

## EXPLIZITE REKURSIONSFORMELN ZUR SCHNELLEN FOURIERTRANSFORMATION

VON

ULRICH OBERST

Einleitung: Die schnelle Fouriertransformation spielt in vielen Gebieten der angewandten Mathematik eine wichtige Rolle, wie man z.B. den im Literaturverzeichnis angegebenen Büchern entnimmt. Eine wesentliche Idee ist die Reduktion der Fouriertransformation einer Gruppe auf diejenige von Unter- und Faktorgruppen. In diesem Vortrag gebe ich explizite und leicht zu programmierende Rekursionsformeln im allgemeinen Fall einer kommutativen endlichen Gruppe an. Die Verallgemeinerung auf nicht kommutative Gruppen wie zum Beispiel bei Beth [3] ist möglich, muß aber im Detail noch ausgeführt werden.

Einführung in die diskrete Fouriertransformation: Die Fouriertransformation ist eine Abbildung

$$\text{Fourier: } K^G \longrightarrow K^G, a \mapsto \hat{a},$$

welche einer Funktion  $a:G \rightarrow K$  auf einer abelschen Gruppe  $G$  mit Werten in einem Koeffizientenbereich  $K$  eine Funktion  $\hat{a}$  auf der Charaktergruppe  $\hat{G}$  von  $G$  zuordnet.

In diesem Vortrag betrachte ich nur (im allgemeinen multiplikativ geschriebene) endliche abelsche Gruppen  $G$  vom vorgegebenen Exponenten  $d > 0$ , für die also

$$g^d = 1, \text{ d.h. } \text{Ordnung}(g) \mid d, \text{ für alle } g \in G$$

gilt. ( $a \mid b := a$  teilt  $b$ ). Jedes solche  $G$  ist bekanntlich isomorph zu einer additiven Gruppe

$$\mathbb{Z}/\mathbb{Z}d(1) \times \dots \times \mathbb{Z}/\mathbb{Z}d(r), 0 < d(i) \mid d, i=1, \dots, r. \quad (\mathbb{Z} = \text{ganze Zahlen})$$

Die  $d(i)$  sind die eindeutig bestimmten invarianten Faktoren von  $G$ , falls man zusätzlich  $d(1) \mid \dots \mid d(r)$  verlangt. Als Koeffizientenbereich sei ein kommutativer Ring  $K$  mit einer primitiven  $d$ -ten Einheitswurzel  $z$  gegeben. Nach Voraussetzung ist also  $z^d = 1$  und hat die von  $z$  erzeugte Gruppe  $\mu := \{1, \dots, z^{d-1}\}$  genau  $d$  Elemente, d.h. die Abbildung

$$\mathbb{Z}/\mathbb{Z}d \cong \mu, \bar{j} \mapsto z^{\bar{j}} := z^j,$$

ist ein Isomorphismus. Für jedes  $G$  (endlich, abelsch, vom Exponenten  $d$ ) gibt es und wähle ich eine nicht ausgeartete, symmetrische, bi-multiplikative Form  $\langle -, - \rangle_G : G \times G \rightarrow \mu$ . Daß die Form nicht ausgeartet ist, besagt, daß die Abbildung

$$(1) \quad G \cong \widehat{G} := \text{Gr}(G, \mu), g \mapsto \langle g, - \rangle_G,$$

von  $G$  in die Charaktergruppe  $\widehat{G}$  der Homomorphismen von  $G$  nach  $\mu$  ein Isomorphismus ist. Vermöge des Isomorphismus (1) identifiziere ich  $G = \widehat{G}$ , d.h.  $g = \langle g, - \rangle_G$ . Im folgenden tritt die Gruppe  $\widehat{G}$  daher nicht mehr explizit auf. Ist  $G$  die additive Gruppe

$$G = \mathbb{Z}/\mathbb{Z}d(1) \times \dots \times \mathbb{Z}/\mathbb{Z}d(r), 0 < d(i) \mid d, i=1, \dots, r,$$

so wähle ich für  $\langle -, - \rangle_G$  die Form

$$\langle -, - \rangle : G \times G \rightarrow \mu, \langle \bar{j}, \bar{k} \rangle := z^{\bar{j} \cdot \bar{k}}, \text{ mit}$$

$$\bar{j} = (\overline{j(1)}, \dots, \overline{j(r)}), \bar{k} = (\overline{k(1)}, \dots, \overline{k(r)}), \overline{j(i)}, \overline{k(i)} \in \mathbb{Z}/\mathbb{Z}d(i),$$

$$\bar{j} \cdot \bar{k} = (\sum \{ j(i)k(i)d/d(i); i=1, \dots, r \})^- \in \mathbb{Z}/\mathbb{Z}d$$

Im Fall  $G = \mathbb{Z}/\mathbb{Z}d$  hat man speziell  $\langle \bar{j}, \bar{k} \rangle = z^{jk}$ .

Zu jedem Gruppenhomomorphismus  $f: G \rightarrow H$  gibt es weiter einen eindeutig bestimmten adjungierten Homomorphismus  $f^*: G \leftarrow H$ , der wie üblich durch die Beziehung

$$\langle f(g), h \rangle_H = \langle g, f^*(h) \rangle_G, g \in G, h \in H,$$

definiert ist. Es ist  $f^{**} = f$ . Weiter ist eine Folge

$$G(1) \xrightarrow{f} G(2) \xrightarrow{g} G(3)$$

von Gruppen und Homomorphismen genau dann exakt, d.h. es gilt  $\text{Bild}(f) = \text{Kern}(g)$ , wenn die duale Folge

$$G(1) \xleftarrow{f^*} G(2) \xleftarrow{g^*} G(3)$$

exakt ist. Die Fouriertransformation ist definitionsgemäß die  $K$ -lineare Abbildung

$$(2) \quad \text{Fourier}_G : K^G \rightarrow K^G, a \mapsto \hat{a}, \hat{a}(\hat{g}) = \sum \{ a(g) \langle g, \hat{g} \rangle ; g \in G \}, \hat{g} \in G.$$

Die Fouriertransformation ist ein  $K$ -Algebrahomomorphismus, wenn man links auf  $K^G$  die Faltung und rechts die komponentenweise Multiplikation nimmt.

(3) Satz: (Fourierinversion) In obiger Situation sind folgende Aussagen äquivalent:

(i) Die Fouriertransformation  $\text{Fourier}_{\mathbb{Z}/\mathbb{Z}d}$  ist bijektiv.

(ii) Für jedes  $i=1, \dots, d-1$  ist  $z^i - 1$  in  $K$  invertierbar.



Mengenabbildungen mit  $\lambda(i) \varrho(i) = \text{Id}_{H(i)}$  usw. Wählt man beliebige unitäre Schnitte  $\varrho(i)$  von  $\mu(i), i=1, \dots, r$ , so sind die übrigen Schnitte eindeutig durch folgende Bedingungen gegeben:

(8) Alle Schnitte sind unitär, d.h. bilden 1 auf 1 ab.

(9)  $\varrho(i-1) \tau(i) = \varrho(i), \varrho(i-1) \gamma(i) = \alpha(i) \varrho(i)$ .

(10) Die  $\varrho(i)$  sind partiell multiplikativ, d.h. für  $k(i) \in K(i)$  und  $h(i) \in H(i)$  gilt  $\varrho(i-1) [\gamma(i)(k(i)) \cdot \tau(i)(k(i))] = \varrho(i-1) \gamma(i)(k(i)) \cdot \varrho(i-1) \tau(i)(h(i))$ .

(11) Satz: Sind Diagramme (6) mit den Bedingungen (7) bis (10) gegeben, so ist die Abbildung

$$\prod \{K(i); i=1, \dots, r\} \rightarrow G, k=(k(i); i=1, \dots, r) \mapsto \prod \{ \alpha(i) \varrho(i)(k(i)); i=1, \dots, r \}$$

bijektiv. ■

Analog zu und aus (6) erhält man durch Dualisieren die kommutativen Diagramme

(12)

$$\begin{array}{ccccccc}
 & & & & & & 1 \\
 & & & & & & \uparrow \\
 & & & & & & K(i) \\
 & & & & & & \uparrow \\
 & & & & & & \lambda(i-1)^* \\
 & & & & & & \leftarrow H(i-1) \leftarrow 1 \\
 & & & & & & \uparrow \gamma(i)^* \\
 & & & & & & \sigma(i) \\
 & & & & & & \uparrow \\
 & & & & & & 1 \\
 & & & & & & \uparrow \\
 & & & & & & v(i)^* \\
 & & & & & & \leftarrow H(i) \leftarrow 1 \\
 & & & & & & \uparrow \\
 & & & & & & 1 \\
 & & & & & & \uparrow \\
 & & & & & & K(i) \\
 & & & & & & \uparrow \\
 & & & & & & \mu(i)^* \\
 & & & & & & \leftarrow G(i) \leftarrow 1 \\
 & & & & & & \uparrow \beta(i)^* \\
 & & & & & & \hat{\sigma}(i) \\
 & & & & & & \uparrow \\
 & & & & & & 1 \\
 & & & & & & \uparrow \\
 & & & & & & \hat{\sigma}(i-1) \\
 & & & & & & \leftarrow G(i-1) \leftarrow 1 \\
 & & & & & & \uparrow \alpha(i-1)^* \\
 & & & & & & 1
 \end{array}$$

Die gestrichelten Schnitte erhält man aus frei gewählten unitären Schnitten  $\hat{\sigma}(i)$  wieder eindeutig unter folgenden zusätzlichen Bedingungen:

(13) Alle Schnitte in (12) sind unitär.

(14)  $\hat{\sigma}(i) \hat{\tau}(i) = \hat{\sigma}(i-1), \hat{\sigma}(i) \mu(i)^* = \lambda(i-1)^* \hat{\sigma}(i)$ .

(15)  $\hat{\sigma}(i)$  ist wieder partiell multiplikativ, d.h. es gilt für  $k(i) \in K(i), g(i-1) \in G(i-1)$

$$\begin{aligned}
 & \hat{\sigma}(i) [\mu(i)^*(k(i)) \cdot \hat{\tau}(i)(g(i-1))] = \\
 & = \hat{\sigma}(i) \mu(i)^*(k(i)) \cdot \hat{\sigma}(i) \hat{\tau}(i)(g(i-1)).
 \end{aligned}$$

## FOURIERTRANSFORMATION

Wieder gilt der

(16) Satz: Diagramme (6) und (12) mit den Nebenbedingungen (7) bis (15) seien gegeben. Dann ist die Abbildung

$$\prod \{ K(i); i=1, \dots, r \} \rightarrow G, (\hat{k}(1), \dots, \hat{k}(r)) \mapsto \prod \{ \lambda(j-1)^* \hat{\sigma}(j)(\hat{k}(j)); j=1, \dots, r \}$$

bijektiv. ■

Die schnelle Fouriertransformation: Die äquivalenten Bedingungen von Satz 3 seien erfüllt. Gegeben sei ferner eine Gruppe  $G$  mit den Diagrammen (6) und (12) und den Nebenbedingungen (7) bis (15). Das Ziel ist es, die Fouriertransformierte  $\hat{a} \in K^G$  zu  $a \in K^G$  schnell zu berechnen. Die Idee ist folgende: Man schreibt die in (2) auftretenden Elemente  $g, \hat{g} \in G$  nach (11) bzw. (16) eindeutig in der Gestalt

$$g = \prod \{ \alpha(i) \sigma(i)(k(i)); i=1, \dots, r \}, \hat{g} = \prod \{ \lambda(j-1)^* \hat{\sigma}(j)(\hat{k}(j)); j=1, \dots, r \}$$

mit Elementen  $k(i), \hat{k}(i) \in K(i)$ . Setzt man diese Ausdrücke in (2) ein, so folgt

$$\langle g, \hat{g} \rangle = \prod_{i,j} \langle \alpha(i) \sigma(i)(k(i)), \lambda(j-1)^* \hat{\sigma}(j)(\hat{k}(j)) \rangle.$$

Mit Hilfe der Nebenbedingungen (7) bis (15) werden die  $r^2$  rechts stehenden Faktoren vereinfacht. Insbesondere sind sie 1 für  $i < j$ .

(17) Satz ("decimation in time"): Seien  $a \in K^G$  und  $\hat{a} \in K^G$  die nach (2) definierte Fouriertransformierte von  $a$ . Induktiv nach  $\varrho = 0, \dots, r$  seien Funktionen

$$a_\varrho : K(1)^* \dots * K(r) \rightarrow K, (l(1), \dots, l(r)) \mapsto a_\varrho(l(1), \dots, l(r)),$$

definiert durch

$$a_0(l(1), \dots, l(r)) := a(\prod \{ \alpha(i) \sigma(i)(l(i)); i=1, \dots, r \}) \text{ und}$$

$$a_{\varrho+1}(l(1), \dots, l(r)) :=$$

$$\sum_k \{ a_\varrho(l(1), \dots, l(\varrho), k, l(\varrho+2), \dots, l(r)) \cdot f_{\varrho+1}(k; l(1), \dots, l(\varrho+1)); k \in K(\varrho+1) \}$$

mit den Faktoren

$$f_{\varrho+1}(k; l(1), \dots, l(\varrho+1)) =$$

$$= \langle k, l(\varrho+1) \rangle \cdot \prod_j \{ \langle \sigma(\varrho+1)(k), \hat{\tau}(\varrho+1) \dots \hat{\tau}(j+1) \mu(j)^*(l(j)) \rangle; j=1, \dots, \varrho \}$$

Dann ist

$$\widehat{a}(\prod \{ \lambda^{(j-1)*} \widehat{\sigma}^{(j)}(\widehat{k}^{(j)}); j=1, \dots, r \}) = a_r(\widehat{k}^{(1)}, \dots, \widehat{k}^{(r)}),$$

$$\widehat{k}^{(g)} \in K(g), g=1, \dots, r. \blacksquare$$

In der Situation des vorigen Satzes bezeichne  $e(i) := \#(K(i)), i=1, \dots, r$ , die Ordnung von  $K(i)$  und  $n = e(1) \dots e(r) = \#(G)$  diejenige von  $G$ . Die Komplexität, d.h. die Anzahl der in  $K$  notwendigen Multiplikationen, der Berechnung von  $\widehat{a}$  aus  $a$  nach (2) ist  $n^2$ , diejenige nach Satz 17 ist  $n(e(1) + \dots + e(r))$ . Das liefert die bekannte Komplexitätsverbesserung von  $n^2$  zu  $n \cdot \log(n)$ . Die Bezeichnung "decimation in time" (vergl. [10], Seite 87) ist sinnvoll, wenn man in der Systemtheorie  $G$  als (diskrete) Zeit und  $\widehat{G}$  (hier gleich  $G$ ) als Frequenz interpretiert. Analog zu Satz 17 erhält man den

(18) Satz ("decimation in frequency"): Sei  $b \in K^G$  mit der Fourier-transformierten  $\widehat{b} \in K^G$ . Man definiert rekursiv nach  $g = r, r-1, \dots, 0$ . Funktionen  $b_g : K(1) \times \dots \times K(r) \rightarrow K$  durch

$$b_r(\widehat{k}^{(1)}, \dots, \widehat{k}^{(r)}) := b(\prod \{ \lambda^{(j-1)*} \widehat{\sigma}^{(j)}(\widehat{k}^{(j)}); j=1, \dots, r \})$$

$$b_{g-1}(l(1), \dots, l(r)) :=$$

$$= \sum_{\widehat{k}} \{ b_g(l(1), \dots, l(g-1), \widehat{k}, l(g+1), \dots, l(r)) g_g(l(g), \dots, l(r); \widehat{k}); \widehat{k} \in K(g) \}$$

$$g_g(l(g), \dots, l(r); \widehat{k}) :=$$

$$= \langle l(g), \widehat{k} \rangle \cdot \prod_i \{ \langle \tau(g) \dots \tau(i-1) \gamma^{(i)}(l(i)), \widehat{\sigma}^{(g)}(\widehat{k}) \rangle; i=g+1, \dots, r \}$$

Dann gilt

$$\widehat{b}(\prod \{ \alpha^{(i)} \sigma^{(i)}(k^{(i)}); i=1, \dots, r \}) = b_0(k(1), \dots, k(r)). \blacksquare$$

Für den wichtigen Spezialfall der zyklischen Gruppe  $G = \mathbb{Z}/\mathbb{Z}d$  erhält man aus (17) und (18) folgende Resultate. Sei  $d = e(1) \dots e(r)$  eine Darstellung von  $d$  als Produkt. Für  $i=0, \dots, r$  seien  $d_1 = e(1) \dots e(i)$  und  $d_2(i) = e(i+1) \dots e(r)$ . Als Gruppen in (6) und (12) wählt man

$$G(i) = \mathbb{Z}/\mathbb{Z}d_1(i), H(i) = \mathbb{Z}/\mathbb{Z}d_2(i), K(i) = \mathbb{Z}/\mathbb{Z}e(i).$$

Als Abbildungen treten für  $m|n|d$  nur die Monomorphismen bzw. Epimorphismen bzw. Schritte der Typen

$$\text{inj: } \mathbb{Z}/\mathbb{Z}m \rightarrow \mathbb{Z}/\mathbb{Z}n, \text{ kan: } \mathbb{Z}/\mathbb{Z}n \rightarrow \mathbb{Z}/\mathbb{Z}m, \sigma: \mathbb{Z}/\mathbb{Z}m \rightarrow \mathbb{Z}/\mathbb{Z}n$$

$$\bar{k} \mapsto \overline{kn/m}, \quad \bar{k} \mapsto \bar{k}, \quad \bar{k} (0 \leq k < m) \mapsto \bar{k}$$

auf. Man identifiziert  $\{0, \dots, d-1\} = \mathbb{Z}/\mathbb{Z}d, k = \bar{k}$ .

## FOURIERTRANSFORMATION

(19) Satz: Voraussetzungen wie oben angegeben. Sei

$$a = (a(0) \dots a(d-1)) \in K^d = K^{\{0, \dots, d-1\}} = K^{Z/Zd}$$

eine Funktion und  $\hat{a} \in K^d$  die Fouriertransformierte, die nach (2) durch

$$\hat{a}(j) = \sum \{ a(i) z^{ij}; i=0, \dots, d-1 \}, 0 \leq j \leq d-1,$$

gegeben ist. Man definiert Funktionen

$$a_{\rho} : \prod_{i=1, \dots, r} \{ 0, \dots, e(i)-1 \} \rightarrow K, l = (l(1), \dots, l(r)) \mapsto a_{\rho}(l),$$

für  $\rho = 0, \dots, r$  induktiv durch

$$a_0(l(1), \dots, l(r)) = a(\sum \{ l(i) d_2(i); i=1, \dots, r \})$$

$$a_{\rho+1}(l(1), \dots, l(r)) =$$

$$\sum_k \{ a_{\rho}(l(1), \dots, l(\rho), k, l(\rho+2), \dots, l(r)) z^{\text{Exp}}; k=0, \dots, e(\rho+1)-1 \},$$

wobei der Exponent Exp durch

$$\text{Exp} = kd_2(\rho+1) \cdot \sum_j \{ l(j) d_1(j-1); j=1, \dots, \rho+1 \}$$

gegeben ist. Schreibt man  $i, 0 \leq i < d$ , eindeutig in der Gestalt

$$i = \sum \{ \hat{k}(j) d_1(j-1); j=1, \dots, r \}, 0 \leq \hat{k}(j) < e(j),$$

so gilt  $\hat{a}(i) = a_r(\hat{k}(1), \dots, \hat{k}(r))$ . ■

Im Spezialfall  $d=2^r, e(i)=2, i=1, \dots, r$ , erhält man daraus das bekannte Resultat von Cooley-Tukey (vergleiche [ 2 ], Algorithm 7.2). Aus Satz 18 folgt analog

(20) Satz: Sei  $\hat{b} \in K^d = K^{Z/Zd}$  die Fouriertransformierte von

$$b = (b(0) \dots b(d-1)) \in K^d = K^{\{0, \dots, d-1\}} = K^{Z/Zd}.$$

Definiere Funktionen

$$b_{\rho} : \{ 0, \dots, e(1)-1 \} \times \dots \times \{ 0, \dots, e(r)-1 \} \rightarrow K$$

rekursiv für  $\rho = r, r-1, \dots, 0$  durch

$$b_r(l(1), \dots, l(r)) = b(\sum_j \{ l(j) d_1(j-1); j=1, \dots, r \})$$

$$b_{\rho-1}(l(1), \dots, l(r)) :=$$

$$\sum_k \{ b_{\rho}(l(1), \dots, l(\rho-1), k, l(\rho+1), \dots, l(r)) z^{\text{Exp}}; k=0, \dots, e(\rho)-1 \}$$

mit  $\text{Exp} = kd_1(\rho-1) \cdot (\sum \{ l(i) d_2(i); i=\rho, \dots, r \})$ .

Für  $j, 0 \leq j \leq d-1$ , in der eindeutigen Darstellung

$$j = \sum_i \{ k(i) d_2(i); i=1, \dots, r \}, 0 \leq k(i) < e(i),$$

gilt dann

$$\hat{b}(j) = b_0(k(1), \dots, k(r)).$$
 ■

Verallgemeinerung: Schnelle Berechnung von Mehrfachsummen

Gegeben seien ein kommutativer Ring  $K$ , beliebige endliche Mengen

$(K(1), \dots, K(r))$  und Funktionen  $f_i, i=1, \dots, r$ ,

$$f_i : K(i) \times K(1) \times \dots \times K(i) \rightarrow K, (k(i), \hat{k}(1), \dots, \hat{k}(i)) \mapsto$$

$$\mapsto f_i(k(i); \hat{k}(1), \dots, \hat{k}(i))$$

U. OBERST

Mit Hilfe dieser Funktionen  $f_i$  definiert man den Operator (die Transformation)

$$(21) F: K^{K(1) \times \dots \times K(r)} \rightarrow K^{K(1) \times \dots \times K(r)}, a \rightarrow Fa, \text{ durch}$$

$$(Fa)(\hat{k}) = \sum_k \left\{ a(k) \prod_{i=1, \dots, r} [f_i(k(i); \hat{k}(1), \dots, \hat{k}(i)); i=1, \dots, r]; \right. \\ \left. k=(k(1), \dots, k(r)) \in K(1) \times \dots \times K(r) \right\}$$

(22) Satz: Die Transformation  $F$  von (21) ist genau dann bijektiv, wenn für alle  $\rho=1, \dots, r$  und  $l(1) \in K(1), \dots, l(\rho-1) \in K(\rho-1)$  als Parameter die Matrix

$A=(A(k, l); k, l \in K(\rho)), A(k, l) := f_\rho(k; l(1), \dots, l(\rho-1), l)$  invertierbar ist. Die Umkehrabbildung  $F^{-1}$  hat dann die gleiche Gestalt wie  $F$  mit anderen Koeffizienten. ■

(23) Satz (Schnelle Berechnung von  $F$ ) Daten wie oben angegeben. Zu einer Funktion  $a: K(1) \times \dots \times K(r) \rightarrow K$  definiert man induktiv für  $\rho=0, \dots, r$  ebensolche Funktionen  $a_\rho$  durch die Bedingungen

$$a_0 := a, a_{\rho+1}(l(1), \dots, l(r)) := \\ = \sum_k \left\{ a_\rho(l(1), \dots, l(\rho), k, l(\rho+2), \dots, l(r)) f_{\rho+1}(k; l(1), \dots, l(\rho+1)); \right. \\ \left. k \in K(\rho+1) \right\}$$

Dann ist  $Fa = a_r$ .

Literaturverzeichnis

1. Achilles, Die Fouriertransformation in der Signalverarbeitung, Springer 1978 (Kapitel 4,5)
2. Aho-Hopcroft-Ullmann, The design and analysis of computer algorithms, Addison-Wesley 1974 (Kapitel 7)
3. Beth, Verfahren der schnellen Fouriertransformation, Teubner 1984
4. Blahut, Theory and practice of error control codes, Addison-Wesley 1983 (Kapitel 11)
5. Brigham, The fast Fourier transform, Prentice-Hall 1974
6. Elliot-Rao, Fast transforms. Algorithms, Analyses, Applications. Academic Press 1982
7. Gold-Rader, Digital processing of signals, Krieger Publishing Company, Malabar, Florida 1983 (Kap. 6,7).
8. Lifermann, Les méthodes rapides de transformation du signal, Masson 1980
9. Mac Williams-Sloane, The theory of error-correcting codes, North-Holland 1983 (Seite 422)
10. Nussbaumer, Fast Fourier transform and convolution algorithms, Springer 1981.