フーリエ変換とMattson-Solomon多項式

武田二郎*, 梶山雄介**

(昭和52年9月8日受理)

Fourier Transform and Mattson-Solomon Polynomial

ZIRŌ TAKEDA and YŪSUKE KAJIYAMA

Abstruct:—In the coding theory, the Mattson-Solomon polynomials play prominent roles. We give an interpretation of them as Fourier transforms of functions taking values in a finite field. We know, in spite of the simplicity of expression, it is concerned deeply with the principle of duality. It seems to solve the riddle of their usefulness.

1. 数直線上の関数のフーリエ変換

数直線R上で定義された実数値(または複素数値)関数f(t)がLebesgue の意味で可積分のとき, $f(t)\in L^1(-\infty,\infty)$と表わす。このような関数では任意の$s\in R$に対して

$$\hat{f}(s)=\int_{-\infty}^{\infty} f(t)\,e^{-its}\,dt$$

が定義される。これを$f(t)$のフーリエ変換と呼び$\mathfrak{F}(f)$で表わす。$\hat{f}(s)$はsの連続関数で

$$\lim_{s\to\pm\infty}\hat{f}(s)=0$$

を満たす。さらに $\hat{f}(s)\in L^1(-\infty,\infty)$ のとき

$$\mathfrak{F}^{-1}(\hat{f})=\frac{1}{2\pi}\int_{-\infty}^{\infty}\hat{f}(s)\,e^{its}\,ds$$

と定義すると, $\mathfrak{F}^{-1}(\hat{f})=f(t)$となり, $\mathfrak{F}^{-1}$は$\mathfrak{F}$の逆変換となる。解析学ではフーリエ変換は関数$f(t)$の性質を調べるための非常に有力な手段になっている。たとえば

$\{f(t+a)\mid a\in R\}$が$L^1(-\infty,\infty)$の全体を張る$\Longleftrightarrow$ $\hat{f}(s)$が零点をもたない。

はWiener のタウバー型定理として著名である。$L^1(-\infty,\infty)$に属する2つの関数$f(t)$, $g(t)$のたたみ込みを

$$f(t)*g(t)=\int_{-\infty}^{\infty} f(\tau)\,g(t-\tau)\,d\tau$$

で定義すると

$$f(t),\ g(t)\in L^1(-\infty,\infty)\Longrightarrow f(t)+g(t)\in L^1(-\infty,\infty),\quad f(t)*g(t)\in L^1(-\infty,\infty)$$

が成り立つ。したがってたたみ込みをもって$L^1(-\infty,\infty)$に属する関数の積と定義すると, $L^1(-\infty,\infty)$は環になる。これは数直線R上の群環(Group Algebra)と呼ばれている。(群論との関連については次節を参照)。なおこの場合$f(t)\cdot g(t)$は$L^1(-\infty,\infty)$に属するとは限らないので, 通常の積(点ごとの積)で$L^1(-\infty,\infty)$は環にならないことを注意しておく。

フーリエ変換では

$$\mathfrak{F}(f+g)=\mathfrak{F}(f)+\mathfrak{F}(g),\ \mathfrak{F}(f*g)=\mathfrak{F}(f)\cdot\mathfrak{F}(g)$$

が成り立つ。第2式が示すように, 2つの関数のたたみ込みのフーリエ変換は個々の関数のフーリエ変換の点ごとの積となる。この結果たたみ込みの性質を調べるときフーリエ変換は非常に便利な手段になる。たとえばあるsで$\hat{f}(s)=0$のときには, 任意の$g(t)\in L^1(-\infty,\infty)$に対して$\mathfrak{F}(f*g)(s)=0$ となるので, フーリエ変換がある点sで0となる$L^1(-\infty,\infty)$の関数の全体

$$Ms\equiv\{\phi(t)\in L^1(-\infty,\infty)\mid\hat{\phi}(s)=0\}$$

は群環のイデアルとなる。実はMsは$L^1(-\infty,\infty)$の極大イデアルであり, 逆に$L^1(-\infty,\infty)$の極大イデアルは

* 茨城大学工学部情報工学科(日立市中成沢町)

** 茨城大学大学院工学研究科情報工学専攻(日立市中成沢町)

このようなものに限られることが知られている。したがって I を $L^1(-\infty,\infty)$ の任意のイデアルとし，I を含むような極大イデアル Ms の集合を考えると，イデアル I に対応して R の点集合 S が定義される：

$$S=\{\ s\mid I\subset Ms\ \}$$

定義から I に属するすべての関数のフーリエ変換は S 上で0となる。S が離散集合，したがって特に有限集合のときには逆にフーリエ変換が S 上で0となる関数はイデアル I に属する：

$$f\in I \iff \hat{f}(s)=0\ ,\ (\ s\in S\ )$$

が証明される。換言すればこのようなイデアル I は対応する集合 S で特性づけられる。

{本節で要約した結果の詳細は，たとえば Loomis の著書[1]を参照}

2. 有限巡回群上のフーリエ変換

数直線 R を加法に関しての群と考えると，R 上で定義された関数 $\chi_s(t)=e^{its}$ は

$$\chi_s(t_1+t_2)=\chi_s(t_1)\cdot\chi_s(t_2),\ |\chi_s(t)|=1$$

を満たし，加群 R の連続な指標になっている。実は R の連続な指標はこの形のものに限られることが証明される。したがって対応

$$s\longmapsto \chi_s(t)$$

によって，加群 R の双対群，すなわち R の連続指標のなす群 $\hat{R}$ は R 自身と同型となる。一方フーリエ変換は加群 R 上で定義された関数を，その双対群 $\hat{R}$ 上の関数に変換する操作と解釈することができる。一般の局所完閉アーベル群 G では，その双対群 $\hat{G}$ は G と同型にはならないが，上述の見地からフーリエ変換は G 上の関数から $\hat{G}$ 上の関数への変換として一般化され，くわしい結果が得られている。([1]参照)。しかしここでは一般論に深入りせず，有限巡回群上の実数値関数のフーリエ変換についてのべる。

以下 $G=\{\ 0,\ 1,\ 2,\cdots\cdots,\ n-1\ \}$ を mod n についての巡回加群とする。

$$\alpha=e^{i2\pi/n}=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$$

とすると，G の指標は $t\in G$ に対して

$$\chi_s(t)=\alpha^{st}=e^{ist2\pi/n}$$

で与えられる χ_s ($s=0,\ 1,\ 2,\cdots\cdots,\ n-1$) である。

$$(\chi_r\cdot\chi_s)(t)=\chi_r(t)\cdot\chi_s(t)=\chi_{r+s}(t)$$

が成り立つので，R の場合と同様に，G の指標群 $\hat{G}$ は G と同型な群となる。G 上で定義された実数値関数 $f(t)$ に対して，そのフーリエ変換を

$$\mathfrak{F}:f(t)\longmapsto \hat{f}(s)=\sum_{t\in G} f(t)\overline{\chi_s(t)}$$
$$(\ s=0,\ 1,\cdots,\ n-1\ ) \quad (1)$$

で定義する。これはつぎのように書き換えられる：

$$\hat{f}(s)=\sum_{t\in G} f(t)\,\chi_s^{-1}(t)=\sum_{t\in G} f(t)\,\chi_{n-s}(t)$$
$$=\sum_{t\in G} f(t)\,\alpha^{(n-s)t}=\sum_{t\in G} f(t)(\alpha^{-s})^t \quad (2)$$

Σ は有限和であるから，収束は問題にならず，前節での Lebesgue 可積分性のような付加条件が不要となり，G 上の任意の実数値関数に対してフーリエ変換が定義される。逆変換は

$$\mathfrak{F}^{-1}(\hat{f})=\frac{1}{n}\sum_{s\in G}\hat{f}(s)\,\chi_s(t)=\frac{1}{n}\sum_{s\in G}\hat{f}(s)(\alpha^t)^s \quad (3)$$

である。なぜなら

$$\sum_{s\in G}\chi_s^{-1}(t')\,\chi_s(t)=\begin{cases}0\ (\ t'\neq t\ \text{のとき})\\ n\ (\ t'=t\ \text{のとき})\end{cases} \quad (4)$$

が成り立つので

$$\mathfrak{F}^{-1}(\hat{f})=\frac{1}{n}\sum_{s\in G}\Big(\sum_{t'\in G} f(t')\,\chi_s^{-1}(t')\Big)\chi_s(t)$$
$$=\frac{1}{n}\sum_{t'\in G} f(t')\Big(\sum_{s\in G}\chi_s^{-1}(t')\,\chi_s(t)\Big)$$
$$=f(t) \quad (5)$$

となる。

G で定義された関数 $f(t)$，$\phi(t)$ に対して，たたみ込みを

$$(f*\phi)(t)=\sum_{\tau\in G} f(\tau)\,\phi(t-\tau) \quad (6)$$

と定義すると，$f(t)$ と $\phi(t)$ にはたたみ込み $f*\phi$ と点ごとの積 $f\cdot\phi$ の2種類の積が定義され，フーリエ変換によって

$$\mathfrak{F}(f*\phi)=\mathfrak{F}(f)\cdot\mathfrak{F}(\phi),\quad \mathfrak{F}(f\cdot\phi)=n^{-1}\,\mathfrak{F}(f)*\mathfrak{F}(\phi) \quad (7)$$

となる。なぜなら

$$\mathfrak{F}(f*\phi)=\sum_{t\in G}\Big(\sum_{\tau\in G} f(\tau)\,\phi(t-\tau)\Big)\overline{\chi_s(t)}$$
$$=\sum_{\tau\in G} f(\tau)\Big(\sum_{t\in G}\phi(t-\tau)\overline{\chi_s(t)}\Big)$$
$$=\sum_{\tau\in G} f(\tau)\Big(\sum_{t\in G}\phi(t)\overline{\chi_s(t+\tau)}\Big)$$
$$=\sum_{\tau\in G} f(\tau)\,\overline{\chi_s(\tau)}\cdot\sum_{t\in G}\phi(t)\overline{\chi_s(t)}$$
$$=\mathfrak{F}(f)\cdot\mathfrak{F}(\phi)$$

$$\mathfrak{F}(f)*\mathfrak{F}(\phi)=\sum_{\sigma\in G}\Big(\sum_{t\in G} f(t)\overline{\chi_\sigma(t)}\Big)\Big(\sum_{\tau\in G}\phi(\tau)\overline{\chi_{s-\sigma}(\tau)}\Big)$$
$$=\sum_{t\in G}\sum_{\tau\in G} f(t)\phi(\tau)\sum_{\sigma\in G}\overline{\chi_\sigma(t)}\,\overline{\chi_{s-\sigma}(\tau)}$$
$$=\sum_{t\in G}\sum_{\tau\in G} f(t)\phi(\tau)\overline{\chi_s(\tau)}\sum_{\sigma\in G}\chi_\sigma(t)\chi_\sigma^{-1}(\tau)$$
$$=n\sum_{t=1}^{n} f(t)\,\phi(t)\,\overline{\chi_s(t)}=n\,\mathfrak{F}(f\cdot\phi)$$

同様の計算で

$$\mathfrak{F}^{-1}(\hat{f}\ast\hat{g})=n\,\mathfrak{F}^{-1}(\hat{f})\cdot\mathfrak{F}^{-1}(\hat{g}),$$
$$\mathfrak{F}^{-1}(\hat{f}\cdot\hat{g})=\mathfrak{F}^{-1}(\hat{f})\ast\mathfrak{F}^{-1}(\hat{g}) \tag{8}$$

が成り立つ

G上の関数$f(t)$はn個のGの元kでとる値$f(k)$を与えれば定まるから，関数をn次元実ベクトルで表わすことができる：

$$f(t)\sim[f(0),f(1),\cdots\cdots,f(n-1)]$$

ベクトルの代りに実係数多項式$\hat{f}(x)$を使うこともできる：

$$f(t)\sim\hat{f}(x)\equiv f(0)+f(1)x+\cdots\cdots+f(n-1)x^{n-1} \tag{9}$$

この多項式表示では自然にx^n-1を法とする積が考えられるが，それは関数のたたみ込みに相当する。なぜなら

$$f(t)\sim f(0)+f(1)x+\cdots\cdots+f(n-1)x^{n-1},$$
$$\phi(t)\sim\phi(0)+\phi(1)x+\cdots\cdots+\phi(n-1)x^{n-1}$$

とすると

$$\hat{f}(x)\cdot\hat{\phi}(x)=(f(0)+f(1)x+\cdots+f(n-1)x^{n-1})\cdot(\phi(0)+\phi(1)x+\cdots+\phi(n-1)x^{n-1})=\sum_{k=0}^{n-1}\Big(\sum_{h=0}^{n-1}f(h)\,\phi(k-h)\Big)x^k$$

これは

$$f(t)\ast\phi(t)\sim\hat{f}(x)\cdot\hat{\phi}(x) \tag{10}$$

を示している。さらに(2)と比較すると，フーリエ変換$\mathfrak{F}(f)$の点sにおける値は$\hat{f}(x)$に$x=\alpha^{-s}$を代入した値にほかならない。したがってG上の関数を**多項式形式に表示することは，実質的に関数のフーリエ変換を考察していることになる。**

3. Mattson-Solomon 多項式

本節では$f(t)$は巡回群$G=\{0,1,\cdots\cdots,n-1\}$で定義され，有限体$GF(q)$に値をとる関数とする。ただし$n\mid q^m-1$とする。この場合には拡大体$GF(q^m)$の中に位数$n$の元$\alpha$がとれる。これら$GF(q)$，$GF(q^m)$をそれぞれ前節の実数体，複素数体になぞらえて考えると

$$\alpha^n=1,\quad \alpha^s\alpha^{n-s}=1\quad(s=0,1,\cdots,n-1)$$

だから

$$\alpha\sim e^{i2\pi/n},$$
$$\alpha^{-s}=\alpha^{n-s}\sim\overline{e^{is2\pi/n}}=e^{-is2\pi/n}$$

となる。そこで群Gの$GF(q^m)$値指標$\chi_s(t)$を

$$\chi_s(t)\equiv\alpha^{st},\quad \overline{\chi_s(t)}\equiv\alpha^{-st}$$

と定めると，$GF(q)$値関数$f(t)$のフーリエ変換を(1)と同じ式によって定義することが可能になる：

$$\mathfrak{F}:f(t)\longmapsto\hat{f}(s)=\sum_{t\in G}f(t)\overline{\chi_s(t)}$$

また$\beta=\alpha^s$（$s\neq0$）のとき

$$(1+\beta+\beta^2+\cdots\cdots+\beta^{n-1})(1-\beta)=1-\beta^n=1-(\alpha^n)^s=0$$

だから，指標の直交性(4)もそのまま成り立つ。$GF(q)$の標数をpとすると，$p\mid q^m$，$n\mid q^m-1$より$p\nmid n$。したがってnは有限体内の非零元であることに注意すれば，逆変換も(3)にならって定義できる：

$$\mathfrak{F}^{-1}(\hat{f})=\frac{1}{n}\sum_{s\in G}\hat{f}(s)\chi_s(t)=\frac{1}{n}\sum_{s\in G}\hat{f}(s)(\alpha^{ts})$$

更に$GF(q)$値関数の場合にも(6)によって関数のたたみ込みを定義すれば，前節と同じ計算で(7)，(8)がそのまま成り立つ。

符号理論ではコード単語は$GF(q)$の元を成分とするn次元ベクトルで与えられる：

$$u=[c_0,c_1,\cdots\cdots,c_{n-1}]\quad(c_i\in GF(q))$$

これは$G=\{0,1,\cdots,n-1\}$上で定義された$GF(q)$値の関数と解釈できる。この関数をフーリエ変換したものを同じベクトル形式で表わすと

$$\mathfrak{F}:u=[c_0,c_1,\cdots,c_{n-1}]\longmapsto v=[b_0,b_1,\cdots,b_{n-1}]$$

$$b_i=\sum_{t\in G}c_k(\alpha^{-s})^k=\sum_{t\in G}c_t\,\alpha^{(n-s)t}\in GF(q^m)$$

となる。符号理論でよく使われるようにコード単語uを多項式

$$p_u(x)=c_0+c_1x+\cdots\cdots+c_{n-1}x^{n-1}$$

で表わすと，vに対応するのは

$$p_v(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1},\quad b_s=p_u(\alpha^{n-s})$$

となる。これは符号理論でMattson-Solomon[2]がコード多項式に同伴する多項式として導入したものになっている。したがってMattson-Solomonの多項式はコード単語のフーリエ変換にほかならない。フーリエ逆変換の式を用いれば

$$c_t=\frac{1}{n}\sum_{s\in G}b_s(\alpha^t)^s\equiv\frac{1}{n}p_v(\alpha^t)$$

となり，vからコードベクトルuが再生される。

BCHコードでは，コード多項式は$GF(q^m)$の元α，α^2，α^3，…，α^dを根にもつものとして定義される。これはMattson-Solomon多項式の係数

$$b_{n-d}=b_{n-(d-1)}=\cdots\cdots=b_{n-1}=0$$

を意味し，それはフーリエ変換が$\hat{G}$の特定の点集合S＝{ $n-d$, $n-(d-1)$, ……, $n-1$ } で0となることにほかならない。つまりBCHコードの定義はコード単語の全体，すなわちたたみ込みを積とするG上の関数の環のイデアルを，そのフーリエ変換がとる，$\hat{G}$内の零点の集合Sで特性づけているのである。つまりタウバー型の特性づけである。

参 考 文 献

[1] L.H.Loomis. An Introduction to Abstract Harmonic Analysis, Van Nostrand (1953)

[2] H.F.Mattson-G.Solomon. *J. Soc. Indus. Appl. Math.*, 9 (1961) 654－669