\frac{1}{2}Sb$. $(A_{11}+A_{12}Q)y_1=\frac{1}{2}(b_1+Q^tb_2)$

$(A_{22}-QA_{12})y_2=\frac{1}{2}(Qb_1-b_2)$

$\Rightarrow x_1=y_1+Q^ty_2$, $x_2=Qy_1-y_2$

2) $G=C_n$, $\rho=\rho_{reg}$, A = zykl. Faltung der Länge n.

Irred. Darst. von C_n: $\rho_e(a^k)=\omega_e^k$, ω_e = n-te Einheitswurzel, $w_e=e^{2\pi i l/n}$ z.B. $e=0,\dots,n-1$

$V_e=\mathrm{sp}\left\{\begin{pmatrix}1\\w_e\\ \vdots\\ w_e^{n-1}\end{pmatrix}\right\}$, $W_n=\begin{pmatrix}1 & 1 & \dots & 1\\ w_0 & w_1 & & w_{n-1}\\ \vdots & & & \vdots\\ w_0^{n-1} & w_1^{n-1} & \dots & w_{n-1}^{n-1}\end{pmatrix}$. $W_n^{-1}AW_n$ = Diagonalmatrix

Satz 12.1: $\underset{\substack{\uparrow\\ \text{Faktor}}}{c_n}\ \underset{\substack{\uparrow\\ \text{Fourier-transf.}}}{W_n^{-1}}AW_n=\begin{pmatrix}a_0 & & 0\\ & \ddots & \\ 0 & & a_{n-1}\end{pmatrix}$.

Beispiele: 3) wie in 2), $\sigma_j(a^k)=w_j^k$, $j=0,\dots,n-1$.

$z^n-1=\prod_{d|n}\Phi_d(z)$, Φ_d Kreisteilungspolynome, n habe Teiler $\underset{1}{d_1},\dots,\underset{n}{d_r}$.

$V^j=\mathrm{sp}\begin{pmatrix}1\\w_j\\ \vdots\\ w_j^{n-1}\end{pmatrix}$. $V_e:=\bigoplus_{\substack{j\\ \Phi_{d_e}(w_j)=0}}V_j$. Sei W_{ne} Basis von V_e. V_e hat gauss. Basis

$\Phi_{d_e}(z)=p_0+p_1z+\dots+p_{c_e}z^{c_e}$, $c_e=\deg\Phi_{d_e}=\varphi(d_e)$.

Spalte von W_{ne}: $1\ \omega_j\dots w_j^{c_e}w_j^{c_e+1}\dots w_j^{(n-1)}$. $0=\Phi_{d_e}(\omega_j)=\sum_{i=0}^{c_e}p_iw_j^i$.

$0=\omega_j\Phi_{d_e}(\omega_j)=\sum_{i=0}^{c_e}p_i\omega_j^{i+1}$

$0=\omega_j^{n-c_e-1}\Phi_{d_e}(\omega_j)=\sum_{i=0}^{c_e}p_iw_j^{i+n-1-c_e}$

$\Rightarrow$ Jede Spalte von W_{ue} erfüllt ein System von $(n - c_e)$ (i.u.) linearen Gleichungen mit ganzzahligen Koeffizienten.

$\Rightarrow sp\{W_{ue}\} = sp\{v_1 \ldots v_{c_e}\}$, v_j **ganzzahlig**.

$S = (W_{u1} \ldots W_{ur})$ ← ganze Basen! $\Rightarrow S^{-1} A S = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_r \end{pmatrix}$, $\dim A_e = c_e$, $c_e =$ Grad$(\Phi$

$n = 3, 4$: Aufg. 23, 22. $n = 6$: $x^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$

$V_1 = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$, $V_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \\ -1 \end{pmatrix}$, $V_3 = \begin{pmatrix} 1 \\ 0 \\ -1 \\ \\ -1 \end{pmatrix} \oplus \begin{pmatrix} -1 \\ 2 \\ -1 \\ -1 \\ 2 \\ -1 \end{pmatrix}$, $V_4 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \\ 0 & 2 \\ -1 & 1 \\ -1 & -1 \\ 0 & -2 \end{pmatrix}$.

$$\left.\begin{array}{l} n=3: x_0 + x_1 + x_2 = 0 \\ \quad x_1 + x_2 + x_3 = 0 \\ \quad\quad x_2 + x_3 + x_4 = 0 \\ \quad\quad\quad x_3 + x_4 + x_5 = 0 \\ \quad\quad\quad\quad x\cancel{\ldots} \end{array}\right\}$$ raten oder Ergänzen zu zyklischer Faltung!!!

$S = \begin{pmatrix} 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 0 & 2 & 1 & 1 \\ 1 & 1 & -1 & -1 & 0 & 2 \\ 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 2 & -1 & -1 \\ 1 & -1 & -1 & -1 & 0 & -2 \end{pmatrix}$, $S^t S = \begin{pmatrix} 6 & & & & & 0 \\ & 6 & & & & \\ & & 4 & & & \\ & & & 12 & & \\ & & & & 4 & \\ 0 & & & & & 12 \end{pmatrix} =: D \Rightarrow S^{-1} = D^{-1} S^t$.

$\underbrace{S^t A S}_{\text{ganzzahlig}} = \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & A_3 & \\ 0 & & & A_4 \end{pmatrix} \begin{array}{c} 1 \\ 1 \\ 2 \\ 2 \end{array}\Bigg\} 6$

Rechenaufwand für $Ax = b$:

6 Divisionen + 8 Multiplikationen.

Satz 12.1(b) $\rho = \sum c_\ell \sigma_\ell$, $\text{Grad}(\sigma_\ell) = f_\ell$, $A = \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_r \end{pmatrix}$, $A_\ell \in \mathbb{C}^{d_\ell \times d_\ell}$, $d_\ell = c_\ell f_\ell$,

$A_\ell = \underbrace{\begin{pmatrix} B_\ell & & 0 \\ & \ddots & \\ 0 & & B_\ell \end{pmatrix}}_{f_\ell}$, B_ℓ: $c_\ell \times c_\ell$.

Beispiel i) $\begin{smallmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{smallmatrix} \cong D_4$. Irr. Darst.:

	r^k	sr^k	Grad
ρ_1	1	1	1
ρ_2	1	-1	1
ρ_3	$(-1)^k$	$(-1)^k$	1
ρ_4	$(-1)^k$	$(-1)^{k+1}$	1
ρ_5	$\begin{pmatrix} i^k & 0 \\ 0 & (-i)^k \end{pmatrix}$	$\begin{pmatrix} 0 & (-i)^k \\ i^k & 0 \end{pmatrix}$	2

ρ_{nat} von D_4 in $\mathbb{C}^9$.

Ausreduktion von $\rho_{nat} = \sum_{\ell=1}^{5} c_\ell \rho_\ell$, $c_\ell = (\chi_{nat}, \chi_\ell)$. gruppenel.

	1	r	r^2	r^3	s	sr	sr^2	sr^3
χ_{nat}	9	1	1	1	3	3	3	3

$\underbrace{1\ 1\ 1}_{\text{Bei Rot. bleibt nur Mittelp. fest.}}$ Spiegel.

$c_1 = (\chi_{nat}, \chi_1) = \frac{1}{8} \sum \chi_{nat}(g_\ell)\chi_1(g_\ell)$

$= 3$, $c_3 = 1$, $c_4 = 1$, $c_2 = 0$, $c_5 = 2$.

$\begin{smallmatrix} \cdot & \cdot & \cdot \\ + & \cdot & + \\ - & - & - \end{smallmatrix} = \begin{smallmatrix} 0&0&0 \\ 1&0&1 \\ -1&0&-1 \end{smallmatrix}$, $\rho_5(g) = \mathrm{Id}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ im wesentlichen!

$V = V_1^1 + V_1^2 + V_1^3 + V_3^1 + V_4^1 + V_5^1 + V_5^2$

und / und

Matrize angewandt auf 1. Vektor von V_5^1 bringt dasselbe wie auf V_5^2!

$V_{1,1}^1$ $V_{1,1}^2$ $V_{1,1}^3$ $V_{3,1}^1$ $V_{4,1}^1$ $V_{5,1}^1$ $V_{5,2}^1$ $V_{5,1}^2$ $V_{5,2}^2$

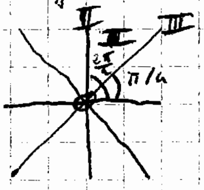
Anordnung der Basis nach 12.1(b): $V_{11}^1, V_{11}^2, V_{11}^3, V_{31}^1, V_{41}^1, V_{51}^1, V_{51}^2, V_{52}^1, V_{52}^2$

$S = \left(+ \,|\, \ldots \right) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 & \ldots \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $S^{-1} A S = \begin{pmatrix} A_1 & & & & \\ & A_2 & & & \\ & & A_3 & & \\ & & & B_5^1 & \\ & & & & B_5^2 \end{pmatrix}$

S sehr einfach!

Systematische Konstruktion von Basen:

Vorgabe: i) $G = D_n$, ii) endliche Punktmenge N in $\mathbb{R}^2$, invariant gegen D_n.



$n = 4$

3 Typen von Punkten:

0) Mittelpunkt, 1) außerhalb der Geraden

2) auf Gerade mit Winkel $\frac{2k\pi}{n}$, 3) auf Gerade mit Winkel $\frac{2k\pi+1}{n}$.

vom Typ 2), 3): $k \cdot n$ Punkte, $k \in \mathbb{N}$. vom Typ 1: $2kn$ Punkte.

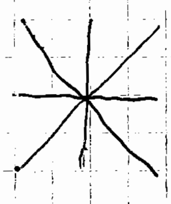
Orbit vom Typ 0: 1 oder keiner, Orbit 1: $2n$, Orbit 2,3: n Pkt.

Orbit = Menge der Punkte aus einem Punkt hervorgegangen durch Anwendung der Perm.

0 / I ρ_1

Numerierung innerhalb der Orbits im Uhrzeigersinn!

	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5^h $(\omega = e^{2h\pi i/n}$, $\alpha = e^{h\pi i/n})$			
0	1	0	0	0	0	0		
I	1	1	1	-1	1	1	-1	1
	1	-1	1	1	1	1	1	-1
	1	1	-1	1	ω	$\bar\omega$	$-\omega$	$\bar\omega$
	1	-1	-1	-1	ω	$\bar\omega$	ω	$-\bar\omega$
	1	1	1	-1	ω^2	$\bar\omega^2$	$-\omega^2$	$\bar\omega^2$
	1	-1	1	1	ω^2	$\bar\omega^2$	ω^2	$-\bar\omega^2$
	1	1	-1	1	ω^{n-1}	$\bar\omega^{n-1}$	$-\omega^{n-1}$	$\bar\omega^{n-1}$
	1	-1	-1	-1	ω^{n-1}	$\bar\omega^{n-1}$	ω^{3n-1}	$-\bar\omega^{n-1}$
II	1	0	0	1	1	1	0	0
	1	0	0	-1	ω	$\bar\omega$	0	0
	1	0	0	1	ω^2	$\bar\omega^2$	0	0
	1	0	0	-1	ω^{n-1}	$\bar\omega^{n-1}$	0	0
III	1		-1		α^{2n-1}	$\bar\alpha^{2n-1}$		
	1		1		α	$\bar\alpha$		
	1		-1		α^3	$\bar\alpha^3$		
	1		1		α^5	$\bar\alpha^5$		



0 : ∴ , I keine, II : $\overset{\rho_1}{+}$, $\overset{\rho_4}{+}$ …

V. Eff. Alg. in Computer-Tomographie

Lit.: Herman, Image Reconstruction from Projections, Academic Press 1980

Louis / Natterer: Math. Problems of CT, Proc. IEEE 71 3 79-399 (1983)

Shepp / Kruskal: CT, New Medical x-ray tech., Am. Math. Monthly 85 / 420-435, 197.

$C^\infty(\mathbb{R}^n)$

α Multiindex, $D^\alpha f = \frac{\partial^{|\alpha|}}{\partial^{\alpha_1} x_1 \cdots \partial^{\alpha_n} x_n} f(x)$, $x^\alpha = \prod x_i^{\alpha_i}$.

Schwartz'scher Raum $\mathcal{S}(\mathbb{R}^n) = \{ f \in C^\infty(\mathbb{R}^n) \mid \sup_{x \in \mathbb{R}^n} |x^\alpha D^\beta f(x)| < \infty \ \forall \alpha, \beta \}$

$C_0^\infty(\mathbb{R}^n) = \{ f \in C^\infty(\mathbb{R}^n) : f$ hat kp. Träger$\}$.

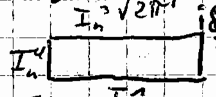
Beisp.: $e^{-|x|^2}$, $e^{-\frac{1}{1-|x|^2}}$.

Def. 13.1: $f \in L_1(\mathbb{R}^n) = \{ f \mid \int_{\mathbb{R}^n} |f| dx < \infty \}$. $\xi \in \mathbb{R}^n$

$$\hat f(\xi) = (2\pi)^{-n/2} \int_{\mathbb{R}^n} f(x) e^{-ix\xi} dx.$$

Beisp.: $n=1$, $f(x) = e^{-x^2} \Rightarrow \hat f(\xi) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-x^2} e^{-ix\xi} dx = \frac{1}{\sqrt{2\pi}} \int e^{-(x+\frac{i\xi}{2})^2} e^{-\frac{\xi^2}{4}} dx$

$= \frac{1}{\sqrt{2\pi}} e^{-\frac{\xi^2}{4}} \int_{-\infty}^{\infty} e^{-(x+i\frac{\xi}{2})^2} dx$



$I_n = I_n^1 + I_n^2 + I_n^3 + I_n^4$

$0 = \int_{I_n} e^{-z^2} dz$. $\left| \int_{I_n^2} e^{-z^2} dz \right| = \left| \int_0^{\xi/2} e^{-(n+i\tau)^2} d\tau \right| = e^{-n^2} \left| \int_0^{\xi/2} e^{-2in\tau} e^{\tau^2} d\tau \right| \leq e^{-n^2} \underbrace{\int_0^{\xi/2} e^{\tau^2} d\tau}_{k} \to 0$ $\quad n \to \infty$

$\Rightarrow \int_{I_n^2} e^{-z^2} dz \to 0$, $\int_{I_n^4} e^{-z^2} dz \to 0$ analog. $\Rightarrow 0 = \int_{-\infty}^{\infty} e^{-z^2} dz - \int_{-\infty}^{\infty} e^{-(i\xi/2+z)^2} dz$

$\Rightarrow \int_{-\infty}^{\infty} e^{-(z+i\xi/2)^2} dz = \int_{-\infty}^{\infty} e^{-z^2} dz \Rightarrow \hat f(\xi) = \frac{1}{\sqrt{2\pi}} e^{-\frac{\xi^2}{4}} \sqrt{\pi} = \frac{e^{-\frac{\xi^2}{4}}}{\sqrt{2}}$.

allgemein $f(x) = e^{-|x|^2} \Rightarrow \hat f(\xi) = 2^{-n/2} e^{-\frac{|\xi|^2}{4}}$.

Rechenregeln für die FT:

1) $f_\varepsilon(x) = f(\varepsilon x) \Rightarrow \hat f_\varepsilon(x) = \varepsilon^{-n} \hat f\left(\frac{\xi}{\varepsilon}\right)$, 2) $f_y(x) = f(x+y) \Rightarrow \hat f_y(\xi) = e^{iy\xi} \hat f(\xi)$.

3) $\int_{\mathbb{R}^n} f(x) \hat g(x) dx = \int_{\mathbb{R}^n} \hat f(\xi) g(\xi) d\xi$, 4) $(D^\alpha f)^\wedge(\xi) = i^{|\alpha|} \xi^\alpha \hat f(\xi)$.

5) $g(x) = x^\alpha f(x) \Rightarrow \hat g(\xi) = i^{|\alpha|} D^\alpha \hat f(\xi)$.

Satz 13.1: Fourier'scher Integralsatz: Die FT bildet $\mathcal{S}(\mathbb{R}^n)$ bijektiv auf sich ab, die Inverse ist gegeben durch $\check f(x) = (2\pi)^{-n/2} \int_{\mathbb{R}^n} f(\xi) e^{i\xi x} d\xi$.

Bew.: i) $\hat f(\xi) = (2\pi)^{-n/2} \int f(x) e^{-ix\xi} dx \in C^\infty(\mathbb{R}^n)$:

$g(x) := x^\beta f(x) \in \mathcal{S}(\mathbb{R}^n)$, $\left| \xi^\alpha D^\beta \hat f(\xi) \right| \underset{R.5}{=} \left| i^{|\beta|} \xi^\alpha \hat g(\xi) \right| \underset{R.4}{=} \left| (-i)^{|\beta|+|\alpha|} (D^\alpha g)^\wedge(\xi) \right|$

$= |(-i)^{|\alpha|+|\beta|}| \, 2\pi^{(-n/2)} \left| \int_{\mathbb{R}^n} D^\alpha g(x) e^{-ix\xi} dx \right| \leq 2\pi^{-n/2} \underbrace{\int_{\mathbb{R}^n} |D^\alpha g(x)| dx}_{= k}$

$\Rightarrow \hat f \in \mathcal{S}(\mathbb{R})$.

ii) $g, f \in \mathcal{S}(\mathbb{R}^n)$: $\int_{\mathbb{R}^n} g(\varepsilon \cdot \xi) \hat{f}(\xi) e^{iy\xi} d\xi \underset{R.1,2}{=} \int_{\mathbb{R}^n} g_\varepsilon(\xi) \hat{f}_y(\xi) d\xi \underset{R.3}{=} \int_{\mathbb{R}^n} \hat{g}_\varepsilon(\xi) f_y(\xi) d\xi$

$$= \varepsilon^{-n} \int_{\mathbb{R}^n} \hat{g}\left(\frac{\xi}{\varepsilon}\right) f_y(\xi) d\xi = \int_{\mathbb{R}^n} \hat{g}(z) f_y(\varepsilon \cdot z) dz$$

$$g(\xi) := e^{-|\xi|^2} \Rightarrow \int e^{-\varepsilon^2 |\xi|^2} \hat{f}(\xi) e^{iy\xi} d\xi = 2^{-\frac{n}{2}} \int_{\mathbb{R}^n} e^{-\frac{|z|^2}{4}} f(\varepsilon \cdot z + y) dz$$

$\varepsilon \to 0$:

$$\int_{\mathbb{R}^n} \hat{f}(\xi) e^{iy\xi} d\xi = f(y) \cdot 2^{-n/2} \int_{\mathbb{R}^n} e^{-\frac{|z^2|}{4}} \underset{z=2\xi}{=} 2^{n/2} f(y) \overbrace{\int_{\mathbb{R}^n} e^{-|\xi|^2} d\xi}^{\pi^{n/2}} = (2\pi)^{n/2} f(y) \square$$

Def.: f, g Fkt. in $\mathbb{R}^n$, eine in $\mathcal{S}(\mathbb{R}^n)$, die andere in $L_1(\mathbb{R}^n)$. $f * g(x) := \int_{\mathbb{R}^n} f(x-y) g(y) dy$

heißt Faltung von f, g. Rechenregeln: $f * g = g * f$, $(g * f) * h = g * (f * h)$.

Satz 13.2: Faltungssatz: f, g wie in 13.2. $(f * g)^\wedge = (2\pi)^{n/2} \hat{f} \cdot \hat{g}$, 2) $(f * g)^\sim = (2\pi)^{n/2} \tilde{f} \tilde{g}$,

3) $(f \cdot g)^\wedge = 2\pi^{-n/2} \hat{f} * \hat{g}$, 4) $(f \cdot g)^\sim = (2\pi^{-n/2}) \tilde{f} * \tilde{g}$.

Bew.: 1, 2: $\int_{\mathbb{R}^n} e^{\pm i\xi x} \int_{\mathbb{R}^n} f(x-y) g(y) dy dx = (2\pi)^{-n/2} \underbrace{\int_{\mathbb{R}^n} g(y) e^{\pm i \xi y}}_{\hat{g}(\xi)} \underbrace{\int_{\mathbb{R}^n} f(x-y) e^{\pm i \xi (x-y)} dx}_{(2\pi)^{n/2} \hat{f}(\xi)} dy$

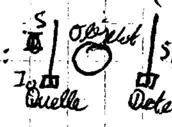
3: $(\hat{f} * \hat{g})^\sim \underset{2.}{=} (2\pi)^{n/2} f \cdot g \Rightarrow \hat{f} * \hat{g} = (2\pi)^{n/2} (f \cdot g)^\wedge$, 4 analog $\square$.

$S^{n-1} := \{\omega \in \mathbb{R}^n \mid |\omega| = 1\}$, $Z = \{(s, w) \mid s \in \mathbb{R}, w \in S^{n-1}\}$, Einheitszylinder im $\mathbb{R}^{n+1}$

$\int_{\mathbb{R}^n} f(x) dx = \int_0^\infty \int_{S^{n-1}} |\sigma|^{n-1} f(\sigma w) dw d\sigma$. $\mathcal{S}(Z)$ analog zu $\mathcal{S}(\mathbb{R}^n)$, Abl. in 1. Koordinate

Def. 13.3: $f \in \mathcal{S}(\mathbb{R}^n)$. Dann heißt die Abb. $R: \mathcal{S}(\mathbb{R}^n) \to \mathcal{S}(Z)$, $Rf(s, w) = \int_{x \cdot w = s} f(x) dx$,

$M := \{x \mid x \cdot w = s\} = (s \cdot w + w^\perp)$ (?). Beisp.: M ist senkrecht zu W, verschoben um s. $\langle s \cdot w + w^\perp, w \rangle = s \cdot 1 + 0 = s$

Prinzip der CT:  s, I Quelle, Detektor glm. bewegt.

$s \in [-1, 1]$. Intens. $= I_0$, gemessen $= I$. $f(x) =$ Absorptionskoeff. des Gew.

$$I = I_0 \cdot \exp\left(-\int_L f(x) dx\right) \Leftrightarrow -\log \frac{I}{I_0} = \int_L f(x) dx. \; g(s, w) = Rf(s, w) = \int_{x \cdot w = s} f(x) dx$$

Problem der CT: Löse die Integralgleichung.

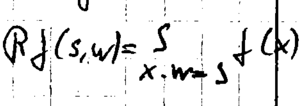
13.3 Projektionssatz, central slice theorem. $f \in \mathcal{S}(\mathbb{R}^n)$, $g = Rf \Rightarrow (2\pi)^{\frac{n-1}{2}} \hat{f}(\sigma \cdot w) = \hat{g}(\sigma, w)$.

Dabei ist $\hat{f}$ n-dim. FT von f, $\hat{g}$ ist 1-dim FT bzgl. 1. Var, $\hat{g}(\sigma, w) = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} g(s, w) e^{-is\sigma} ds$.

Bew.: $\hat{g}(\sigma, w) = (2\pi)^{-1/2} \int_{\mathbb{R}} g(s, w) e^{-is\sigma} ds$

$$= (2\pi)^{-1/2} \int_{\mathbb{R}} \int_{x \cdot w = s} f(x) e^{-is\sigma} dx ds = (2\pi)^{-\frac{1}{2}} \int_{\mathbb{R}^n} f(y) e^{-iy(\sigma w)} dy$$

$$= (2\pi)^{\frac{n-1}{2}} \hat{f}(\sigma \cdot w).$$



Daten gegeben $\forall s$ und $\omega_0 \Rightarrow \hat{g}(\sigma, \omega_0)$ gegeben $\forall \sigma$.

$w = \binom{\cos\varphi}{\sin\varphi}$, $w_0 = \binom{\cos\varphi_0}{\sin\varphi_0}$ $\Rightarrow \hat{f}(\sigma \cdot \omega_0)$ gegeben $\forall \sigma \Rightarrow \hat{f}$ gegeben auf Geraden durch Ursprung

Def. 13.4: $R^*: \mathcal{S}(Z) \to \mathcal{S}(\mathbb{R}^n)$, $(R^* g)(x) = \int_{S^{n-1}} g(x \cdot \omega, \omega) d\omega$ heißt Rückprojektion.

Bem. $n = 2$: $R^* g(x) = \int_0^{2\pi} g\left(x \binom{\cos\varphi}{\sin\varphi}, \binom{\cos\varphi}{\sin\varphi}\right) d\varphi$

Radon-Trafo: $Rf(s,w) = \int_{xw=s} f(x)\,dx$

CT: zu lösen $g(s,w) \overset{n=2}{=} Rf(s,w) = \int_{x\cdot w=s} f(x)\,dx$

Kernspin: $n=3$ ähnlich. Projektionssatz: $(2\pi)^{\frac{n-1}{2}} \underbrace{\hat f(\sigma w)}_{n\text{-dim}} = \underbrace{\hat g(\sigma, w)}_{1\text{-dim}}$

§14. Rekonstruktionsalgorithmen

$Z = \{(s,w),\ s\in\mathbb{R},\ w=(\cos\varphi,\sin\varphi)^t,\ \varphi\in[0,2\pi]\}$

$supp(f)\subset D=\{|x|\le 1\} \Rightarrow g(s,w)$ für $|s|>1$

Nur endlich viele Daten $g(s_i,w_j)$, $i=-q..q$, $j=0..p-1$
normal: $s_i=\frac{i}{q}$, $i=-q..q$, $\varphi_j = j\cdot\frac{\pi}{p}$, $j=0..p-1$

$g(s,w)=g(-s,-w)$, denn das bedeutet vertauschen von Quelle und Empf.!

$p=c\cdot q$, in unserem Fall $p=\pi q$.

a) Die Fourier Rek.; Lit.: F. Natterer, Fourier-Reconstr. in Tom., Num. Math. 47, 343-353 (1985)

Proj.: $(2\pi)^{1/2}\hat f(\sigma w) = \hat g(\sigma,w)$. Bekannt: $g(s,w) \xrightarrow[\text{Int.}]{\text{num.}} \hat g(\sigma,w) \xrightarrow[\text{Proj.}]{} \hat f(\sigma\cdot w) \xrightarrow[\text{Int.}]{\text{num.}} f(x)$

Gegeben: $g(\frac{i}{q}, w_j)$, $i=-q..q$. $k\in\mathbb{Z}$.

Trapezregel: $\hat g(k\pi, w_j) \approx \frac{1}{\sqrt{2\pi}}\frac{1}{q}\sum_{l=-q}^{q-1} g(s_l,w_j)\,e^{-2ik\pi l/2q}$

$$= \frac{1}{\sqrt{2\pi}}\cdot\frac{1}{q}\sum_{l=0}^{2q-1} g(s_{l-q},w_j)\,e^{-2\pi i kl/2q}\cdot(-1)^k$$

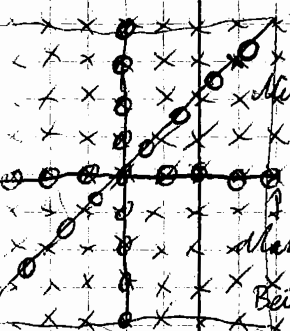
$$= (-1)^k\cdot\frac{1}{\sqrt{2\pi}}\cdot\frac{1}{q}\sum_{l=0}^{2q-1} g(s_{l-q},w_j)\,e^{-2\pi i kl/2q}.$$

FFT der Länge $2q$ liefert Appr. an $\hat g(k\pi, w_j)$, $k=0..2q-1$ oder auch $-q..q-1$, denn $e^{-2\pi i(k-2q)l/2q} = e^{-2\pi i kl/2q}$, also $\hat g((k-2q)\pi, w_j) = \hat g(k\pi, w_j)$

Anwendung von FFT-Techniken für Ber. von f aus $\hat f$:

$f(x_l) = \frac{1}{2\pi}\int_{\mathbb{R}}\int_{\mathbb{R}} \hat f(\xi)\,e^{i\xi x_l}\,d\xi$, $x_l = (\frac{l_1}{q},\frac{l_2}{q})$. $l_i=-q..q$

$$\approx \frac{1}{2\pi}\sum_{k_2=-q}^{q-1}\Big(\sum_{k_1=-q}^{q}\hat f(\xi_{k_1},\xi_{k_2})\,e^{i\xi_{k_1} l_1/q}\Big)e^{i\xi_{k_2}\frac{l_2}{q}}\cdot\Delta\xi_{k_1}\,\Delta\xi_{k_2}$$



Mit $\xi_{k_i}=k_i\pi$: $= \frac{1}{2\pi\,\pi^2}\sum_{k_2=-q}^{q-1}\Big(\sum_{k_1=-q}^{q-1}\hat f(k_1\pi,k_2\pi)\,e^{2\pi i k_1 l_1/2q}\Big)e^{2\pi i k_2 l_2/2q}$

$$= (-1)^{l_1+l_2}\cdot\frac{1}{2\pi\,\pi^2}\sum_{k_2=0}^{2q-1}\Big(\sum_{k_1=0}^{2q-1}\hat f((k_1-q)\pi,(k_2-q)\pi)\,e^{2\pi i k_1 l_1/2q}\Big)e^{2\pi i k_2 l_2/2q}$$

Man braucht also $\hat f(k_1\pi,k_2\pi)$. Proj.-satz $\Rightarrow \hat g(k\pi,w_j) = (2\pi)^{1/2}\hat f(k\pi w_j)$, $k=-q..q-1$.

Beisp.: $q=4$, $p=4$, o = bek., * = ges. ($\hat f$). Bekannt: $\hat f$ auf polarem Gitter, ges. auf kart. Gitter. Interpolation liefert also das Gewünschte.

Alg. I $j=0..p-1$: Ber. Appr. $\hat g_{j,k}$ an $\hat g(k\pi,w_j)$, $k=-q..q-1$ durch FFT.

Ber. $\hat f_{j,k}$ Approx an $\hat f(k\pi w_j)$ durch Projektionssatz.

II Interpoliere aus diesen Werten $\hat f_n$ an $\hat f(k_1\pi,k_2\pi)$, $k=k_1,k_2\in\mathbb{Z}^2$, $k_i=-q..q-1$

III Ber. Appr. f_l an $f(\frac{l}{q})$, $l=l_1,l_2$, $l_i=-q..q$ durch FFT

Rechenaufwand: I. p - FFT der Lg. $2q$ $(\mathcal{O}(p\cdot q\cdot\log q))$

II. „nearest neighbour", $\mathcal{O}(q^2)$, raffin. Meth.: $\mathcal{O}(q^2\log^2 p)$.

III $2\cdot q$ FFT der Lg. $2q$ $\mathcal{O}(q^2\log q)$. $p=\pi q$.

Rechenaufwand: $\mathcal{O}(q^2\log q)$, bzw. $\mathcal{O}(q^2\log^2 q)$.

b) Die gefilterte Rückprojektion: Ramachandran / Lakshminarayanan, Ramlau, Kala

Satz 14.1 (1. Radon'sche Inversionsformel)

$f\in\mathcal{S}(\mathbb{R}^n)$, $g=Rf$ und I^{n-1} Operator auf $\mathcal{S}(\mathbb{R})$ def. durch $(I^{n-1}h)^\wedge(\sigma)=|\sigma|^{n-1}\hat h(\sigma)$.

Dann gilt $f=\frac12(2\pi)^{1-n}R^*I^{n-1}g$.

Bew.: $f(x)=(2\pi)^{-n/2}\int_{\mathbb{R}^n}\hat f(\xi)e^{i\xi x}d\xi=(2\pi)^{-n/2}\int_0^\infty\int_{S^{n-1}}\sigma^{n-1}\hat f(\sigma\cdot\omega)e^{i\sigma\omega x}d\omega\, d\sigma$

$=\frac12(2\pi)^{-n/2}\left[\int_0^\infty\int_{S^{n-1}}\sigma^{n-1}\hat f(\sigma\omega)e^{i\sigma\omega x}d\omega\, d\sigma+\int_{-\infty}^0\int_{S^{n-1}}|\sigma|^{n-1}\hat f(\sigma\omega)e^{i\sigma\omega x}d\omega\, d\sigma\right]$

$=\frac12(2\pi)^{-n/2}\int_{\mathbb{R}}\int_{S^{n-1}}|\sigma|^{n-1}\hat f(\sigma\omega)e^{i\sigma\omega x}d\omega\, d\sigma$

$\underset{P.S.}{=}\frac12(2\pi)^{-n/2}(2\pi)^{\frac{1-n}{2}}\int_{S^{n-1}}\underbrace{\int_{\mathbb{R}}|\sigma|^{n-1}\hat g(\sigma,\omega)e^{i\sigma(\omega x)}d\sigma}_{=c\cdot I^{n-1}g(x\omega,\omega)}d\omega$

$=\frac12 2\pi^{1-n}(R^*I^{n-1}g)(x)$

$n=2$: $\omega=(\cos\varphi,\sin\varphi)$. $f(x)=\frac12\frac{1}{2\pi}\int_0^{2\pi}I^1g(x\cdot\omega,\omega)d\varphi=\frac12\cdot\frac{1}{2\pi}\int_0^{2\pi}\frac{1}{\sqrt{2\pi}}\int_{-\infty}^\infty|\sigma|\hat g(\sigma,\omega)e^{i\sigma x\omega}d\sigma\, d\varphi$

$=\frac12(2\pi)^{-3/2}\int_0^{2\pi}\int_{-\infty}^\infty|\sigma|\hat g(\sigma,\omega)e^{i\sigma x\omega}d\sigma\, d\varphi$. $g(-s,-\omega)=g(s,\omega)$

$\hat g(\sigma,-\omega)e^{-i\sigma x\omega}=(2\pi)^{-1/2}\int g(s,-\omega)e^{-is\sigma}ds\, e^{-i\sigma x\omega}=2\pi^{-1/2}\int g(-s,\omega)e^{-is\sigma}ds\, e^{-i\sigma x\omega}$

$=(2\pi)^{-1/2}\int g(t,\omega)e^{-it(-\sigma)}dt\, e^{-i\sigma x\omega}=\hat g(-\sigma,\omega)e^{-i\sigma x\omega}$

$(\cos(\varphi+\pi),\sin(\varphi+\pi))^t=-\omega\Rightarrow f(x)=(2\pi)^{-3/2}\cdot\frac12\left(\int_0^\pi\int_{\mathbb{R}}|\sigma|\hat g(\sigma,\omega)e^{-\sigma x\omega}d\sigma\, d\varphi+\int_0^\pi\int_{\mathbb{R}}|\sigma|\hat g(\sigma,\omega)e^{-i\sigma x\omega}d\sigma\, d\varphi\right)$

$f(x)=\int_0^\pi\int_{\mathbb{R}}|\sigma|\hat g(\sigma,\omega)e^{i\sigma x\omega}d\sigma\, d\varphi\cdot 2\pi^{-3/2}$

$f(x)=\frac{1}{2\pi}\int_0^\pi q(x\omega,\omega)d\varphi$, $\hat q(\sigma,\omega)=|\sigma|\hat g(\sigma,\omega)$. Im inneres Integral: tausche $(-\infty,\infty)$ gegen $(-b,b)$.

Allg.: Ber. $\int_{-\infty}^\infty F_b(\sigma)|\sigma|\hat g(\sigma,\omega)e^{i\sigma x\omega}d\sigma$, F_b Tiefpaß, d. h. $\hat F_b(\sigma)=0$ für $|\sigma|>b$

Berechne $f_F(x)=\frac{1}{2\pi}\int_0^\pi q_F(x\omega,\omega)$, $\hat q_F(\sigma,\omega)=F(\sigma)|\sigma|\hat g(\sigma,\omega)$

Faltungssatz: $q_F=(2\pi)^{-1/2}\gamma * g$, $\hat\gamma(\sigma)=F(\sigma)|\sigma|$. γ zu berechnen in Aufg.

Alg.: I. $j=0..p-1$, ber. $q_F(s_\ell,\omega_j)=2\pi^{-1/2}\sum_{k=-q}^{q}\gamma(s_\ell-s_k)g(s_k,\omega_j)$ $s_\ell=\frac{\ell}{q}$, $\ell=-q..q$, (evtl. FFT), $\omega_j=(\cos\varphi_j,\sin\varphi_j)$, $\varphi_j=j\cdot\frac{\pi}{p}$.

II $x_k=\frac{k}{q}$, $k=(k_1,k_2)\in\mathbb{Z}^2$, $k_i=-q..q$. Interp. $q_F(x_k\omega_j,\omega_j)$ in der 1. Var.

III Ber. Approx. f_k an $f_F(x_k)$ durch $f_k=\frac{1}{2\pi}\frac{\pi}{p}\sum_{j=0}^{p-1}q_F(x_k\omega_j,\omega_j)$ (Trapez)

Rechenaufwand I. $\mathcal{O}(pq^2)$ (FFT: $\mathcal{O}(pq\log q)$)

II. lineare Interpol.: $\mathcal{O}(pq^2)$, III $\mathcal{O}(pq^2)\to\mathcal{O}(q^3)$,

§ 14. Rekonstruktionsalg.

a) Fourier, b) gef. Rückproj., c) Der diskrete alg. Alg., F. N.: Efficient implementation of 'optimal' algorithms in CT, Math. Meth. in Appl. Sci. 2 (1980), 545–

F. N.: Einige Beiträge der Math zur CT, ZAMM 64 T252–T260, 1984

Idee: Arnold Lent, 1975. Alg. Algorithmen: diskretisiere die Integralgleichung, $\Rightarrow$ LGS, löse es. (z. B. ART: algebraic reconstruction technique). Überdecke das Einheitsquadrat mit quadr. Gitter. Ann.: f ist konstant auf jedem Quadr. (pixel = picture element) (256·256). Numeriere pixels $(1 .. n^2)$, Strahldurchgänge $(p\cdot(2q+1))$. a_{ij} := Länge des Schnittes des j. Strahls mit i-tem Pixel.

$g_j = \sum_{i=1}^{n^2} a_{ij} f_i$; $g = Af$, A ist $(p\cdot(2q+1), n^2)$ Matrix. (Praxis: $n = 256, p = 480, q = 128 \Rightarrow (122800, 65536)$

FH: Daten gehen hervor aus Streifenintegralen, d. h. $f_i = \tau_j \Delta f$, $p \cdot q$ Daten d

$$g_{ij} = \int_{-1}^{1} w_j(s)\, Rf(s, \theta_i)\, ds, \quad w_j(s) = \begin{cases} 1 & |s - s_j| \le d/2 \\ 0 & \text{sonst} \end{cases}$$
$i = 0..p-1, j = 1..q.$

$$\Rightarrow g_j = \int_{-1}^{1} w_j(s) \int_{-\sqrt{1-s^2}}^{\sqrt{1-s^2}} f(s\cdot\theta_i + t\cdot\theta_i^\perp)\, dt\, ds$$

$$\underset{x := s\theta_i + t\theta_i^\perp}{=} \int_D w_j(x\cdot\theta_i) f(x)\, dx.$$

$L_1(D) = \{ f \text{ auf } D \mid \int |f| dx < \infty \}$. $L_2(D) = \{ f \text{ auf } D \mid \int |f|^2 dx < \infty \}$, vollst., norm. VR

Norm def. durch $\langle f, g \rangle := \int_D f(x) \bar{g}(x)\, dx$. $\|f\|^2 = \int_D |f|^2 dx$.

$$\underset{\chi_{ij}(x) = w_j(x\cdot\theta_i)}{=} \langle \chi_{ij}, f \rangle_{L_2(D)}. \quad \chi_{ij}(x) = \begin{cases} 1 & x \in L_{ij} = \{x \in D \mid |x\cdot\theta_i - s_j| < \frac{d}{2}\} \\ 0 & \text{sonst} \end{cases}$$

$\Rightarrow$ System von Integralgleichungen. $g_{ij} = \langle \chi_{ij}, f \rangle = R_{ij} f$, $i = 0..p-1$, $j = 1..q$

$R_i := \begin{pmatrix} R_{i1} \\ \vdots \\ R_{iq} \end{pmatrix}$, $g_i = \begin{pmatrix} g_{i1} \\ \vdots \\ g_{iq} \end{pmatrix} \Rightarrow g_i = R_i f$, $i = 0..p-1$. $R := \begin{pmatrix} R_0 \\ \vdots \\ R_{p-1} \end{pmatrix}$, $g = \begin{pmatrix} g_0 \\ \vdots \\ g_{p-1} \end{pmatrix}$, $g = Rf$.

$R: L_2(D) \to \mathbb{R}^{pq}$, große Lösungsmenge. Gesucht: f_M: $Rf_M = g$, $Rf' = g \Rightarrow \|f'\| \ge \|f_0\|$.

Def $R^*: \mathbb{R}^{pq} \to L_2(D)$, $R^* h = \sum_{i,j} \chi_{ij}(x) h_{ij}$ (Adjungierte)

$f_M = R^*(RR^*)^{-1} g$. Bew.: i) $\langle Rf, g \rangle_{\mathbb{R}^{pq}} = \langle f, R^* g \rangle_{L_2(D)}$

$\| \sum_{i,j} \langle \chi_{ij}, f \rangle_{L_2(D)}\, g_{ij} = \langle \sum_{i,j} \chi_{ij} g_{ij}, f \rangle_{L_2(D)}$

ii) $Rf_M = (RR^*)(RR^*)^{-1} g = g$ ✓. Sei $Rf = g$. $\|f_M\|^2 = \langle f_M, f_M \rangle = \langle R^*(RR^*)^{-1} g, f_M \rangle_{L_2(D)}$

$= \langle (RR^*)^{-1} g, Rf_M \rangle_{\mathbb{R}^{pq}} = \langle (RR^*)^{-1} g, Rf \rangle_{\mathbb{R}^{pq}} = \langle R^*(RR^*)^{-1} g, f \rangle = \langle f_M, f \rangle$

$\Rightarrow \|f_M\|^2 = |\langle f_M, f \rangle| \underset{C-S}{\le} \|f_M\| \|f\| \Rightarrow$ Beh.

Die Tikhonov-Regularisierung

geg.: $Ax = b$ unterbestimmt, $(x = A^* z)$ $AA^* z = b$. (AA^*) ist pos. semi def.

Betr. $(AA^* + \gamma I) z = b$, $\gamma > 0$: verb. Kondition. Problem: finde γ.

$Rf = g$; $f_M = R^*(RR^*)^{-1} g$.

Alg.: 1. Ber. Lsg. h von $RR^{*+\gamma I} h = g$. $(h = R^{*-1} f_u)$, $RR^*: \mathbb{R}^{pq} \to \mathbb{R}^{qp}$ $\Rightarrow (pq, pq)$-Matrix.
2. Ber. $f_u = R^* h$

$$RR^* h = \begin{pmatrix} R_0 R^* h \\ \vdots \\ R_{p-1} R^* h \end{pmatrix}, \quad R_i R^* h = \begin{pmatrix} R_{i1} R^* h \\ \vdots \\ R_{iq} R^* h \end{pmatrix}, \quad R_{is} R^* h = \langle \mathcal{X}_{is}, R^* h \rangle_{L_2(D)}$$

$$= \langle \mathcal{X}_{is}, \sum_{l,k} \mathcal{X}_{l,k} h_{l,k} \rangle_{L^2(D)} = \sum_{l,k} \langle \mathcal{X}_{is}, \mathcal{X}_{lk} \rangle_{L_2(D)} h_{lk}$$

$RR^* =$

$$\begin{matrix} \langle \mathcal{X}_{0,1}, \mathcal{X}_{0,1} \rangle & \dots & \langle \mathcal{X}_{0,1}, \mathcal{X}_{(p-1)q} \rangle \\ \langle \mathcal{X}_{(p-1)q}, \mathcal{X}_{01} \rangle & \dots & \langle \mathcal{X}_{(p-1)q}, \mathcal{X}_{(p-1)q} \rangle \end{matrix}$$

Teile ein in Blöcke der Länge und Breite q.

$= (R_i R_s^*)_{i,s = 0..p-1}$, $R_s h = \sum_{l=1}^{q} \mathcal{X}_{sl} h_{sl}$.

Rot in $\mathbb{R}^2$: $U = \begin{pmatrix} \cos \Delta\varphi & \sin \Delta\varphi \\ -\sin \Delta\varphi & \cos \Delta\varphi \end{pmatrix}$, $U^t = U^{-1}$. $\mathcal{X}_{se}(x) = \omega_e(x \cdot \Theta_s) = \omega_e(x \cdot U^s \Theta_0)$

$= \omega_e((U^{-s} x) \Theta_0) = \mathcal{X}_{0e}(U^{-s} x)$

$$(R_i R_s^*)_{k,e} = \langle \mathcal{X}_{ik}, \mathcal{X}_{s,e} \rangle_{L^2} = \langle \mathcal{X}_{0k} \circ U^{-i}, \mathcal{X}_{0e} \circ U^{-s} \rangle_{L^2}$$

$$= \int_D \mathcal{X}_{0k}(U^{-i} x) \mathcal{X}_{0e}(U^{-s} x) dx \underset{x = U^i y}{=} \int_D \mathcal{X}_{0k}(y) \mathcal{X}_{0e}(U^{i-s}) y \, dy$$

$$= \langle \mathcal{X}_{0k}, \mathcal{X}_{0e} \circ U^{i-s} \rangle_{L^2}.$$

Also ist Block S_{is} von $R_i R_s^*$ nur abhängig von $i-s$!

$$(S_{-s})_{k,e} = \langle \mathcal{X}_{0k}, \mathcal{X}_{0e} \circ U^{s} \rangle_{L^2} = \langle \mathcal{X}_{0k} U^{-s}, \mathcal{X}_{0e} \rangle_{L^2} = (S_s)_{e,k}$$

$$RR^* + \gamma I = \begin{pmatrix} S_0 + \gamma I & S_1 & S_2 & \dots & S_{p-1} \\ S_{-1} & S_0 + \gamma I & S_1 & S_2 & \\ S_{-2} & S_{-1} & S_0 + \gamma I & S_1 & S_2 \dots \\ \vdots & & & & \\ S_{1-p} & & & & S_0 + \gamma I \end{pmatrix}$$ ist Block-Toeplitzmatrix.

verwende Alg. von Bitmead-Anderson 1. $(RR^* + \gamma I)^{-1} = L_1 V_1 + L_2 V_2$ $(O(pq^2 \log^2 p))$ Ops

2. $h = L_1 V_1 g + L_2 V_2 g$, 4 Faltungen, Länge p, Vektorenlänge q. $O(pq^2 + pq \log p)$

3. $f_u(\frac{k}{q}) = R^* h = \sum_{i,s} \mathcal{X}_{is}(\frac{k}{q}) h_{is} = \sum_{\frac{k}{q} \in \text{Streifen}} h_{is}$ $\quad O(p q^2)$

$\varphi_i = i \cdot \Delta\varphi$, $\Delta\varphi = \frac{2\pi}{p}$, $\Rightarrow U^p = I$.

$$\Rightarrow (S_{p-s})_{k,e} = \langle \mathcal{X}_{0k}, \mathcal{X}_{0e} \circ U^{s-p} \rangle_{L^2(D)} = \langle \mathcal{X}_{0k}, \mathcal{X}_{0e} \cdot U^s \rangle_{L_2(D)} = (S_{-s})_{k,e}$$

Damit is $RR^* + \gamma I$ (Block-) zykl. Faltung. (FFT anwenden)

$$(RR^* + \gamma I) h = g \to (\hat{S}_k + \gamma I) \hat{h}_k = \hat{g}_k, \; k = 0..p-1.$$

Alg.: I i) Ber. S_s, $\hat{S}_s$. ii) Ber. $(\hat{S}_s + \gamma I)^{-1}$, speichere. ~~III Ber.~~

II i) Ber. $\hat{g}_k$. ii) Ber. $\hat{h}_k = (\hat{S}_s + \gamma I)^{-1} \hat{g}_k$. iii) Ber. h durch inverse FT.

III Ber. $f_u(\frac{k}{q}) = \sum_{i,s} h_{is}$

Schritt I nur einmal!! Rechenaufwand (II+III):

II i) $O(p \cdot \log q \cdot q)$, ii) $p \cdot q^2$, iii) $O(p \cdot q \log q)$, III $O(pq^2)$.

Insges. $O(pq^2)$, $p = c \cdot q$: $O(cq^3)$. $(S_s)_{ke} = \langle \mathcal{X}_{0k}, \mathcal{X}_{0e} \circ U^s \rangle_{L^2} = \int_D \mathcal{X}_{0k} \mathcal{X}_{se} dx =$ Flächeninhalt von $D \cap L_{0k} \cap L_{se}$

4) Darstellung abelscher Gruppen: Sei G abelsch. $G = C_{n_1} \oplus \dots \oplus C_{n_r}$.

$\hat{G}$ ist Gruppe und isomorph zu G.

Satz 16.3: G abelsch, H Untergruppe, $\hat{L} = \{\rho \in \hat{G} : \rho(h) = 1, h \in H\}$. Dann gilt

(a) $\hat{H} \simeq \hat{G}/\hat{L}$. (b) $\hat{L} \cong (G/H)^\wedge$.

Bew.: (a) $\rho \Rightarrow \sigma = \mathrm{Rest}_H \rho = \rho|H$. $\hat{G} = \{\rho_1 \dots \rho_n\}$. $n = |G|$. $\sigma_1 = \sigma_2 \Leftrightarrow \rho_1 = \rho_2$ auf H

$\Leftrightarrow \rho_1 \rho_2^{-1} \in \hat{L} \Leftrightarrow \rho_1, \rho_2$ in gleicher Nebenklasse von $\hat{L}$ ($\Rightarrow$ auch: injektiv).

Abb ist Homomorphismus. zu zeigen: surjektiv. Es reicht zu zeigen,

$|\hat{H}| = |\hat{G}/\hat{L}|$. $|G| = n_1 \dots n_r$, $H = C_{m_1} \oplus \dots \oplus C_{m_r}$, $m_i | n_i$.

$|\hat{G}| = n_1 \dots n_r$, $|\hat{H}| = m_1 \dots m_r$, $|\hat{L}| = \frac{n_1}{m_1} \dots \frac{n_r}{m_r}$, $|\hat{G}/\hat{L}| = m_1 \dots m_r = |\hat{H}|$

(b) a) $\Rightarrow \hat{L} \cong \hat{G}/\hat{H} = (G/H)^\wedge$ Beweis?

Ordne $G, \hat{G}$ nach Nebenklassen. $G = \dot{\bigcup}_{i=1}^{k} s_i H$, $|H| = m$, $|G| = n \Rightarrow km = n$.

$= s_1 h_1 \dots s_1 h_m, s_2 h_1 \dots s_2 h_m \dots s_k h_1 \dots s_k h_m$.

$\hat{H} = \{\sigma_1 \dots \sigma_m\}$, $\hat{L} = \{\lambda_1 \dots \lambda_k\}$, $\lambda_i \in \hat{G}$.

$\hat{G}$: $\lambda_1\sigma_1 \dots \lambda_1\sigma_m, \lambda_2\sigma_1 \dots \lambda_2\sigma_m, \dots, \lambda_k\sigma_1 \dots \lambda_k\sigma_m$ (Produkt im Sinne von $\hat{G}$).

Satz 16.4: G abelsch, H Untergruppe von G, $\varepsilon(s) = \begin{pmatrix} \sigma_1(s) & & 0 \\ & \ddots & \\ 0 & & \sigma_m(s) \end{pmatrix}$, $s \in G$. Diagonal

$W_G = (W_{G/H} \otimes I_m) \begin{pmatrix} \varepsilon(s_1) & & 0 \\ & \ddots & \\ 0 & & \varepsilon(s_k) \end{pmatrix} (I_k \otimes W_H)$ ← Drehfaktoren

$\Gamma_{16.3}$ Bew.: G abelsch, $H \trianglelefteq G$. $\hat{L} = \{\rho : \rho(h) = 1 \, \forall h \in H \Rightarrow \hat{H} \simeq \hat{G}/\hat{L}$, $\hat{L} \simeq (G/H)^\wedge$

$G = C_{n_1} \oplus \dots C_{n_r}$, $n_i = p_i^{a_i}$. OE $r = 1$, $G = C_n$. $G = \{1, a \dots a^{n-1}\}$, $\hat{G} = \{\rho_0 \dots \rho_{n-1}\}$.

$\rho_s(a^{ke}) = \omega_n^{sk}$, $\omega_n = e^{2\pi i/n}$. $H = \{1, a^k \dots a^{k(m-1)}\}$. $\hat{H} \simeq C_m$. $\hat{H} = \{\sigma_0 \dots \sigma_{m-1}\}$, $\sigma_j(a^{ke}) = \omega_{m}^{je}$

$\hat{L} = \{\rho_1, \rho_m \dots \rho_{m(k-1)}\} \simeq C_k \Rightarrow \hat{H} \simeq C_m \simeq C_n/C_k \cong \hat{G}/\hat{L}$. (b) genauso. ⌟

Satz 16.4 G abelsch, H Untergruppe. $G = \bigcup s_i H$, $\hat{G} = \bigcup \lambda_i \hat{H}$, $\hat{L} = \{\lambda_1 \dots \lambda_k\}$, $H = \{h_1 \dots h_m\}$, $\hat{H} = \{\sigma_1 \dots \sigma_m\}$

Ordne $G, \hat{G}$ nach Nebenklassen, d.h. $G \overset{(*)}{=} s_1 h_1 \dots s_1 h_m, s_2 h_1 \dots s_2 h_m \dots s_k h_1 \dots s_k h_m$ $= g_1 \dots g_n$

$\hat{G} = \lambda_1\sigma_1 \dots \lambda_1\sigma_m, \lambda_2\sigma_1 \dots \lambda_2\sigma_m \dots \lambda_k\sigma_1 \dots \lambda_k\sigma_m \Rightarrow W_G = (W_{G/H} \otimes I_m) \begin{pmatrix} \varepsilon(s_1) & & \\ & \ddots & \\ & & \varepsilon(s_k) \end{pmatrix} (I_k \otimes W_H)$.
$= \rho_1 \dots \rho_n$

$$W_G = \begin{pmatrix} \rho_1(g_1) & \dots & \rho_1(g_n) \\ \vdots & & \vdots \\ \rho_n(g_1) & \dots & \rho_n(g_n) \end{pmatrix} \overset{(*)}{=} \begin{pmatrix} \rho_1(s_1h_1) \dots \rho_1(s_1h_m) \dots \rho_1(s_kh_1) \dots \rho_1(s_kh_m) \\ \vdots \\ \rho_n(s_1h_1) \dots \rho_n(s_1h_m) \dots \rho_n(s_kh_1) \dots \rho_n(s_kh_m) \end{pmatrix}$$

$\rho_m(h_m) = \lambda_k(h_m)\sigma_m(h_m) = \sigma_m(h_m)$, denn $\lambda | H = \mathrm{Id}$.

$D(s_k) = \begin{pmatrix} \rho_1(s) & & \\ & \ddots & \\ & & \rho_n(s) \end{pmatrix}$, $R = \begin{pmatrix} \rho_1(h_1) \dots \rho_1(h_m) \\ \vdots \\ \rho_n(h_1) \dots \rho_n(h_m) \end{pmatrix} =$ $\begin{pmatrix} D(s_1)R, \dots, D(s_k)R \end{pmatrix}$ $(**) \Rightarrow R = \begin{pmatrix} W_H \\ \vdots \\ W_H \end{pmatrix}$, $W_H = \begin{pmatrix} \sigma_1(h_1) & \dots & \sigma_1(h_m) \\ \sigma_m(h_1) & \dots & \sigma_m(h_m) \end{pmatrix}$.

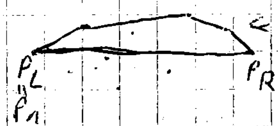
i schreitet P_{i+1} über e_1, e_2, wenn $i<n$ usw. bis n, liefert $O(\log n)$.

§18 Konvexe Hüllen.

$KH(S) = \bigcap_{\substack{k \text{ konvex} \\ S \subseteq k}} k$. Sei $|S| = n$.

Satz 18.1: Sei S die Menge der Ecken eines einfachen, d.h. doppelpunktfreien, Polygons. Dann kann man $KH(S)$ in $O(n)$ Ops berechnen.

Bew.: 1) Vereinfachung:



$\leftarrow$ oberer Teil der $KH(S)$; $S = P_1 .. P_n$

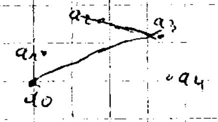
Programm zur Berechnung des oberen Teils von $KH(S)$

Stack: $q_0 .. q_t$ (op) Ausgangssituation: $q_0 .. q_t = P_R P_L$.

```
/* Suche ersten Punkt in oberer Hälfte */

s=2; push(pR); push(PL);
do while (ps unter L(pR,PL));
s=s+1;
end; push(ps);
/* q0,q1,q2 = PR, PL, PS */
```

C_t Kegel mit Spitze q_t berandet von den Strahlen $\overrightarrow{q_t, q_0}$; $\overrightarrow{q_{t-1}, q_t}$ — gerichtet!



$x \in C_t \Leftrightarrow x$ rechts von $L(q_t, q_0)$ und rechts oben auf $L(q_{t-1}, q_t)$

$O(n)$

```
Do while (s<n);
skip: s:=s+1; if ps ∈ Ct then goto skip;
Do while (qt-1, qt, ps) Linkskurve; pop(qt); end;
push(ps);
end;
```

gegen Uhrzeiger; $O(1)$ pro Lauf $+ O(n)$ insgesamt

s	$q_0 .. q_t$	Bemerkung
4	$P_R P_L P_4$	
5	$P_R P_L P_5$	
6	$P_R P_L P_5 P_6$	
7	$P_R P_L P_5 P_6$	$P_7 \in C_t$
8	$P_R P_L P_5 P_6 P_8$	
⋮		

Lemma: skip $\Rightarrow$ Es ist erfüllt:

(a) Stack $P_0 .. P_S$

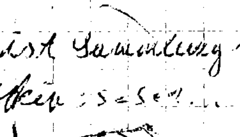
(b) $q_0 .. q_t$ konvexes Polygon

(c) Jede Ecke von $KH(S)$ ist in $q_0 .. q_t$, $p_{s+1} .. p_n$ enthalten.

(a) ✓

(b) $q_0 .. q_t$ ist Sammlung von Rechtskurven $\Rightarrow q_0 .. q_t$ konvex.

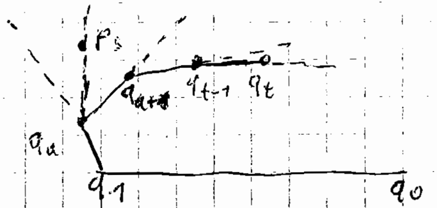
(c) 1. Bei skip: $s = s+1$ ... wird keine Ecke der oberen Hülle weggeworfen. Sonst:



P_s weggeworfen $\Rightarrow P_s \in C_t$. P_s kann nicht in (\\\) liegen

$\Rightarrow P_s$ in (|||) $\Rightarrow \overline{p_s q_t}$ schneidet $\overline{p_L q^t}$ Widerspruch, da Polygon einfach.

2. $pop(q_t)$ beseitigt keine Hüllenpunkte.
Annahme: $q_t .. q_{t-1}, q_{t+1}$ entfernt, q_t nicht.



p_s liegt oberhalb der - - -Geraden, insb. $L(q_a, q_{a+1})$; $q_{a+1} \dots q_t$ unterhalb $L(q_a, p_s)$, und damit ~~unterhalb~~ im Innern oder auf dem Rand von $q_0, q_1 \dots q_a\, p_s \dots p_n = q_0$. Also sind $q_{a+1} \dots q_t$ nicht Eckpunkte von $KH(S)$.

$a \geq 1$, dann $p_R p_s p_t$ Rechtskurve

Beweis der Richtigkeit: Abbruch mit $s = n$, weil p_n $(= q_0)$ nicht in C_t.

Stack nach Ablauf: $q_0 \dots q_t = p_n = q_0$ konvex

Satz 18.2: $|S| = n \Rightarrow KH(S)$ in $O(\log n \cdot n)$ Ops berechenbar.

Bew.: Ordne S lexikographisch nach x- bzw. y-Koordinate an. $O(n \log n)$ Zeit des Sortierens

Wende dann Satz 18.1 an. $O(n)$ KH (Polygonzug)

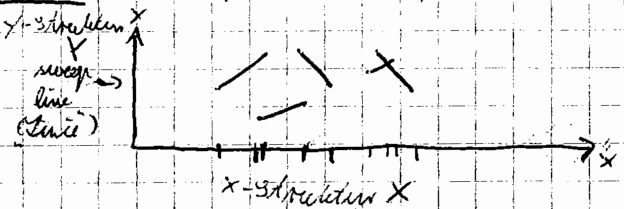
§ 19. Schnittprobleme

Seien n Strecken $L_1 \dots L_n$ gegeben. Gesucht sind alle Schnittpunkte.

Schulmeth.: $O(n^2)$. Das ist optimal für n^2 Schnittpunkte. Eff. Alg.: $s << n$ Schnittpunkte

Satz 19.1: Man kann die Schnittpunkte von n Strecken in $O((n+s) \log n)$ Operationen berechnen ($s = \#$Schnittpkte).

Beweis: Prinzip: linescan, linear scan, sweep line, plane sweep:



Die Y-Struktur besteht aus den Strecken L_i, welche mit der sweep line einen nichtleeren Durchschnitt haben. L_i links der Linie heißt tot, L_i rechts der Linie heißt schlafend.

Y geordnet: $L_i \leq L_j$, wenn dies für die Y-Koord. der Schnittpunkte mit der sweep line gilt.

Operationen auf Y, welche sich in $O(\log |Y|)$ Operationen ausführen lassen:

insert (L): ~~Addiere~~ füg ein Linie zur Y-Struktur, ordnungsgerecht.

delete (L): Entferne L aus Y.

pred (L): Vorgänger von L i. Sinne der Ordnung in Y.

succ (L): Nachfolger von L i. S. der Ordnung von Y.

interchange (L, L'): Vertausche L, L', wenn $L \geq L'$

Balancierter Baum.

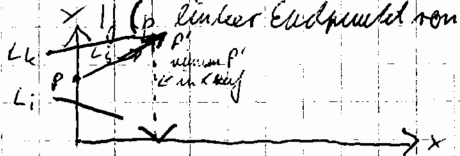
Zusatzvoraussetzungen: Keine zwei End- oder Schnittpunkte der $L_1 \dots L_n$ haben gleiche x-Koordinate.

Algorithmus, der Liste der Schnittpunkte druckt:

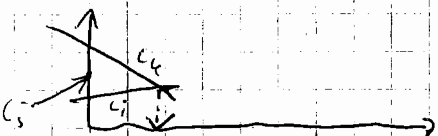
$Y = \emptyset$

$X = 2n$ Endpunkte von $L_1 \dots L_n$, geordnet nach ihrer X-Koordinate ($O(n \log n)$).

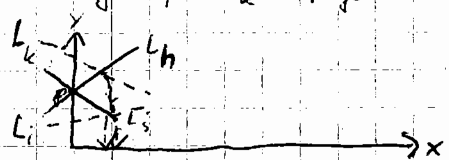
do While ($X \neq \emptyset$);
p = Min(X); /* p wird Position der sweep line */
X = X - {p};



If (p linker Endpunkt von L_j) then do;
insert (L_j);
L_i = pred(L_j); L_k = succ(L_j);
$X = X \cup (L_i \cap L_j) \cup (L_k \cap L_j)$;
End; **I**



If (p rechter Endpunkt von L_j) then do;
L_i = pred(L_j); L_k = succ(L_j); **II**
delete(L_j);
If (($L_i \cap L_k$) rechts von sweep line) Then $X = X \cup (L_i \cap L_k)$;
End;

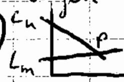


If ($\{p\} = L_k \cap L_i$ für ein (k, i)) then do;
interchange (L_k, L_j)
~~L_i = pred(L_h)~~ **III**
L_i = pred(L_k); L_k = succ(L_j);
If (($L_i \cap L_j$) rechts der Linie) Then $X = X \cup (L_i \cap L_j)$;
If (($L_k \cap L_H$) rechts der Linie) Then $X = X \cup (L_k \cap L_H)$; **IV**
put (p);
end;

end;

Lemma: X hat folgende Invarianzeigenschaften:

a) X enthält alle Endpunkte rechts der sweep line
b) X enthält zu je 2 benachbarten aktiven Strecken deren Schnittpunkt rechts der Linie
c) X enthält zu je 2 beliebigen aktiven Strecken deren Schnittpunkt rechts der Linie, falls zwischen diesem und der Linie kein weiterer End- oder Schnittpunkt liegt.

Beweis: a) ✓
b) Wegen I, II, III, IV: Jede Veränderung in X erfordert Hinzunahme des Nachbarschnittpkt. □
c)  Beh.: P ist dabei, wenn kein weiterer End- oder Schnittpunkt links von ihm liegt, denn: falls P nicht dabei, gibt es Schnitt- oder Endpunkte zwischen Linie und P.
Falls L_n, L_m nicht benachbart, gibt es eine Strecke dazwischen. Diese muß L_n, L_m links von P schneiden, oder dort enden □.

[Strassen / Karatsuba: schnelle Multiplikation
26.5.86 / kopieren!]

Schönhage - Strassen

VII Gewinnung eff. Alg.

§20. Divide & conquer versus plane sweep

Beisp.: Max. zushgd. Teilsummen, $a(1)..a(n) \in \mathbb{Z}$.

Gesucht: $\mathrm{Max}_{i \le j+1} \sum_{k=i}^{j} a(k) = S(1..n)$

1) Schulmeth.: $\Theta(n^3)$

2) Divide & conquer: Ber. $S(1..n/2), S(n/2..n), s_1 = \mathrm{Max}_{i \le \frac{n}{2}+1} \sum_{k=i}^{n/2} a(k), s_2 = \mathrm{Max}_{i \ge \frac{n}{2}} \sum_{k=n/2}^{i} a(k)$

$M(n) = 2M(n/2) + \Theta(n) = \Theta(n \log n)$

3) Plane sweep: $X = \{1..n\}$. $\forall i: \begin{cases} S(1..i) \\ s = \mathrm{Max}_{j \le i+1} \sum_{k=j}^{i} a(k) \end{cases}$

```
Init: S=0; s=0;
do i=1 to n;
  s = max{s+a(i), 0}
  S = max{S,s};
end;
```

§21. Dynamische Optimierung

Beispiel 1) Rundreiseproblem:

Geg.: n Städte, Kosten von i nach j sind $d(i,j) = d(j,i)$.

Ges.: Weg $i_1..i_n$: $d(i_1,i_2) + d(i_2,i_3) + \dots + d(i_n,i_1)$ minimal.

Schulmeth.: $\Theta((n+1)(n!))$. Dyn. Opt.:

$S \subseteq \{2..n\}$, 1 Ausgangspunkt. Sei $i \in S$.

$C(S,i)$ = Min. Kosten für Reise von 1 durch sämtliche Punkte von S nach i.

Bellmann'sche Gleichung: $C(S,i) = \mathrm{Min}_{k \in S \setminus \{i\}} \{ C(S - \{i\}, k) + d(k,i) \}$.

Satz 21.1 Das Rundreiseproblem kann in $\Theta(n^2 2^n)$ Operationen gelöst werden.

Bem.: $\frac{(n+1)!}{n^2 \cdot 2^n} \sim \frac{\sqrt{2\pi}\, n^{2n/2} e^{-n}}{n^2 \cdot 2^n} |_{n+1} = \frac{\sqrt{2\pi}\,(n+1)^{(n+3)/2} e^{-n-1}}{n^2 \cdot 2^n} = \frac{\sqrt{2\pi}}{e} \frac{(n+1)^{3/2}}{n^2} \left(\frac{n+1}{2e}\right)^n \to \infty$

Ber.: $C(S,i)$ für $|S| = 2,3..n-1$ $\forall i \in S$.

$|S| = 1$: $\Theta(1)$, $C(\{i\},i) = d(1,i)$. Sei nun $|S| = \ell$.

$\sum_{\ell=1}^{n-1} \binom{n-1}{\ell} \ell \cdot (\ell-1)$

#Mengen mit $|S|=\ell$ — # $i \in S$ — # k, die geprüft werden müssen

$\frac{\partial^2}{\partial x^2} \sum_{\ell=0}^{n} \binom{n}{\ell} x^\ell = (1+x^n)\frac{\partial^2}{\partial x^2}$

$\sum_{\ell=0}^{n} \binom{n}{\ell} \ell(\ell-1) x^{\ell-2} = n(n-1)(1+x)^{n-2}$

$= (n-1)(n-2)\, 2^{n-3}$

$= \Theta(n^2 \cdot 2^n)$

Lsg.: $\mathrm{Min}_i \{ C(\{2..n\}, i) + d(i,1) \}$ = Min. Kosten

Optimale Rundreise: Notiere die Stellen, an denen das Minimum jeweils ang. wird.

Satz 21.2: Es ist möglich, in $O(n^2)$ Operationen festzustellen, ob eine bestimmte Reise minimal ist - oder nicht.

Bew.: Prüfe Bellmann'sche Gleichung für $S_k = \{i_1 .. i_k\}$.

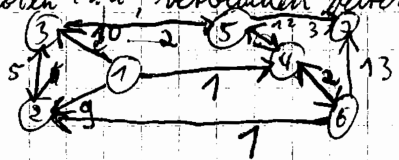
Folgerung: Rundreiseproblem $\in NP$, ~~Probleme~~ Lösungen sind vorgegeben in $O(\cancel{n})$ überprüfbar.

$P = \{$Klasse der Probleme, die in polynomialer Zeit lösbar sind$\}$.

$P = NP$?

2) Kürzeste Wege in Netzwerken.

Netzwerk = Knoten $1 .. n$, verbunden durch Pfeile.



A, E Mengen von Knoten. Finde billigsten Weg von A nach E.

1) Schulweg: $O(n!)$

2) Dyn. Opt.: $f(p)$ = Min. Kosten von p nach E. l_{pq} = Kosten von $p \to q$; 0 für $p = q$; ∞ falls kein Weg von p nach q.

Bellmann: $f(p) = \min_{q \neq p} \{ l_{pq} + f(q) \}$

Lösung durch Iteration: $f^{(k+1)}(p) = \min_{q \neq p} \{ l_{pq} + f^{(k)}(q) \}$, $f^{(1)}(p) = \min_{q \in E} l_{pq}$.

Satz 21.3: Es gebe einen kürzesten Weg von p nach q aus k Pfeilen. Dann ist für $l \geq k$: $f^{(l)}(p) = f^{(k)}(p) = f(p)$.

Bew.: $F^{(k)}(p)$ = Länge des kürzesten Weges von p nach E, der aus höchstens k Pfeilen besteht.

$F^{(1)}(p) = \min_{q \in E} l_{pq}$. $F^{(k+1)}(p) = \min_{q \neq p} \{ F^{(k)}(q) + l_{pq} \} \Rightarrow F^{(k)} = f^{(k)}$ (!).

Bem. 1) Ein min. Weg kann höchstens die Länge $(n-1)$ haben (klar), $l_{pq} \geq 0$.

$\Rightarrow$ Es reicht, $f^{(1)} .. f^{(n-1)}$ zu ber.

2) Sei $|A|, |E| = 1$. $f^{(k+1)}(p)$ aus $f^{(k)}$: $O(n)$; $f^{(k+1)}$ aus $f^{(k)}$: $O(n^2)$,

$\forall f^{(k)}$: $O(n^3)$.

3) Optimaler Weg: $f^{(n-1)}(p) = \min_{q \neq p} \{ f^{(n-2)}(q) + l_{pq} \}$, wird angenommen.

Notiere die Minima. Beisp.: $A = \{1\}$, $E = \{7\}$.

$p \backslash k$	1	2	3	4	5	6	q^*
1	∞	∞	15	15	15	14	4
2	∞	∞	10	10	10	10	3
3	∞	5	5	5	5	5	5
4	∞	15	15	15	13	13	6
5	3	3	3	3	3	3	7
6	13	13	13	11	11	11	2
(7)							

WS 85/86

Literatur zur Vorlesung:

"Effiziente Algorithmen"

1. H.J. Nussbaumer: "Fast Fourier Transform and Convolution Algorithms", 2. Auflage
   Springer-Verlag, 1982

2. T. Beth: Verfahren der schnellen Fourier-Transformation,
   Teubner Studienbücher, Informatik

3. K. Mehlhorn: "Effiziente Algorithmen", Teubner-Studienbücher

4. Aho/Hocroft/Ullman: "The Design and Analysis of Computer Algorithms"
   Addison-Wesley, 1974

5. Donald E. Knuth: "The Art of Computer Programming", Vol. 2,
   Addiscn-Wesley Publishing Company, 1969

vergleich mit $f*g=h$, $\hat f(\rho)\hat g(\rho)=n\hat h(\rho)$, $\rho\in\hat G$. $\hat g(\rho)=n(\hat f(\rho))^{-1}\hat h(\rho)$

Inversion von Matrizen der Dim. $d_1, d_2 \,..\, d_r$

§16. FFT auf abelschen Gruppen.

1) Tensorprodukte. Seien U, V VR endlicher dim. $U=sp\{u_1..u_p\}$, $V=sp\{v_1..v_q\}$.

$U\otimes V = sp\{u_i v_j : i=1..p, j=1..q\}$. dim $U\otimes V = pq$.

$W\in U\otimes V$. $w=\sum_{i,j=1}^{p,q} w_{ij}u_iv_j$. $w'=\sum w'_{ij}u_iv_j \Rightarrow w+w'=\sum(w_{ij}+w'_{ij})u_iv_j$. $\lambda w=\sum\lambda w_{ij}u_iv_j$

2) Tensorprodukt von lin. Abb. $\alpha: U\to U$, $\beta: V\to V$. $\alpha\times\beta: W\to W$; $W=U\times V$.

$\alpha\times\beta(u_kv_l)=\alpha(u_k)\beta(v_l)$ mit: $(\sum_k x_ku_k)(\sum_l y_lv_l)=\sum_{k,l}x_ky_l(u_kv_l)$

A Matrixdarstellung für α bzgl. $\{u_1..u_p\}$, B für β bzgl. $\{v_1..v_q\}$

$u=\sum_i x_iu_i$. $\alpha(u)=\sum_i(Ax)_iu_i$. $\alpha(u_k)=\sum_i a_{ik}u_i$, $A=(a_{ik})$.

$\alpha\otimes\beta(u_kv_l)=\sum_i a_{ik}u_i\cdot\sum_j b_{jl}v_l=\sum_i\sum_j a_{ik}b_{jl}u_iv_j$.

$w=\sum_{k,l}w_{kl}u_kv_l$. $\alpha\otimes\beta(w)=\sum_{k,l,i,j}a_{ik}b_{jl}w_{kl}u_iv_j=\sum a_{ki}b_{jl}w_{ij}u_kv_l$

Lexikographische Anordnung der Komponenten in W:

$$\begin{array}{c|ccc} & u_1v_j & \cdots & u_pv_j\\ \hline u_1v_l & a_{11}b_{lj} & \cdots & a_{1p}b_{lj}\\ \vdots & \vdots & & \\ u_pv_l & a_{p1}b_{lj} & & a_{pp}b_{lj}\end{array}\quad (l=1..q)\qquad A\otimes B=\begin{pmatrix}a_{11}B & \cdots & a_{1p}B\\ \vdots & & \vdots\\ a_{p1}B & \cdots & a_{pp}B\end{pmatrix}\Rightarrow Tr(\alpha\otimes\beta)=Tr(\alpha)\cdot Tr(\beta).$$

3) Darstellung der direkten Produkte von G.

Sei $G=A\odot B$. $|G|=n$, $|A|=p$, $|B|=q$, $n=pq$. $\hat A=\{\sigma_1..\sigma_r\}$, $\hat B=\{\tau_1..\tau_s\}$ Liste irred. Darst. von A, B

Satz 16.1: $\rho_{lk}(ab)=\sigma_l(a)\otimes\tau_k(b)$. ρ_{lk} sind irred., paarw. inäq. Darst. von G,

$\hat G=\{\rho_{lk}\}$. Bew.: (a) ρ_{lk} irred., d.h. $(\chi_{lk},\chi_{lk})=1$, $\chi_{lk}=Tr(\rho_{lk})$.

$(\chi_{lk},\chi_{lk})=\frac{1}{pq}\sum_{a\in A, b\in B}\chi_{lk}(ab)\overline{\chi_{lk}(ab)}=\sum Tr(\rho_{lk}(ab))\overline{Tr(\rho_{lk}(ab))}=\sum\varphi_l(a)\psi_k(b)\overline{\varphi_l(a)}\,\overline{\psi_k(b)}=1$ □

$\varphi_l=Tr(\sigma_l)$, $\psi_k=Tr(\tau_k)$ $(\sigma_l,\tau_k$ irred.$)$.

(b) ρ_{lk} paarw. inäq. (c) $\hat G=\{\rho_{lk}\}$. $\underbrace{\text{Grad}(\rho_{lk})}_{d_{lk}}=\underbrace{\text{Grad}(\sigma_l)}_{d_l}\underbrace{\text{Grad}(\tau_k)}_{c_k}$

$\sum_{l,k}d_{lk}^2=\sum_{l,k}d_l^2c_k^2=\underbrace{\sum_l d_l^2}_{p}\underbrace{\sum_k c_k^2}_{q}=pq=|G|\Rightarrow$ Beh. □

$\hat f(\rho)=\frac{1}{n}\sum_{t\in G}f(t)\rho(t)$. $W_G=\begin{pmatrix}\rho_1(g_1)&\cdots&\rho_1(g_n)\\ \vdots & & \vdots\\ \rho_m(g_1)&\cdots&\rho_m(g_n)\end{pmatrix}$ $G=\{g_1..g_n\}$. $\hat G=\{\rho_1..\rho_m\}$

Satz 16.2: $G=A\odot B$. Ordnet man G, $\hat G$ lexikographisch, d.h. $G=\{a_1b_1..a_1b_q, a_2b_1..a_pb_q\}$

$\hat G=\{\sigma_1\otimes\tau_1..\sigma_1\otimes\tau_s, \sigma_2\otimes\tau_1..\sigma_r\otimes\tau_s\}$ Dann gilt: $W_G=W_A\otimes W_B$. Produkt ist Tensorprod. lin. Abb.

$$W_G=\begin{pmatrix}\sigma_1(a_1)\otimes\tau_1(b_1) & \cdots\ \sigma_1(a_1)\otimes\tau_1(b_q) & \cdots\ \sigma_1(a_p)\otimes\tau_1(b_q)\\ \sigma_1(a_1)\otimes\tau_2(b_1) & \cdots\ \sigma_1(a_1)\otimes\tau_2(b_q) & \cdots\ \sigma_1(a_p)\otimes\tau_1(b_q)\\ \sigma_1(a_1)\otimes\tau_s(b_1) & \cdots\ \sigma_1(a_1)\otimes\tau_s(b_q) & \cdots\ \sigma_1(a_p)\otimes\tau_1(b_q)\\ \sigma_2(a_1) & & \\ \vdots & & \\ \sigma_r(a_1)\otimes\tau_1(b_1) & \cdots\ \sigma_r(a_1)\otimes\tau_1(b_q) & \\ \sigma_r(a_1)\otimes\tau_s(b_1) & \cdots\ \sigma_r(a_1)\otimes\tau_s(b_q) & \end{pmatrix}=\begin{pmatrix}\sigma_1(a_1)\otimes W_B & \sigma_1(a_2)\otimes W_B\\ \\ \sigma_r(a_1)\otimes W_B & \sigma_r(a_2)\otimes W_B\end{pmatrix}=W_A\otimes W_B$$

IV FT auf Gruppen. § 15 Einführung

G Gruppe, $|G| = n$, $\hat{G} = \{\rho_1 .. \rho_r\}$, ρ_i inaeq. irred. Darst. von G.

($\hat{G}$ heißt „Dual" von G für G abelsch)

Def 15.1: $f: G \to \mathbb{C}$. $\hat{f}(\rho) = \frac{1}{|G|}\sum_{t \in G} f(t)\rho(t)$: FT von F.

Beisp.: 1) $G = C_n$. $\rho_s(a^k) = \omega_n^{sk}$, $\omega_n = e^{2\pi i/n}$, $s = 0 .. n-1$, $G = \{1 .. a^{n-1}\}$

$\underbrace{\hat{f}(\rho_j)}_{\hat{f}_j} = \frac{1}{n}\sum_{k=0}^{n-1} \underbrace{f(a^k)}_{f_k}\omega_n^{jk}$

2) $G = C_{n_1} \otimes .. \otimes C_{n_p}$. Dir. Prod. $= \{a_1^{k_1} \cdots a_p^{k_p} : 0 \le k_i < n_i, i = 1 .. p\}$

Irred. Darst.: $\rho_{s_1} .. \rho_{s_p}(a_1^{k_1} \cdots a_p^{k_p}) = \omega_{n_1}^{s_1 k_1} \cdots \omega_{n_p}^{s_p k_p}$

$\hat{f}(\rho_{s_1} .. \rho_{s_p}) = \frac{1}{\prod n_i}\sum_{k_1=0}^{n_1-1} .. \sum_{k_p=0}^{n_p-1} f(a_1^{k_1} \cdots a_p^{k_p})\,\omega_{n_1}^{s_1 k_1} \cdots \omega_{n_p}^{s_p k_p}$; p-dim FT

3) Hadamard-Walsh-Trafo: $G = C_2 \otimes .. \otimes C_2$, p-mal

$\hat{f}_{s_1 .. s_p} = 2^{-p}\sum_{0 \le k_1 .. k_p \le 1} f_{k_1 .. k_p}(-1)^{\sum s_i k_i}$ (z.B. Pratt „Digital Image Processing")

4) $G = D_n$. $\hat{f}(\rho_j) = \frac{1}{2n}\sum_{k=0}^{n-1}\left(f(r^k)\rho_j(r^k) + f(sr^k)\rho_j(sr^k)\right)$

$\hat{f}(\rho_{s,h}) = \frac{1}{2n}\sum_{k=0}^{n-1}\left(f(r^k)\begin{pmatrix}\omega_n^{kh} & 0 \\ 0 & \omega_n^{-kh}\end{pmatrix} + f(sr^k)\begin{pmatrix}0 & \omega_n^{-kh} \\ \omega_n^{kh} & 0\end{pmatrix}\right)$

Bemerkung: $\hat{f}(\rho) = d_\rho \times d_\rho$-Matrix, $d_\rho = \deg\rho$, $\sum_{\rho \in \hat{G}} d_\rho^2 = n$. ($\hat{f}(\rho)$ hat „dim" n).

Def 15.2: $f, g: G \to \mathbb{C}$, $f * g(r) = \sum_{\substack{t \cdot s = r \\ t, s \in G}} f(t)g(s)$ $(r \in G) = \sum_{s \in G} f(rs^{-1})g(s)$

Satz 15.1: $(f * g)^\wedge(\rho) = n \cdot \hat{f}(\rho) \cdot \hat{g}(\rho)$

Bew.: $(f * g)^\wedge(\rho) = \frac{1}{n}\sum_{r \in G}(f * g)(r)\rho(r) = \frac{1}{n}\sum_{r \in G}\sum_{s \in G} f(rs^{-1})g(s)\rho(r)$

$\underset{rs^{-1} = t}{=} \frac{1}{n}\sum_{s \in G} g(s)\sum_{t \in G} f(t)\underbrace{\rho(t \cdot s)}_{\rho(t)\rho(s)}$

$= \sum_{s \in G} g(s)\,\hat{f}(\rho)\rho(s) = n \cdot \hat{f}(\rho) \cdot \frac{1}{n}\sum_{s \in G} g(s)\rho(s) = n\,\hat{f}(\rho)\hat{g}(\rho)$.

Satz 15.2: Die Fourier'sche Inversionsformel lautet $f(t) = \sum_{\rho \in \hat{G}} d_\rho \operatorname{tr}\left(\hat{f}(\rho)\rho(t^{-1})\right)$

Bew.: $\frac{1}{n}\sum_{\rho \in \hat{G}} d_\rho \operatorname{tr}(\hat{f}(\rho)\rho(t^{-1})) = \frac{1}{n}\sum_{\rho \in \hat{G}} d_\rho \operatorname{tr}\left(\sum_{r \in G} f(r)\underbrace{\rho(r)\rho(t^{-1})}_{\rho(rt^{-1})}\right)$

$\underset{rt^{-1} = s}{=} \frac{1}{n}\sum_{\rho \in \hat{G}} d_\rho \operatorname{tr}\sum_{s \in G} f(st)\rho(s) = \frac{1}{n}\sum_{s \in G} f(st)\underbrace{\sum_{\rho \in \hat{G}} d_\rho \operatorname{tr}\rho(s)}_{\operatorname{tr}(\rho_{reg}) = \chi_{reg}(s) = \delta_{s1} \cdot n}$

$= f(t)$

A (n,n)-Matrix, $a_{ki} = f(s_k s_i^{-1})$, $G = \{\overset{1}{s_1} .. s_n\}$, $f: G \to \mathbb{C}$.

$(Ax)_k = (f * g)(s_k)$, $x = \begin{pmatrix} g(s_1) \\ \vdots \\ g(s_n)\end{pmatrix}$

Satz 15.3: A ist Faltung auf $G \Leftrightarrow A$ hat Symmetrien der regulären Darstellung von G. (Beweis: ?)

Anwendung von 12.1 auf $Ax = b$: $S^t A S = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_r\end{pmatrix}$, $A_i \in d_e^2 \times d_e^2$, $A_i = \begin{pmatrix} B_i & & \\ & \ddots & \\ & & B_i\end{pmatrix}$, $B_i \in d_e \times d_e$, $\rho = \sum_{e=1}^{r} d_e \rho_e$, $\hat{G} = (\rho_1 .. \rho_r)$

$S^t A S x = b$: d_k Systeme der Dim. d_k mit identischer Matrix; $k = 1 .. r$