

$\mathbb{Z}_4$ の拡大環から得られる Hadamard 差集合

東京女子大・文理 山田美枝子 (Mieko Yamada)

東京女子大・文理 山本幸一 (Koichi Yamamoto)

§ 1. Hadamard 差集合.

1. 既知の結果.

定理 A (Mann). v が 2 の非自明な (v, k, λ) ブロックデザインのパラメータは

$$v = 2^{2s}, \quad k = 2^{s-1}(2^s \pm 1), \quad \lambda = 2^{s-1}(2^{s-1} \pm 1), \quad n = 2^{2s-2}$$

で与えられるものに限る. その関連行列で成分 0 を -1 で置き換えたものは 2^{2s} 次の正則 (regular) な Hadamard 行列である. また各行和が一定 $\pm 2^{s-1}$ になる.

定理 B (Turyn, 山本ら). 位数 2^{2s} のアーベル群 G の上に $(2^{2s}, 2^{s-1}(2^s - 1), 2^{s-1}(2^{s-1} - 1))$ 差集合があれば, G の指数 (exponent) k について $k \leq s+1$ となる.

定義. 上のパラメータを持つ差集合と, G 上の Hadamard 差集合 とする.

定理 C 位数がそれぞれ $2^{2s_1}, 2^{2s_2}$ のアーベル群 G_1, G_2 の上

の Hadamard 差集合 D_1, D_2 があれば

$$D_1 \times D_2' \cup D_1' \times D_2$$

は直積 $G_1 \times G_2$ 上の Hadamard 差集合である。' は余集合を示す。

定理 D (Turyn) 有限体 $K = GF(2^s)$ で、 $K \times K$ の中

$$(l+m, lm) \quad (l \neq m)$$

なる対の集合は、群 $K \times K$ 上の Hadamard 差集合である。

2. 定理 B から $s \geq 2$ ならば、 $v = 2^{2s}$ なる巡回 Hadamard 差集合は存在しない。定理 D に見るように基本アーベル群上には対応する Hadamard 差集合が存在する。

本稿では 4 位巡回群 Z_4 と個の直積 Z_4^s 上に Hadamard 差集合を構成する。これは Liebler-Mena の取扱った環 $Z_4 = \mathbb{Z}/4\mathbb{Z}$ の代数拡大 R の性質を用いて行われる。

3. 一般に加法群 G の群環 $\mathbb{Z}G$ の元 $\sum_{\alpha \in G} c_\alpha \alpha$ と、 G 上に定義された、値域 $\mathbb{Z}$ の関数 $f: f(\alpha) = c_\alpha$ を同一視する。たとえば G はまた G 上いたる所 α なる値を取る関数をも表わす。また $\mathbf{0}$ は 0 の特性関数を表わす。また $\mathbf{1}$ は

$$\mathbf{0}(0) = 1, \quad \mathbf{0}(\alpha) = 0 \quad (\alpha \neq 0)$$

G 上の 2 つの関数 f, g からその convolution 積 $f * g$ を

$$(f * g)(\alpha) = \sum_{\beta \in G} f(\beta) g(\alpha - \beta)$$

で定義する。また f の共役 $\hat{f}$ は

$$\hat{f}(\alpha) = f(-\alpha)$$

から定義されるものとする。

この記号によれば, アーベル群 G の部分集合 D が (ν, R, λ) 差集合であるという条件は

$$(1) \quad D * \hat{D} = nO + \lambda G$$

と書き直すことができる。むしろ $n = R - \lambda$ 。

4. アーベル群 G の (加法的) 指標 μ は $\mu(\alpha)$ が 1 の ν 乗根である。

$$\mu(\alpha + \beta) = \mu(\alpha)\mu(\beta)$$

我々が考えるものは $f = \sum_{\alpha \in G} f(\alpha)\alpha$ のとき

$$(2) \quad \mu(f) = \sum_{\alpha \in G} f(\alpha)\mu(\alpha)$$

とおくことにより, 群環 $\mathbb{Z}G$ 上に拡張できる。そして

$$f=0 \Leftrightarrow \text{"凡ての指標 } \mu \text{ について } \mu(f)=0"$$

指標 μ の全体は位数 ν の群で, G の元 α の特性函数 l_α

$$\begin{aligned} l_\alpha(\beta) &= 1 & (\beta = \alpha \text{ のとき}), \\ &= 0 & (\beta \neq \alpha \text{ のとき}) \end{aligned}$$

は

$$l_\alpha = \frac{1}{\nu} \sum_{\mu \in M} \bar{\mu}(\alpha) \mu$$

となる。 M は指標群。上式は指標の直交関係と呼ばれるものである。

前出 convolution 積は, 群環 $\mathbb{Z}G$ の元としての積に当る。したがって, G の指標 μ について

$$\mu(f * g) = \mu(f)\mu(g),$$

$$\mu(\hat{f}) = \overline{\mu(f)} \quad - : \text{共役複素数}$$

§ 2. $\mathbb{Z}_4$ の拡大環 $\mathcal{R}$

5. $F = GF(2)$, $K = GF(2^s)$, $s \geq 2$ とし, F 上の monic 原始多項式

$$(3) \quad f(x) = x^s + c_1 x^{s-1} + \cdots + c_s$$

において, 係数 $c_1, \dots, c_s$ を $\text{mod } 4$ で動かす, その根 ξ が

$$\xi^{2^s-1} = 1$$

を満たすようにすることができる. ξ を $\mathbb{Z}_4$ に添加して生ずる

$\mathbb{Z}_4$ の代数的拡大環 $\mathbb{Z}_4(\xi)$ を $\mathcal{R}$ で表わす.

この環 $\mathcal{R}$ は $\mathbb{Z}_4$ 上 s 次代数的で, 根基 (radical) $\mathcal{R} = 2\mathcal{R}$ をも

ち, 剰余類体 $\mathcal{R}/\mathcal{R}$ は $K = GF(2^s)$ である. 剰余類体の代表は,

いわゆる Teichmüller 代表系

$$(4) \quad \mathcal{T} = \{0, 1, \xi, \xi^2, \dots, \xi^{2^s-2}\}$$

から取ることができる. $\mathcal{T}$ はまた $\mathcal{R}$ の中で, 方程式

$$x^{2^s} = x$$

の根であるものの全体となる.

この代表系を用いれば, $\mathcal{R}$ の元 α が, 一意的に

$$\alpha = \alpha_0 + 2\alpha_1, \quad \alpha_0, \alpha_1 \in \mathcal{T}$$

と書き表わされる.

しばらく α によって定まる α_0 を $\alpha_0 = \tau(\alpha)$ と書くことに

する.

$\mathcal{R}$ の正則元 (逆元を持つもの) の全体 $\mathcal{R}^* = \mathcal{R} - \{0\}$ は $2^s(2^s-1)$ 位の群で, $\alpha \in \mathcal{R}^*$ に対して

$$\alpha \longrightarrow \tau(\alpha)$$

は, $\mathcal{R}^*$ から $\{1\}$ の上への準同型写像である. その核は, $\tau(\alpha) = 1$ なる α , すなわち

$$1 + 2\beta, \quad \beta \in \mathcal{V}$$

の形の元, いわゆる主単数 (principal unit) の作る主単数群 $\mathcal{E}$ である. なお主単数 $1 + 2\beta$ においては β が $\mathcal{R}/\mathcal{I} = K$ の元とみなすことも便利であるから, 主単数は $1 + 2l$, $l \in K$ の形に書くことにする. ここで

$$(1 + 2l)(1 + 2m) = 1 + 2(l + m) \quad (l, m \in K)$$

によって, 主単数群 $\mathcal{E}$ は, K の加法群と同型である. かくて, $\mathcal{R}^*$ は $\{1\}$ と $\mathcal{E}$ の直積である.

6. $\mathcal{R}$ の元 $\alpha = \alpha_0 + 2\alpha_1$ には

$$\alpha^F = \alpha_0^2 + 2\alpha_1^2$$

を対応せると, F は環 $\mathcal{R}$ の自己同型である.

これを $\mathcal{R}$ の Frobenius 自己同型 と呼ぶ.

[証明] $(\alpha\beta)^F = \alpha^F\beta^F$ は簡単である. $\alpha = \alpha_0 + 2\alpha_1$, $\beta = \beta_0 + 2\beta_1$

ならば $\alpha\beta = \alpha_0\beta_0 + 2(\alpha_0\beta_1 + \alpha_1\beta_0)$, $\alpha_0\beta_0 \in \mathcal{V}$ で,

$$(\alpha\beta)^F = (\alpha_0\beta_0)^2 + 2(\alpha_0\beta_1 + \alpha_1\beta_0)^2 = \alpha_0^2\beta_0^2 + 2\alpha_0^2\beta_1^2 + 2\alpha_1^2\beta_0^2$$

$$= \alpha^F \beta^F$$

$(\alpha + \beta)^F = \alpha^F + \beta^F$ を確かめるのに, $\tau(\alpha)$ の具体形を必要とする.

$$(5) \quad \tau(\alpha) = \alpha^{2^s}$$

$$(6) \quad \tau(\alpha + \beta) = \tau(\alpha) + \tau(\beta) + 2\alpha^{2^{s-1}}\beta^{2^{s-1}}$$

何となく $\alpha = \alpha_0 + 2\alpha_1$ より $\alpha^{2^s} = \alpha_0^{2^s} = \alpha_0$ である (5) である.

したがって

$$\tau(\alpha + \beta) = (\alpha + \beta)^{2^s} = \alpha^{2^s} + \beta^{2^s} + 2\alpha^{2^{s-1}}\beta^{2^{s-1}} = \alpha_0 + \beta_0 + 2\alpha^{2^{s-1}}\beta^{2^{s-1}},$$

$$\alpha + \beta = (\alpha_0 + \beta_0 + 2\alpha^{2^{s-1}}\beta^{2^{s-1}}) + 2(\alpha_1 + \beta_1 + \alpha^{2^{s-1}}\beta^{2^{s-1}}),$$

$$\begin{aligned} (\alpha + \beta)^F &= (\alpha_0 + \beta_0 + 2\alpha^{2^{s-1}}\beta^{2^{s-1}})^2 + 2(\alpha_1 + \beta_1 + \alpha^{2^{s-1}}\beta^{2^{s-1}})^2 \\ &= (\alpha_0 + \beta_0)^2 + 2(\alpha_1^2 + \beta_1^2 + \alpha^{2^s}\beta^{2^s}) = \alpha_0^2 + \beta_0^2 + 2(\alpha_1^2 + \beta_1^2) \\ &= \alpha^F + \beta^F \end{aligned}$$

これから ξ と共に $\xi^F, \xi^{F^2}, \dots, \xi^{F^{s-1}}$ が原始多項式 (3) の根となる. しかし他には根がない. (3) の根は $\text{mod } \pi$ では, $\xi, \xi^F, \dots, \xi^{F^{s-1}}$ のいずれかであるから, $\xi^{2^t} + 2\beta$ が根ならば,

$$0 = f(\xi^{2^t} + 2\beta) = f(\xi^{2^t}) + 2f'(\xi^{2^t})\beta = 0,$$

$f'(\xi^{2^t})\beta = 0$ であるが, $f'(\xi^{2^t}) \neq 0$ (K において) だから, $\beta = 0$ とななければならない.

また Frobenius 自己同型で不変なものは $\mathbb{Z}_q$ の元に限る.

$$\alpha = \alpha_0 + 2\alpha_1, \quad \alpha^F = \alpha_0^2 + 2\alpha_1^2 \quad \text{ならば} \quad \alpha_0^2 = \alpha_0, \quad \alpha_1^2 = \alpha_1 \quad \text{で Teichmüller}$$

系 (4) の元だから, $\alpha_0 = 0$ または 1 , $\alpha_1 = 0$ または 1 . よって $\alpha = 0, 1, 2, 3$ のいずれかとなる.

ゆえに $\mathcal{R}$ の自己同型は Frobenius 自己同型 F の中だけで, $\mathcal{R}$ の自己同型群は F の生成する s 位巡回群となる.

7. $\mathcal{R}$ の元 α の相対トレース $S_{\mathcal{R}/\mathbb{Z}_4} \alpha$ を

$$S_{\mathcal{R}/\mathbb{Z}_4} \alpha = \alpha + \alpha^F + \alpha^{F^2} + \cdots + \alpha^{F^{s-1}}$$

と定義すると, 値は $\mathbb{Z}_4$ に属して, 以下

$$S_{\mathcal{R}/\mathbb{Z}_4}(\alpha + \beta) = S_{\mathcal{R}/\mathbb{Z}_4} \alpha + S_{\mathcal{R}/\mathbb{Z}_4} \beta.$$

これは F 上 K の元 a の相対トレース

$$S_{K/F} a = a + a^F + a^{F^2} + \cdots + a^{F^{s-1}}$$

と類似であるが, $\alpha = \alpha_0 + 2\alpha_1$ とすると α_0 は K の元と見て,

$$S_{\mathcal{R}/\mathbb{Z}_4} \alpha \equiv S_{K/F} \alpha_0 \pmod{\mathcal{R}}$$

§3. $\mathcal{R}$ の加法的指標, 乗法的指標, Gauss の和 および Jacobi の和.

8. K を F 上のベクトル空間と見て

$$f(x, y) = S_{K/F} xy$$

は非退化双一次形式である. 非退化とは

$$\forall a \in K \text{ について } S_{K/F}(a) = 0 \implies a = 0$$

の意味で, その真であることは $S_{K/F}(c) = 1$ なる $c \in K$ が存在

することから分る. もしすべての c について $S_{K/F}(c) = 0$ ならば,

$$c + c^2 + c^4 + \cdots + c^{2^{s-1}} = 0$$

で, 2^{s-1} 次の多項式 $x^{2^{s-1}} + x^{2^{s-2}} + \cdots + x^2 + x$ が 2^s 個の根を持つこと

と なって矛盾する。

したがって K から F への '1次函数' g は, ある b につき,

$$g(a) = S_{K/F}(ba) \quad (a \in K)$$

の形に書かれる。したがってまた, 加法群 K の加法的指標は

$$(7) \quad \lambda(a) = (-1)^{S_{K/F}(la)} \quad (a \in K)$$

の形である。この指標を λ_l で表わすことにする。

次に $\mathcal{R}$ から, 基礎環 $\mathbb{Z}_4$ への1次函数 g は, ある β につき

$$g(\alpha) = S_{\mathcal{R}/\mathbb{Z}_4}(\beta\alpha) \quad (\alpha \in \mathcal{R})$$

の形をしている。

実際 $S_{\mathcal{R}/\mathbb{Z}_4}(\beta\alpha)$ が1次函数であるのは明白だが, なお

$$\forall \alpha \quad S_{\mathcal{R}/\mathbb{Z}_4}(\beta\alpha) = 0 \implies \beta = 0.$$

何と分れば $\alpha = \alpha_0 + 2\alpha_1$, $\beta = \beta_0 + 2\beta_1$ のとき

$$S_{\mathcal{R}/\mathbb{Z}_4}(\beta\alpha) - S_{\mathcal{R}/\mathbb{Z}_4}(\beta_0\alpha_0) = 0$$

がすべての α_0 について成立ち $\beta_0 = 0$. よって $\beta = 2\beta_1$ だが

$$S_{\mathcal{R}/\mathbb{Z}_4}(2\beta_1\alpha) = 0, \quad S_{\mathcal{R}/\mathbb{Z}_4}(\beta_1\alpha) = 0 \quad \text{がすべての } \alpha \text{ について成立つ}$$

ので $\beta_1 = 0$, 結局 $\beta = 0$ となる。

したがってまた, $\mathcal{R}$ の加法的指標は, ある β について

$$(8) \quad \lambda(\alpha) = i^{S_{\mathcal{R}/\mathbb{Z}_4}(\beta\alpha)} \quad (i = \sqrt{-1})$$

の形をしていることが分る。この指標は λ_β と書くことにす

る。たとえば

$$\lambda_l(a) = \lambda_1(la) \quad (l, a \in K),$$

$$\lambda_\beta(\alpha) = \lambda_1(\beta\alpha) \quad (\alpha, \beta \in \mathcal{R})$$

が成立し、指標の直交関係から

$$(9) \quad \sum_{l \in K} (-1)^{S_{K/F}(la)} = \begin{cases} 2^s & (a=0 \text{ のとき}), \\ 0 & (a \neq 0 \text{ のとき}), \end{cases}$$

$$(10) \quad \sum_{\beta \in \mathcal{R}} i^{S_{\mathcal{R}/\mathbb{Z}_2}(\beta\alpha)} = \begin{cases} 2^{2s} & (\alpha=0 \text{ のとき}), \\ 0 & (\alpha \neq 0 \text{ のとき}). \end{cases}$$

を得る。

9. $\mathcal{R}^*$ の指標 χ は、取る値が 1 の $2(2^s-1)$ 乗根で

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta) \quad (\alpha, \beta \in \mathcal{R}^*)$$

をみたすものである。それらは乗法を自然的に定義するとき、 $\mathcal{R}^*$ と同型な、指標群 X を構成する。

$\mathcal{R}^*$ の指標 χ は $\alpha \in \mathcal{R}$ については $\chi(\alpha) = 0$ と定義してしまつて、 $\mathcal{R}$ 全体で定義されたものと見ることにする。これを $\mathcal{R}$ の指標、または加法的指標と区別するために、 $\mathcal{R}$ の乗法的指標と呼ぶ。

$$\chi_0(\alpha) = 1 \quad (\alpha \in \mathcal{R}^*)$$

なるものが単位指標 χ_0 である。

本稿では χ の取る値が実数である、つまり ± 1 である指標を取り扱う。これら 実指標 は、 $\mathcal{R}^*$ の部分群 $\{1\}$ 上では値 1 を取り、結局主単数群 $\mathcal{E}$ の指標であるに過ぎない。すなわち、

$$\chi((1+2a)\xi^m) = \chi(1+2a)$$

χ は主単数群 E 上の指標である. $\psi(a) = \chi(1+2a)$ とおけば, ψ は K の加法群の指標で **8** に示したように $\psi(a) = (-1)^{S_{KF}(la)}$ ならしめる $l \in K$ がある. その l によって

$$\chi = \chi_l$$

と書くことにする. すなわち

$$\chi_l((1+2a)\xi^m) = (-1)^{S_{KF}(la)}$$

またさらに

$$\chi_l \chi_m = \chi_{l+m}$$

すなわち, 実指標の乗法群と K の加法群が同型である.

10. $\mathcal{O}$ の指標 χ から, **4**, (2) の線に沿って, 和

$$G(\chi) = \lambda_1(\chi) = \sum_{\alpha \in \mathcal{O}^*} \chi(\alpha) \lambda_1(\alpha)$$

を作り, これを χ に属する Gauss の和 と呼ぶ.

定理 1. χ が実指標 χ_l , $l \neq 0$ ならば

$$G(\chi_l) = 2^s \cdot i^{S_{\mathcal{O}/\mathcal{Z}_4}} l^{2^s}$$

$$\begin{aligned} \text{[証明]} \quad \lambda_1(\chi_l) &= \sum_{m=0}^{2^s-2} \sum_{a \in K} (-1)^{S_{KF}(la)} \cdot i^{S_{\mathcal{O}/\mathcal{Z}_4}((1+2a)\xi^m)} \\ &= \sum_{m=0}^{2^s-2} i^{S_{\mathcal{O}/\mathcal{Z}_4} \xi^m} \sum_{a \in K} (-1)^{S_{KF}(l+\xi^m)a} \end{aligned}$$

内側の和は (9) によって $l+\xi^m \equiv 0 \pmod{\mathcal{O}}$ なる m についてのみ, 値 2^s を取り, 他では 0 となる. そのような ξ^m はちょうど $\tau(l)$ 個, (5) から $\xi^m = l^{2^s}$ しかあって

$$G(\chi_l) = \lambda_1(\chi_l) = 2^s \cdot i^{S_{\mathcal{O}/\mathcal{Z}_4}} l^{2^s}$$

11. 実指標 χ_l の間の convolution 積が必要である。

定理 2. $\chi_0 * \chi_0 = (2^{2s} - 2^s) \mathbf{1} - 2^s \chi_0.$

$l \neq 0$ ならば $\chi_0 * \chi_l = 0,$

$$\chi_l * \chi_l = \chi_l(-1) (2^{2s} \mathbf{0} - 2^s (1 - \chi_0)).$$

$l, m, l+m \neq 0$ ならば $\chi_l * \chi_m = \chi_{l+m}(-1) 2^s \chi_{l+m}.$

ここに $\mathbf{1}$ は至る ± 3 を取る函数である。

[証明] $\alpha \in \mathcal{R}^*$ ならば

$$\begin{aligned} (\chi_0 * \chi_0)(\alpha) &= \sum_{\beta \in \mathcal{R}} \chi_0(\beta) \chi_0(\alpha - \beta) = \sum_{\beta \in \mathcal{R}} \chi_0(\alpha\beta) \chi_0(\alpha - \alpha\beta) \\ &= \sum_{\beta \in \mathcal{R}} \chi_0(\beta) \chi_0(1 - \beta) = \sum_{\beta \in \mathcal{R}^*} \chi_0(\beta) = \sum_{\beta \in \mathcal{R}} \chi_0(\beta) - \sum_{\beta \in \mathcal{E}} \chi_0(\beta) \\ &= \sum_{\beta \in \mathcal{R}^*} \chi_0(\beta) - \sum_{\beta \in \mathcal{E}} \chi_0(\beta) = \# \mathcal{R}^* - \# \mathcal{E} = 2^{2s} - 2^{s+1}. \end{aligned}$$

$\alpha \in \mathcal{R}$ ならば

$$(\chi_0 * \chi_0)(\alpha) = \sum_{\beta \in \mathcal{R}^*} \chi_0(\beta) \chi_0(\alpha - \beta) = \# \mathcal{R}^* = 2^{2s} - 2^s.$$

これより $\chi_0 * \chi_0 = (2^{2s} - 2^s) \mathbf{1} - 2^s \chi_0$ を得る。

同様に $\alpha \in \mathcal{R}^*$ ならば

$$\begin{aligned} (\chi_l * \chi_0)(\alpha) &= \sum_{\beta \in \mathcal{R}} \chi_l(\beta) \chi_0(\alpha - \beta) = \sum_{\beta \in \mathcal{R}} \chi_l(\alpha\beta) \chi_0(\alpha - \alpha\beta) \\ &= \chi_l(\alpha) \sum_{\beta \in \mathcal{R}} \chi_l(\beta) \chi_0(1 - \beta) = \chi_l(\alpha) \sum_{\beta \in \mathcal{R}^*} \chi_l(\beta) = \chi_l(\alpha) \left(\sum_{\beta \in \mathcal{R}} \chi_l(\beta) - \sum_{\beta \in \mathcal{E}} \chi_l(\beta) \right) \\ &= 0 - 0 = 0. \end{aligned}$$

$\alpha \in \mathcal{R}$ ならば

$$(\chi_l * \chi_0)(\alpha) = \sum_{\beta \in \mathcal{R}^*} \chi_l(\beta) \chi_0(\alpha - \beta) = \sum_{\beta \in \mathcal{R}^*} \chi_l(\beta) = 0.$$

したがって $\chi_l * \chi_0 = 0$ を得る。

また, $\alpha \in \mathcal{O}^*$ ならば

$$\begin{aligned} (\chi_\ell * \chi_\ell)(\alpha) &= \sum_{\beta \in \mathcal{O}} \chi_\ell(\alpha\beta) \chi_\ell(\alpha - \alpha\beta) = \sum_{\beta \in \mathcal{O}^*} \chi_\ell(\beta) \chi_\ell(1 - \beta) \\ &= \sum_{\beta \in \mathcal{O}^*} \chi_\ell\left(\frac{1 - \beta}{\beta}\right) = \sum_{\beta \in \mathcal{O}^*} \chi_\ell\left(-1 + \frac{1}{\beta}\right) = \sum_{\beta \in \mathcal{O}^*} \chi_\ell(-1 + \beta) \\ &= \sum_{\beta \in \mathcal{O}} \chi_\ell(\beta) - \sum_{\beta \in \mathcal{O}} \chi_\ell(-1 + \beta) = 0 - 0 = 0. \end{aligned}$$

$\alpha \in \mathcal{O}$ ならば, $\alpha = 2a$, $a \in K$ となる, $a \neq 0$ の時は

$$\begin{aligned} (\chi_\ell * \chi_\ell)(2a) &= \sum_{\beta \in \mathcal{O}^*} \chi_\ell(\beta) \chi_\ell(2 - \beta) = \sum_{\beta \in \mathcal{O}^*} \chi_\ell\left(-1 + \frac{2}{\beta}\right) \\ &= \sum_{\beta \in \mathcal{O}^*} \chi_\ell(-1 + 2\beta) = \sum_{\beta \in \mathcal{O}} \chi_\ell(\beta) - \sum_{\beta \in \mathcal{O}} \chi_\ell(-1 + 2\beta) = -\chi_\ell(-1) \# \mathcal{O} \\ &= -\chi_\ell(-1) 2^s. \end{aligned}$$

$\alpha = 0$ になるとは

$$(\chi_\ell * \chi_\ell)(0) = \sum_{\beta \in \mathcal{O}^*} \chi_\ell(\beta) \chi_\ell(-\beta) = \chi_\ell(-1) \# \mathcal{O}^* = \chi_\ell(-1) (2^{2s} - 2^s).$$

したがって

$$\chi_\ell * \chi_\ell = \chi_\ell(-1) \left((2^{2s} - 2^s) \mathbf{0} - 2^s (\mathbf{1} - \chi_0) \right)$$

を得る.

最後に $\chi_\ell * \chi_m$ について, $\alpha \in \mathcal{O}^*$ ならば

$$(\chi_\ell * \chi_m)(\alpha) = \sum_{\beta \in \mathcal{O}} \chi_\ell(\alpha\beta) \chi_m(\alpha - \alpha\beta) = \chi_{\ell+m}(\alpha) \sum_{\beta \in \mathcal{O}} \chi_\ell(\beta) \chi_m(1 - \beta).$$

$\alpha \in \mathcal{O}$ ならば,

$$\begin{aligned} (\chi_\ell * \chi_m)(\alpha) &= \sum_{\beta \in \mathcal{O}} \chi_\ell(\beta) \chi_m(\alpha - \beta) = \chi_m(-1) \sum_{\beta \in \mathcal{O}} \chi_\ell(\beta) \chi_m(\beta) \\ &= \chi_m(-1) \sum_{\beta \in \mathcal{O}} \chi_{\ell+m}(\beta) = 0. \end{aligned}$$

したがって

$$\chi_\ell * \chi_m = J(\chi_\ell, \chi_m) \chi_{\ell+m},$$

$$J(\chi_\ell, \chi_m) = \sum_{\alpha \in \mathbb{R}} \chi_\ell(\alpha) \chi_m(1-\alpha).$$

ここに現われた量 $J(\chi_\ell, \chi_m)$ が, χ_ℓ と χ_m に関する Jacobi の和 である.

このままではこれ以上変形ができないが, 定理 1 を援用して

$$\begin{aligned} \lambda_1(\chi_\ell * \chi_m) &= \lambda_1(\chi_\ell) \lambda_1(\chi_m) = G(\chi_\ell) G(\chi_m) = 2^{2s} i^{S_{\mathbb{R}/\mathbb{Z}_4}(\ell^2 + m^2)} \\ &= J(\chi_\ell, \chi_m) G(\chi_{\ell+m}) = 2^s i^{S_{\mathbb{R}/\mathbb{Z}_4}(\ell+m)^2} J(\chi_\ell, \chi_m), \end{aligned}$$

$$J(\chi_\ell, \chi_m) = 2^s i^{S_{\mathbb{R}/\mathbb{Z}_4}(\ell^2 + m^2 - (\ell+m)^2)}$$

の肩にあるものは, (6) から

$$(\ell+m)^2 = \ell^2 + m^2 + 2\ell^{2^{s-1}}m^{2^{s-1}}$$

だから

$$J(\chi_\ell, \chi_m) = 2^s (-1)^{S_{K/F}(\ell m)^{2^{s-1}}} = 2^s (-1)^{S_{K/F} \ell m} = 2^s \chi_{\ell m}(-1)$$

で, $\chi_\ell * \chi_m = 2^s \chi_{\ell m}(-1) \chi_{\ell+m}$ が得られ, 定理 2 の凡ての式が証明された.

§ 4. $\mathbb{R}^*/\{5\}$ の coset の合併から生ずる Hadamard 差集合

12. やれわれが最初に気づいたのは次の

定理 3 $\mathcal{R}^*$ の指数 2 の部分群は $\mathcal{R}$ 上の Hadamard 差集合である。

であるが、ここにはもっと一般的な定理 4, 5 を述べ、その特別な場合として考える。

$\mathcal{R}^*/\{\xi\}$ の coset $E_a = \{(1+2a)\xi^m\}$ は 2^{s-1} 個合併した集合 $\mathcal{D} = \bigcup_{a \in A} E_a$, $\#A = 2^{s-1}$ が $\mathcal{R}$ 上の Hadamard 差集合であることは、

$$E_a = \sum_{m=0}^{2^{s-2}} (1+2a)\xi^m, \quad \mathcal{D} = \sum_{a \in A} E_a$$

について (1) から

$$(11) \quad \mathcal{D} * \hat{\mathcal{D}} = 2^{2^{s-2}} \mathbf{0} + 2^{s-1} (2^{s-1} - 1) \mathbf{1}$$

であるが、

$$E_a = 2^{-s} \sum_{\ell \in K} \chi_{\ell}(a) \chi_{\ell} = 2^{-s} \sum_{\ell \in K} (-1)^{\sum_{k \in F} \ell a_k} \chi_{\ell}$$

だから

$$\mathcal{D} = \sum_{\ell \in K} \omega_{\ell} \chi_{\ell}, \quad \omega_{\ell} = \sum_{a \in A} (-1)^{\sum_{k \in F} \ell a_k}$$

により、次のように変形される。

$$\begin{aligned} \mathcal{D} * \hat{\mathcal{D}} &= 2^{-2s} (\omega_0 \chi_0 + \sum' \omega_{\ell} \chi_{\ell}) * (\omega_0 \chi_0 + \sum' \omega_{\ell} \hat{\chi}_{\ell}) \quad (\sum' = \sum_{\ell \neq 0} \text{の意}) \\ &= 2^{-2s} (\omega_0^2 \chi_0 * \chi_0 + \sum' \omega_{\ell}^2 \chi_{\ell} * \hat{\chi}_{\ell} + \sum'_{\ell} \sum'_{m} \omega_{\ell} \omega_m \chi_{\ell} * \hat{\chi}_m) \end{aligned}$$

ここに最初の 2 項は定理 2 によって

$$\begin{aligned} &2^{-2s} (\omega_0^2 (2^s (2^s - 1) \mathbf{0} + 2^s (2^s - 1) (\mathbf{1} - \mathbf{0})) - 2^s \chi_0) \\ &\quad + \left(\sum' \omega_{\ell}^2 \right) (2^s (2^s - 1) \mathbf{0} - 2^s (\mathbf{1} - \mathbf{0}) + 2^s \chi_0) \\ &= 2^{-2s} \left((\omega_0^2 + \sum' \omega_{\ell}^2) 2^s (2^s - 1) \mathbf{0} + (2^s (2^s - 1) \omega_0^2 - 2^s \sum' \omega_{\ell}^2) (\mathbf{1} - \mathbf{0}) + (\omega_0^2 - \sum' \omega_{\ell}^2) 2^s \chi_0 \right) \end{aligned}$$

これは $\mathcal{D} * \hat{\mathcal{D}}$ における $\mathbf{0}$ の係数は $\# \mathcal{D} = 2^{s-1}(2^s - 1)$ だから

$$\omega_0^2 + \sum' \omega_\ell^2 = 2^{2s-1}, \quad \omega_0 = 2^{s-1} \quad \text{より} \quad \sum' \omega_\ell^2 = 2^{2s-2}$$

したがって結局上式より

$$2^{s-1}(2^s - 1)\mathbf{0} + 2^{s-2}(2^s - 2)(1 - \mathbf{0}) = 2^{2s-2}\mathbf{0} + 2^{s-1}(2^{s-1} - 1)\mathbf{1}$$

となる。これが (11) の右辺に等しいので、(11) を成立させるには残余項に当る部分が

$$2^{2s} \sum_{\ell} \sum_{\substack{m \\ \ell \neq m}} \omega_\ell \omega_m \hat{\chi}_\ell * \chi_m = 0$$

であることが必要十分である。定理 2 より、上式

$$\begin{aligned} &= 2^{-2s} \sum_{\ell} \sum_{\substack{m \\ \ell \neq m}} \omega_\ell \omega_m \chi_\ell * \hat{\chi}_m = 2^{-s} \sum_{\ell} \sum_{\substack{m \\ \ell \neq m}} \omega_\ell \omega_m (-1)^{S_{KF} \ell m} \chi_m (-1) \chi_{\ell+m} \\ &= 2^{-s} \sum_{\substack{R \\ \ell \neq 0, \ell \neq R}} \left(\sum_{\ell} (-1)^{S_{KF} R \ell} \omega_\ell \omega_{R+\ell} \right) \chi_R \end{aligned}$$

で、 χ_R ($R \in K$) は一次独立であるから (11) の成立条件は

$$\sum_{\substack{\ell \neq 0, \ell \neq R}} (-1)^{S_{KF} R \ell} \omega_\ell \omega_{R+\ell} = 0.$$

定理 4. $\mathcal{D}$ が Hadamard 差集合であるための必要十分条件は

$$\omega_\ell = \sum_{a \in A} (-1)^{S_{KF} \ell a}$$

に対して

$$\sum_{\substack{\ell \neq 0, \ell \neq R}} (-1)^{S_{KF} R \ell} \omega_\ell \omega_{R+\ell} = 0 \quad (R \neq 0)$$

が成立つことである。

注意: $S_{KF} R = 1$ ならば、結論の式は自動的に成立する。ゆえに上の条件は、

$S_{K/F}R=0, R \neq 0$ のとき $(l, l+R), l \neq 0, l \neq R$ なる対に對する和

$$\sum_{\text{pair}} (-1)^{S_{K/F} R l} \omega_l \omega_{l+R} = 0$$

と書くこともできる。

系として定理3が証明される。事実 $\mathcal{A}$ の指数 2 の部分群は、 K の指数 2 の部分群 A から $\{(1+2a)\xi^m; a \in A, 0 \leq m \leq 2^s-2\}$ と与っている。 $a \in A$ に $(-1)^{S_{K/F} l a}$ を対応させたものは、 A の一つの指標 $\tilde{a}$ 、和 $\omega_l = \sum_{a \in A} (-1)^{S_{K/F} l a}$ は、上の指標が A の単位指標 $\tilde{a}$ なければ $\omega_l = 0$ 、また単位指標ならば $\omega_l = 2^{s-1}$ となる。単位指標をとる l は、凡ての $a \in A$ に対して $S_{K/F} l a = 0$ ならしめる l 、すなわち、 A の‘直交補空間’の元 l で、そのような l は唯一個しかない。したがって定理4に述べる条件が成立して、 D は Hadamard 差集合になる。

13. 次に convolution 積に関する公式、定理1, 定理2に依りなして D が Hadamard 差集合になるための条件を求めておく。その代りに使う原理は、 $\mathcal{A}$ の凡ての加法的指標 λ_β について

$$\left. \begin{aligned} \lambda_\beta(D * \hat{D}) &= 2^{2s-2} & (\beta \neq 0) \\ &= 2^{2s-2} (2^s - 1)^2 & (\beta = 0) \end{aligned} \right\}$$

が成立つことである。左辺は

$$\lambda_\beta(D) \overline{\lambda_\beta(D)}$$

で $\beta=0$ の時は自明だから $\beta \neq 0$ とするとき $\lambda_\beta(D) \overline{\lambda_\beta(D)} = 2^{2s-2}$ をしる。

さて $\lambda_\beta(\mathcal{D}) = \sum_{\alpha \in A} \sum_{m=0}^{2^s-2} i^{S_{\beta/2^4} \beta (1+2\alpha) \xi^m}$ は Gauss の数体 $\mathbb{Q}(i)$ の整数 i , イ
デアル と いて は

$$(\lambda_\beta(\mathcal{D}))(\overline{\lambda_\beta(\mathcal{D})}) = 2^{2s-2}$$

であるが, $\mathbb{Q}(i)$ で素数 2 は 分解して $2 = (1+i)^2$, $(1+i)$ は $\mathbb{Z}[i]$
に属する 2 の素因数である. したがって イデアル と いて は

$$(\lambda_\beta(\mathcal{D})) = (1+i)^{2s-2} = (2^{s-1})$$

したがって $\lambda_\beta(\mathcal{D}) = 2^{s-1} v_\beta$ とおくとき v_β は $\mathbb{Z}[i]$ の単数 ± 1 ,
 $\pm i$ になる.

14. さらに変形してゆくために $a \in K$ に対して

$$z_a = \lambda_1(E_a) = \sum_{m=0}^{2^s-2} i^{S_{\beta/2^4} (1+2a) \xi^m}$$

と置く.

まず $\beta \in E_b$ ならば $\lambda_\beta(E_a) = z_{a+b}$, $\lambda_{2\beta}(E_a) = -1$ であることを証
明しておく.

事実 $\beta = (1+2b)\xi^u$ ならば

$$\begin{aligned} \lambda_\beta(E_a) &= \sum_{m=0}^{2^s-2} i^{S_{\beta/2^4} \beta (1+2a) \xi^m} = \sum_{m=0}^{2^s-2} i^{S_{\beta/2^4} (1+2a)(1+2b) \xi^{m+u}} \\ &= \sum_{m=0}^{2^s-2} i^{S_{\beta/2^4} (1+2a+2b) \xi^m} = \lambda_1(E_{a+b}) = z_{a+b}. \end{aligned}$$

同様に $\lambda_{2\beta}(E_a) = \lambda_2(E_{a+b})$ であるが, 一般に $\lambda_2(E_a) = -1$ であ
る:

$$\lambda_2(E_a) = \sum_{m=0}^{2^s-2} (-1)^{S_{K/F} (1+2a) \xi^m} = \sum_{m=0}^{2^s-1} (-1)^{S_{K/F} \xi^m} = -1$$

特に $\lambda_{2\beta}(\mathcal{D}) = -2^{s-1}$ であり, 13. に述べた条件で $\lambda_{2\beta}(\mathcal{D})/2^{s-1}$ が単数

である' が満足される

定理 5. $\mathcal{D}$ が $\mathbb{R}$ 上の Hadamard 差集合であるための必要十分条件は

$$z_a = \sum_{m=0}^{s-2} i^{S_{R/2}(1+2a)m} \xi^m$$

に対して, $\rho \in K$ につき

$$\sum_{a \in A+B} z_a = 2^{s-1} v_\rho, \quad v_\rho \in \{\pm 1, \pm i\}$$

が成立することである.

系 として A が群の場合には, $A+B=A$ またはある C について $A+C$ であり,

$$\sum_{a \in A} z_a = \sum_{m=0}^{s-2} i^{S_{R/2} m} \sum_{a \in A} (-1)^{S_{K/F} a \xi^m}$$

だが, 内側の和は **12** に示したように ξ^m が A の直交補空間の元の時だけ 2^{s-1} になり他は 0 になるから

$$\sum_{a \in A} z_a = 2^{s-1} i^{S_{R/2} m} \xi^m, \quad m \text{ は } S_{K/F}(\xi^m a) = 0 \quad (a \in A) \text{ なる値}$$

また $\sum_{a \in A+C} z_a$ については, $A \cup (A+C) = K$ であり $\sum_{a \in K} z_a = 0$ より, $\sum_{a \in A+C} z_a =$

$-\sum_{a \in A} z_a = -2^{s-1} i^{S_{R/2} m} \xi^m$ となって, 定理 5 の条件が満足されて, $\mathcal{D}$

が Hadamard 差集合になる.

例. $s=3$. $f(x)=x^3+2x^2+x+3$. coset E_a の表.

E_{000}	E_{100}	E_{010}	E_{001}	E_{110}	E_{011}	E_{111}	E_{101}
100	300	120	102	320	122	322	302
010	030	012	230	032	232	212	210
001	003	021	023	223	203	201	021
132	312	110	310	330	332	112	130
233	211	011	031	033	213	231	013
331	113	133	131	311	333	111	313
121	323	321	101	123	301	103	303

$100=1, 010=5, 001=5^2$ ϵ $xyz = x+yz+zy^2$ の意味である。

$$z_{000} = -3+2i, z_{100} = -3-2i, z_{010} = 1-2i, z_{001} = 1-2i, z_{110} = 1+2i, z_{011} = 1-2i, \\ z_{111} = 1+2i, z_{101} = 1+2i.$$

$A=\{0, \xi^a, \xi^b, \xi^c\}$ を (a, b, c) で表わして, 定理 5 の条件をチェックすると, 次の 19 個の差集合が出来る。

$$0, 1, 3. \quad 0, 1, 5. \quad 0, 1, 6. \quad 0, 2, 3. \quad 0, 2, 5. \quad 0, 2, 6. \quad 0, 3, 4. \quad 0, 3, 5. \quad 0, 3, 6. \quad 0, 4, 5. \quad 0, 4, 6. \quad 1, 2, 4. \\ 1, 3, 5. \quad 1, 3, 6. \quad 1, 5, 6. \quad 2, 3, 5. \quad 2, 3, 6. \quad 2, 5, 6. \quad 3, 4, 5. \quad 3, 4, 6. \quad 4, 5, 6.$$

これらに平行移動と Frobenius 自己同型で換えると次の 4 個になる。

$$\text{No.1} \quad 1, 2, 4; \quad \text{No.2} \quad 0, 1, 3; \quad \text{No.3} \quad 1, 5, 6;$$

$$\text{No.4} \quad 0, 1, 5.$$

以上の中 No.1, No.2, No.3 は群で, No.4 は非群である。

その Hall 不変数は次のようになる。

	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64
No.1, No.2, No.3	7	0	0	0	936	0	9584	0	31836	0	3584	0	336	0	0	0	28
No.4	0	0	0	0	0	112	2492	9352	15869	9184	2492	168	42	0	12	0	0

したがって群と非群は差集合として非同型である。(この 2 種類は Hadamard 行列として非同型である。)

群 No.1, No.2, No.3 から生ずる差集合の自己同型群を求めると, それぞれ位数 672, 224, 224 の群である。さらに No.2 のものは, 中心の位数が 2, No.3 のものは中心の位数が 1. したがって, これらの差集合は互に非同型であることが分る。

同様のことを $s=4$ について行なうと, 195 個の差集合が得られる. 平行移動と Frobenius 自己同型で, それらは 18 個に分れる. うち 5 個は群, 13 個は非群である. これらは全て非同型であろうと信ぜられるが, おのれの自己同型群を計算するには莫大な時間が必要である.

15. 最後にひと言. 定理 5 に述べた方法が簡単で, しかも有効であるのに, 定理 4 を先に挙げたのは, そちらの方がより基本的であるからである. 事実, 定理 4 の方法はいわゆる distance-regular digraph にもそのままあてはまる.

文献

- [1] H. B. Mann, Addition Theorems, New York 1965
- [2] K. Yamamoto, Pacific J. 13 (1963), 337-352
- [3] R. J. Turyn, Pacific J. 15 (1965), 319-346
- [4] R. A. Liebler and R. A. Mena, preprint.