離散 Fourier 変換

梅谷 武

作成：2000-08-14 更新：2005-04-20

離散 Fourier 変換の概念を可換環 R 上へ一般化し、複素数上や整数の剰余環上の離散 Fourier 変換の性質や高速算法の議論を統一的に行なえるようにすることを目的とする。最初に離散 Fourier 変換を可換環 R 上で定義し、その諸性質を整理する。その上で高速算法について論ずる。
IMS:20000814001; NDC:413.66; keywords:Fourier 展開,Fourier 変換, 畳み込み, 群環;

目　　次

1　離散 Fourier 変換

1.1　離散 Fourier 変換の定義

可換環 R 上で離散 Fourier 変換を定義するには次の条件が必要である。

条件 1.1 (離散 Fourier 変換を定義するための必要条件) R を可換環とする。

1. $\exists n$: 自然数, $\exists \zeta \in R : \zeta$は 1 の原始 n 乗根 $(i.e. \zeta^n = 1, n > k > 0 \to \zeta^k \neq 1)$
2. $\exists n^{-1} \in R (i.e. n$ を R の元とみなしたときにその逆元が存在する)
3. $n > k > 0 \to \sum_{i=0}^{n-1} \zeta^{ik} = 0$

上の条件の下で、ζ によって生成される巡回群を $G = \{1, \zeta, \cdots, \zeta_{n-1}\}$ とする。G から R への関数全体の集合を $C(G) = \{f : G \to R\}$ とすると、$C(G)$ には R から自然に加法と乗法が定義され、それによって可換環となる。さらにスカラー倍を自然に定義することによって R 上の多元環となる。

定義 1.2 (C(G) 上の双線形形式 (,)) $C(G)$ 上の双線形形式 $(,) : C(G) \times C(G) \to R$ を次のように定義する。

$$(f, g) = n^{-1} \sum_{i=0}^{n-1} f(\zeta^i) g(\zeta^{-i}), \ \ f, g \in C(G)$$

上の定義で $\zeta^{-i} = \zeta^{n-i}$ であることに注意せよ。これが R 上の双線形形式になることは明らかなので証明は略す。次の定理は、$C(G)$ がこの双線形形式について直交な基底をもつことを示す。

定理 1.3 (C(G) 上の標準直交基底とその Fourier 展開) $k = 0, \cdots, n-1$ について $e_k(\zeta^i) = \zeta^{ik}$ によって $e_k : C(G) \to R$ を定義すると $\{e_k : k = 0, \cdots, n-1\}$ は $C(G)$ の直交基底となる。すなわち、任意の $f \in C(G)$ は、

$$f = \sum_{i=0}^{n-1} (f, e_i) e_i$$

と一意的に表現することができる。これを f の *Fourier* 展開と呼ぶ。

証明

$$\begin{aligned}(e_k, e_l) &= n^{-1} \sum_{i=0}^{n-1} \zeta^{ik} \zeta^{-il} \\ &= n^{-1} \sum_{i=0}^{n-1} \zeta^{i(k-l)}\end{aligned}$$

ここで、条件 *3.* を使うと

$$\begin{aligned}(e_k, e_l) &= 0, \ k \neq l \\ (e_k, e_l) &= 1, \ k = l\end{aligned}$$

となり、$\{e_k : k = 0, \cdots, n-1\}$ が互いに直交していることがわかる。$\sum_{i=0}^{n-1} \lambda_i e_i = 0$ と仮定すると、$k = 0, \cdots, n-1$ に対して

$$\begin{aligned}\lambda_k &= \sum_{i=0}^{n-1} \lambda_i (e_i, e_k) \\ &= (\sum_{i=0}^{n-1} \lambda_i e_i, e_k) \\ &= 0\end{aligned}$$

となるから、$\{e_k : k = 0, \cdots, n-1\}$ は線形独立である。$f \in C(G), k = 0, \cdots, n-1$ について、

$$\begin{aligned}\sum_{i=0}^{n-1} (f, e_i) e_i(\zeta^k) &= \sum_{i=0}^{n-1} (n^{-1} \sum_{l=0}^{n-1} f(\zeta^l) \zeta^{-il}) \zeta^{ik} \\ &= n^{-1} \sum_{l=0}^{n-1} f(\zeta^l) (\sum_{i=0}^{n-1} \zeta^{i(k-l)}) \\ &= n^{-1} f(\zeta^k) (\sum_{i=0}^{n-1} \zeta^0) \\ &= f(\zeta^k)\end{aligned}$$

となることから証明が終了する。ここでも条件 *3.* が使われている。■

Fourier 変換及び逆 Fourier 変換を定義する。

定義 1.4 (Fourier 変換・逆 Fourier 変換) *Fourier* 変換 $F : C(G) \to C(G)$ を次のように定義する。

$$F(f)(\zeta^k) = \sum_{s=0}^{n-1} f(\zeta^s)\zeta^{sk},\ f \in C(G),\ k = 0, \cdots, n-1$$

逆 *Fourier* 変換 $F^{-1} : C(G) \to C(G)$ を次のように定義する。

$$F^{-1}(f)(\zeta^r) = n^{-1} \sum_{t=0}^{n-1} f(\zeta^t)\zeta^{-tr},\ f \in C(G),\ r = 0, \cdots, n-1$$

1.2 離散 Fourier 変換の性質

定理 1.5 (R-加群としての同型性) *Fourier* 変換 $F : C(G) \to C(G)$ は $R-$ 加群 としての同型写像を与え、逆 *Fourier* 変換 F^{-1} はその逆写像である。

証明 線形性は明らかである。条件 *3.* を使うことによって以下のように同型性を示すことができる。

$$\begin{aligned}
F^{-1} \cdot F(f)(\zeta^r) &= n^{-1} \sum_{t=0}^{n-1} F(f)(\zeta^t)\zeta^{-tr} \\
&= n^{-1} \sum_{t=0}^{n-1} (\sum_{s=0}^{n-1} f(\zeta^s)\zeta^{st})\zeta^{-tr} \\
&= n^{-1} \sum_{s=0}^{n-1} f(\zeta^s)(\sum_{t=0}^{n-1} \zeta^{t(s-r)}) \\
&= n^{-1} f(\zeta^r)(\sum_{t=0}^{n-1} \zeta^0) \\
&= f(\zeta^r)
\end{aligned}$$

$$\begin{aligned}
F \cdot F^{-1}(f)(\zeta^k) &= \sum_{s=0}^{n-1} F^{-1}(f)(\zeta^s)\zeta^{sk} \\
&= \sum_{s=0}^{n-1} (n^{-1} \sum_{t=0}^{n-1} f(\zeta^t)\zeta^{-ts})\zeta^{sk} \\
&= n^{-1} \sum_{t=0}^{n-1} f(\zeta^t)(\sum_{s=0}^{n-1} \zeta^{s(k-t)}) \\
&= n^{-1} f(\zeta^k)(\sum_{s=0}^{n-1} \zeta^0) \\
&= f(\zeta^k)
\end{aligned}$$

■

$C(G)$ には R から誘導される自然な積の他に、畳み込みと呼ばれる積を定義することができる。

定義 1.6 (C(G) 上の畳み込み) $f, g \in C(G)$ に対して、畳み込み $f * g \in C(G)$ を次のように定義する。

$$f * g(\zeta^r) = \sum_{i=0}^{n-1} f(\zeta^{r-i})g(\zeta^i),\ r = 0, \cdots, n-1$$

$C(G)$ はこの畳み込みを積としても可換環となり、さらに R 上の多元環となる。これを G の R 上の群環と呼び、$R[G]$ と書く。$C(G)$ と $R[G]$ は $R-$ 加群としては同じものであるが、積の違いを区別するために記号を使い分ける。

命題 1.7 $R[G]$ は R 上の可換な多元環である。

1. $\delta \in R[G] : \delta(1) = 1, \delta(\zeta^i) = 0, i = 1, \cdots, n-1$ とすると $f * \delta = f, f \in R[G]$
2. $f * g = g * f, f, g \in R[G]$
3. $f * (g * h) = (f * g) * h, f, g, h \in R[G]$
4. $f * (g + h) = f * g + f * h, f, g, h \in R[G]$
5. $(\lambda f) * g = \lambda(f * g), \lambda \in R, f, g \in R[G]$

証明 *1.* は直接計算する。

$$\begin{aligned} f * \delta(\zeta^r) &= \sum_{i=0}^{n-1} f(\zeta^{r-i})\delta(\zeta^i) \\ &= f(\zeta^r) \end{aligned}$$

2. は $r - i = t$ と変数変換すればよい。

$$\begin{aligned} f * g(\zeta^r) &= \sum_{i=0}^{n-1} f(\zeta^{r-i})g(\zeta^i) \\ &= \sum_{i \equiv 0 (mod\, n)}^{n-1} f(\zeta^{r-i})g(\zeta^i) \\ &= \sum_{t=r-(n-1)}^{r} f(\zeta^t)g(\zeta^{r-t}) \\ &= g * f(\zeta^r) \end{aligned}$$

3. は可換性を利用する。

$$\begin{aligned} f * (g * h)(\zeta^r) &= \sum_{i=0}^{n-1} (g * h)(\zeta^{r-i})f(\zeta^i) \\ &= \sum_{i=0}^{n-1} (\sum_{j=0}^{n-1} g(\zeta^{(r-i)-j})h(\zeta^j))f(\zeta^i) \\ &= \sum_{j=0}^{n-1} (\sum_{i=0}^{n-1} g(\zeta^{(r-j)-i})f(\zeta^i))h(\zeta^j) \\ &= \sum_{j=0}^{n-1} (f * g)(\zeta^{r-j})h(\zeta^j) \\ &= (f * g) * h(\zeta^r) \end{aligned}$$

4. と *5.* は明らかである。■

定理 1.8 (R-多元環としての同型性) *Fourier* 変換 $F : R[G] \to C(G)$ は $R-$ 多元環としての同型写像を与え、逆 *Fourier* 変換 F^{-1} はその逆写像である。すなわち、同値な性質

1. $F(f*g)=F(f)F(g), f,g\in R[G]$
2. $F^{-1}(fg)=F^{-1}(f)*F^{-1}(g), f,g\in C(G)$
3. $F(fg)=F(f)*F(g), f,g\in C(G)$
4. $F^{-1}(f*g)=F^{-1}(f)F^{-1}(g), f,g\in R[G]$

が成り立つ。

証明 *1.* のみを証明すればよい。

$$\begin{aligned}
F(f*g)(\zeta^i) &= \sum_{s=0}^{n-1} f*g(\zeta^s)\zeta^{si} \\
&= \sum_{s=0}^{n-1}(\sum_{t=0}^{n-1} f(\zeta^{s-t})g(\zeta^t))\zeta^{si} \\
&= \sum_{s=0}^{n-1}\sum_{t=0}^{n-1} f(\zeta^{s-t})\zeta^{(s-t)i}g(\zeta^t)\zeta^{ti} \\
&= \sum_{t=0}^{n-1}(\sum_{s=0}^{n-1} f(\zeta^{s-t})\zeta^{(s-t)i})g(\zeta^t)\zeta^{ti} \\
&= \sum_{t=0}^{n-1} F(f)(\zeta^i)g(\zeta^t)\zeta^{ti} \\
&= F(f)(\zeta^i)F(g)(\zeta^i)
\end{aligned}$$

■

定理 1.9 (構造定理) R 上の多項式環 $R[X]$ から $R[G]$ への $R-$ 線形写像を

$$X^r \to e_r,\ r=0,\cdots,n-1$$

を線形拡張するように定義する。この核は (X^n-1) であり、$R[X]/(X^n-1)$ と $R[G]$ は $R-$ 加群として同型である。さらに、この同型写像は $R-$ 多元環としての同型を与える。

証明 $R-$ 加群として同型であることは明らかである。$a(X),b(X)\in R[X]/(X^n-1)$ を

$$\begin{aligned}
a(X) &= a_{n-1}X^{n-1}+\cdots+a_1X+a_0,\ a_i\in R,\ i=0,\cdots,n-1 \\
b(X) &= b_{n-1}X^{n-1}+\cdots+b_1X+b_0,\ b_i\in R,\ i=0,\cdots,n-1
\end{aligned}$$

とすると、同型写像は

$$a_s\to a(\zeta^s),\ b_t\to b(\zeta^t)$$

というような対応により、$a,b\in R[G]$ を定める。$c(X)=a(X)b(X)\in R[X]/(X^n-1)$ とすると

$$\begin{aligned}
c(X) &= c_{n-1}X^{n-1}+\cdots+c_1X+c_0,\ c_i\in R \\
c_r &= \sum_{s+t\equiv r(mod\, n)} a_sb_t
\end{aligned}$$

となるが、この係数は同型写像により、

$$c(\zeta^r)=\sum_{i=0}^{n-1} a(\zeta^{r-i})b(\zeta^i)$$

に対応するが、これは $c=a*b$ を示している。■

今後、上の対応によって $R[X]/(X^n-1)$ と $R[G]$ を同一視する場合がある。その場合、上の記号で多項式の係数 $a_i \in R$ の添え字は n を法として考える。もし、i が $0,\cdots,n-1$ 以外の値をとるときは、暗黙のうちに $i \leftarrow i\%n$ という変換を施すことにする。

1.3 高速乗算法への応用

次節で高速 Fourier 変換について論ずるが、Fourier 変換が高速に計算できることを利用して $R[X]/(X^n-1)$ の乗算を高速に行なうことができる。

算法 1.10 (多項式の高速乗算法) $a(X), b(X) \in R[X]/(X^n-1)$ を

$$a(X) = a_{n-1}X^{n-1} + \cdots + a_1X + a_0,\ a_i \in R,\ i = 0,\cdots,n-1$$
$$b(X) = b_{n-1}X^{n-1} + \cdots + b_1X + b_0,\ b_i \in R,\ i = 0,\cdots,n-1$$

その積 $c(X) = a(X)b(X) \in R[X]/(X^n-1)$ を

$$c(X) = c_{n-1}X^{n-1} + \cdots + c_1X + c_0,\ c_i \in R$$
$$c_r = \sum_{i=0}^{n-1} a_{r-i}b_i$$

と表現する。この計算を次の手順で行なう。

Step 1. $(a_0,\cdots,a_{n-1}), (b_0,\cdots,b_{n-1})$ に対して、その *Fourier* 変換 $(a'_0,\cdots,a'_{n-1}), (b'_0,\cdots,b'_{n-1})$ を計算する。

Step 2. 項毎に乗算して $(c'_0,\cdots,c'_{n-1}) = (a'_0b'_0,\cdots,a'_{n-1}b'_{n-1})$ とする。

Step 3. $(c'_0,\cdots,c'_{n-1})$ に対して、その逆 *Fourier* 変換 $(c_0,\cdots,c_{n-1})$ を計算する。

証明 定理 *1.8* と定理 *1.9* はこの算法の正当性を示している。■

2 高速 Fourier 変換

2.1 Cooley-Tukey 型高速算法

補題 2.1 可換環 R が自然数 N と $2N$ について、離散 *Fourier* 変換の必要条件を満たし、G_N を 1 の原始 N 乗根 ζ_N から生成される巡回群、G_{2N} を 1 の原始 $2N$ 乗根 ζ_{2N} から生成される巡回群であり、さらに

$$\zeta_{2N}^2 = \zeta_N$$

が成り立ち、$G_N \subset G_{2N}$ となっていると仮定する。このとき、$R[G_N]$ の元に対する *Fourier* 変換が高々 M 回の加算と乗算で計算できるとすれば、$R[\zeta_{2N}]$ の元に対する *Fourier* 変換は高々 $2M+6N$ 回の加算と乗算で計算できる。

証明 $f \in R[\zeta_{2N}]$ に対して、$f_{even}, f_{odd} \in R[\zeta_N]$ を

$$f_{even}(\zeta_N^u) = f(\zeta_{2N}^{2u}),\ u = 0,\cdots,N-1$$
$$f_{odd}(\zeta_N^v) = f(\zeta_{2N}^{2v+1}),\ v = 0,\cdots,N-1$$

によって定める。f の *Fourier* 変換について、次の式が成り立つ。

$$\begin{aligned} F(f)(\zeta_{2N}^k) &= \sum_{i=0}^{2N-1} f(\zeta_{2N}^i)\zeta_{2N}^{ik} \\ &= \sum_{u=0}^{N-1} f(\zeta_{2N}^{2u})\zeta_{2N}^{2uk} + \sum_{v=0}^{N-1} f(\zeta_{2N}^{2v+1})\zeta_{2N}^{(2v+1)k} \\ &= \sum_{u=0}^{N-1} f_{even}(\zeta_N^u)\zeta_N^{uk} + \sum_{v=0}^{N-1} f_{odd}(\zeta_N^v)\zeta_N^{vk}\zeta_{2N}^k \\ &= F(f_{even})(\zeta_N^k) + F(f_{odd})(\zeta_N^k)\zeta_{2N}^k \end{aligned}$$

$\zeta_{2N}^k, k = 0, \cdots, 2N-1$ は高々 $2N$ 回の乗算で計算できる。また仮定より、$F(f_{even})$ と $F(f_{odd})$ は高々 $2M$ 回で計算できる。これらと上の式を利用すると $F(f)$ は高々 $2M + 6N$ 回の加算と乗算で計算できることがわかる。■

定理 2.2 (Cooley-Tukey 型高速算法) 可換環 R が自然数 $N = 2^n$ とそのすべての約数について、離散 *Fourier* 変換の必要条件を満たし、$K|N$ ならば $G_K \subset G_N$ となっていると仮定する。このとき、ζ_N が与えられたとすると、$R[G_N]$ の元に対する *Fourier* 変換は高々 $n2^{n+2} = 4Nlog_2N$ 回の加算と乗算で計算できる。

証明　$M(n)$ で $N = 2^n$ の場合に *Fourier* 変換の計算に要する加算と乗算の回数を表わす。n に関する帰納法で証明する。$n = 1$ のとき、

$$\begin{aligned} F(f)(\zeta^0) &= f(\zeta^0)\zeta^0 + f(\zeta^1)\zeta^0 = f(\zeta^0) + f(\zeta^1) \\ F(f)(\zeta^1) &= f(\zeta^0)\zeta^0 + f(\zeta^1)\zeta^1 = f(\zeta^0) + f(\zeta^1)\zeta^1 \end{aligned}$$

より、$M(1) = 3 \leqq 1 \times 2^{1+2}$ となる。$M(n) \leqq n2^{n+2}$ であると仮定すると補題より、

$$M(n+1) \leqq 2M(n) + 6 \times 2^n \leqq 2M(n) + 8 \times 2^n = (n+1)2^{n+3}$$

となり、帰納法により証明された。■

参考文献

Fourier 解析

[F1] T. W. Koerner(高橋 陽一郎訳), “フーリエ解析大全 *(*上*)*”, 朝倉書店, 1996

[F2] T. W. Koerner(高橋 陽一郎訳), “フーリエ解析大全 *(*下*)*”, 朝倉書店, 1996

[F3] 大浦 拓哉, *FFT* の概略と設計法

算法

[S1] 野下浩平, 高岡忠雄, 町田元, “基本的算法”, 岩波書店, 1983

[S2] D.E.Knuth(中川圭介訳), “準数値算法/算術演算”, サイエンス社, 1986

ディジタル信号処理

[D1] 電子情報通信学会, “ディジタル信号処理の基礎”, コロナ社, 1988