符号の複数のシェルがt-デザインをなす条件について

早稲田大学基幹理工学部　粟田　円佳
Madoka Awada
School of Fundamental Science and Engineering, Waseda University

1　はじめに

長さnの符号Cに対して，$C^{\perp} = C^{\sigma}$を満たす置換$\sigma \in S_n$が存在するとき，Cをisodual符号という．また，任意の符号語$c = (c_1, \ldots, c_n) \in C$に対し，

$$\mathrm{wt}(c) := |\{j \mid c_j \neq 0,\ 1 \leq j \leq n\}|,$$
$$C_\ell := \{c \in C \mid \mathrm{wt}(c) = \ell\},$$

と定義する．$\mathbb{F}_q$上の長さ$p+1$の拡大平方剰余符号$\widetilde{Q}_{q,p+1}$を考えよう．これはIsodual符号である．$\widetilde{Q}_{q,p+1}$の自己同型群は$PSL(2,p)$を含み，この群が2重可移群であることから，$(\widetilde{Q}_{q,p+1})_\ell$は，2-design構造をなす．最近Bonnecaze–Solé（2021）により，長さ42の拡大平方剰余符号の$(\widetilde{Q}_{2,42})_{10}$のみ3-design構造をなすことが発見された[5]．この3-designの存在性は，自己同型群などの手法を用いて説明できていない．また特別のℓにおいてt-値が上がる例は大変珍しく，その後発見された例は石川氏によるもの[6]，その他ごくわずかである．

本講究録ではまず，$\widetilde{Q}_{q,p+1}$のJacobi多項式と調和重さ多項式を用いて，$(\widetilde{Q}_{q,p+1})_\ell \cup ((\widetilde{Q}_{q,p+1})^{\perp})_\ell$が3-designをなすことを示す．次に，Bonnecaze–Solé が発見したものと同様に，自己同型群などの手法を用いて説明できないデザイン構造の候補となる無限系列を構成したため，その構成方法について詳述する．さらに，符号の3個以上のシェルの和集合をとることによって，t-値が上がることを示し，これを平方剰余符号の一般化であるm乗剰余符号に適用する．

本講究録では，第2節で符号理論を導入する．第3節で符号と組合せデザインの関係を述べ，第4節で符号がt-designであるかを判定できるJacobi多項式と調和重さ多項式を紹介する．第5節で主結果と証明の概略を紹介しよう．

2　符号理論

定義 2.1 (線形符号). 有限体$\mathbb{F}_q$上の(n,k)線形符号Cとは，ベクトル空間$\mathbb{F}_q^n$のk次元部分空間である．また，Cの元を，符号語と呼ぶ.

次に，線形符号を表現することができる生成行列を定義する：

定義 2.2 (生成行列)**.** 有限体 $\mathbb{F}_q$ 上の (n,k) 線形符号 C の生成行列 G とは，行ベクトルが C の基底となっている $k \times n$ 行列である．

生成行列の他に，パリティ検査行列を用いて線形符号を表現することもできる．これを定義するために，内積，双対符号を定義する：

定義 2.3 (内積，双対符号)**.** $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$，$y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$ に対して，内積を以下で定義する：

$$(x, y)_E = \sum_{i=1}^{n} x_i y_i.$$

また，C の双対符号を以下のように定義する：

$$C^{\perp,E} = \{y \in \mathbb{F}_q^n \mid (x, y)_E = 0, \forall x \in C\}.$$

$C = C^{\perp,E}$ のとき，C を自己双対符号と呼ぶ．

注意 2.4. $q = r^2$ のとき，内積としてエルミート内積を用いる場合もあり，$x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{r^2}^n$，$y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{r^2}^n$ に対して，以下で定義する：

$$(x, y)_H = \sum_{i=1}^{n} x_i {y_i}^r.$$

また，C のエルミート双対符号を以下のように定義する：

$$C^{\perp,H} = \{y \in \mathbb{F}_{r^2}^n \mid (x, y)_H = 0, \forall x \in C\}.$$

$C = C^{\perp,H}$ のとき，C をエルミート自己双対符号と呼ぶ．

定義 2.5 (パリティ検査行列)**.** 有限体 $\mathbb{F}_q$ 上の (n,k) 線形符号 C のパリティ検査行列 H とは，双対符号 $C^{\perp,*}$ $(*: E, H)$ の基底を行ベクトルに並べた $(n-k) \times n$ 行列である．

例 2.1. $\mathbb{F}_2$ 上の長さ 3 の符号 C を，

$$C = \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\},$$

とする．このとき，C の基底として $(1,1,0), (1,0,1)$ を選べるので，C はベクトル空間 $\mathbb{F}_2^3$ の 2 次元部分空間であり，$(3,2)$ 線形符号である．また，C の生成行列 G は以下のようになる：

$$G = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

ここで，C の双対符号 $C^{\perp,E}$ は，

$$C^{\perp,E} = \{(0,0,0), (1,1,1)\},$$

となるので，$C^{\perp,E}$ の基底として $(1,1,1)$ を選ぶことができ，$C^{\perp,E}$ のパリティ検査行列 H は以下のようになる：

$$H = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}.$$

次に，平方剰余符号を定義するため，巡回符号を定義する：

定義 2.6 (巡回符号). $\mathbb{F}_q$ 上の (n,k) 線形符号 C について，$(c_1,c_2,\ldots,c_{n-1},c_n)\in C$ ならば，$(c_2,c_3,\ldots,c_n,c_1)\in C$ のとき，C を巡回符号と呼ぶ．また，巡回符号 C は，$\mathbb{F}_q[x]/(x^n-1)$ のイデアル (f) に対応し，f は C の生成多項式と呼ばれる．

平方剰余符号は，巡回符号の特別な場合である：

定義 2.7 (平方剰余符号). p を，q が p を法として平方剰余となるような奇素数とする．符号 C の生成多項式 f が以下で与えられるとき，長さ p の巡回符号 C を，$\mathbb{F}_q$ 上の平方剰余符号という：

$$f:=\prod_{\ell\in(\mathbb{F}_p^*)^2}(x-\alpha^\ell)\ (\text{ここで, }\alpha\text{は位数 }p\text{ の元}).$$

ここで，線形符号の座標をひとつ増やすことで，より長い符号を構成することを考え，これを「拡大符号」と呼ぶ．平方剰余符号の拡大符号は以下の通りである：

定義 2.8 (拡大平方剰余符号). $\mathbb{F}_q$ 上の長さ p の平方剰余符号を $Q_{q,p}$ とすると，$\mathbb{F}_q$ 上の長さ $p+1$ の拡大平方剰余符号 $\widetilde{Q}_{q,p+1}$ は以下で定義される：

$$\widetilde{Q}_{q,p+1}=\{(c_1,\ldots,c_p,c_{p+1})\in\mathbb{F}_q^{p+1}\mid(c_1,\ldots,c_p)\in Q_{q,p},\sum_{i=1}^{p+1}c_i=0\}.$$

例 2.2. 2 は 7 を法として平方剰余となるので，$\mathbb{F}_2$ 上の長さ $p=7$ の平方剰余符号 $Q_{2,7}$ を考える．$\mathbb{F}_7^*=\mathbb{F}_7\setminus\{0\}$ とすると，

$$\begin{aligned}(\mathbb{F}_7^*)^2&=\{1^2,2^2,3^2,4^2,5^2,6^2\}\\&=\{1,4,2,2,4,1\}\\&=\{1,2,4\},\end{aligned}$$

より，$Q_{2,7}$ の生成行列 G は，$v_7=(1,1,0,1,0,0,0)$ の巡回シフトを行ベクトルとして並べた以下の行列となる：

$$G=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\end{bmatrix}.$$

また，G の各行の和はすべて $3\equiv1\pmod 2$ であるので，$Q_{2,7}$ の拡大符号 $\widetilde{Q}_{2,8}$ の生成行列 $\widetilde{G}$ は，G の 8 列目に 1 を並べた以下の行列となる：

$$\widetilde{G}=\begin{bmatrix}1&1&0&1&0&0&0&1\\0&1&1&0&1&0&0&1\\0&0&1&1&0&1&0&1\\0&0&0&1&1&0&1&1\end{bmatrix}.$$

平方剰余符号は，m 乗剰余符号の特別な場合であり，m 乗剰余符号は以下で定義される：

定義 2.9 (m 乗剰余符号). p を， $q \mid (p-1)$ を満たす素数とし， q を，p を法として m 乗剰余となる自然数とする．また，$\mathbb{F}_p^*$ を q 個のコセット A_i $(i = 0, 1, \ldots, q-1)$ に分割し，そのうち A_0 を，p を法として m 乗剰余となる数の集合と定義する．符号 C の生成多項式 f が以下で与えられるとき，長さ p の巡回符号 C を，$\mathbb{F}_q$ 上の m 乗剰余符号という：

$$f := \prod_{a \in A_0} (x - \alpha^a) \text{ (ここで, } \alpha\text{は位数 } p \text{ の元).}$$

したがって，平方剰余符号は，m 乗剰余符号の $m = 2$ の場合である．また，$\mathbb{F}_q$ 上の長さ p の m 乗剰余符号を，$\mathrm{PR}_q^m(p)$ と表す.

3　符号と組合せデザイン

3.1　符号と組合せデザイン

組合せデザインとは，集合族の対称性を図る指標である．符号理論では，t-design の t-値が大きい符号は誤り訂正能力が高いことが知られている．そのため，t-値が大きい符号を見つけることが，符号理論における大きな課題のひとつである．

以下，$X = \{1, 2, \ldots, n\}$, $\mathcal{B} \subset \binom{X}{k}$ として，t-design を定義する．

定義 3.1 (t-design). $\mathcal{D} = (X, \mathcal{B})$ が t-design (t-(n, k, λ)) であるとは，任意の $T \in \binom{X}{t}$ について，

$$\lambda = |\{B \in \mathcal{B} \mid T \subseteq B\}|$$

が一定に定まることである．

例 3.1.

$$\begin{cases} X = \{1, 2, 3, 4, 5, 6, 7\}, \\ \mathcal{B} = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{5, 6, 1\}, \{6, 7, 2\}, \{7, 1, 3\}\}. \end{cases}$$

とおく．このとき，任意の $T \in \binom{X}{2}$ について，

$$|\{B \in \mathcal{B} \mid T \subseteq B\}| = 1.$$

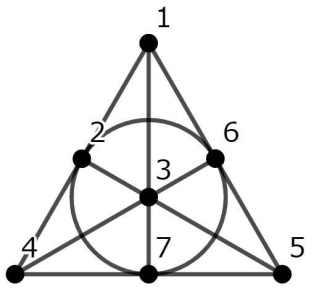
であるので，$(X, \mathcal{B})$ は 2-$(7, 3, 1)$ design である．

注意 3.2. 例 3.1 において，X は以下の図の頂点の集合，$\mathcal{B}$ は以下の図の線の集合に対応している．頂点を 2 つ選ぶと，それらを通る線が 1 本決まることからも，$(X, \mathcal{B})$ は 2-design であると判断することができる．

t-design は符号から構成できる．長さ n の符号 C，$c = (c_1, c_2, \ldots, c_n) \in C$ に対し，

$$\mathrm{supp}(c) := \{i \mid c_i \neq 0\},$$
$$\mathcal{B}(C_\ell) := \{\mathrm{supp}(c) \mid c \in C_\ell\},$$

とする．$(X, \mathcal{B}(C_\ell))$ が t-design であるとき，C_ℓ が t-design であるという．



例 3.2. H を，以下の生成行列からなるハミング $[7,4]$ 符号とする：

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

ここで，$H_3 = \{c \in C \mid \mathrm{wt}(c) = 3\}$ とおくと，H_3 は以下の符号語からなる：

$$\begin{array}{ll} (1,1,0,1,0,0,0), & (1,0,0,0,1,1,0), \\ (0,1,1,0,1,0,0), & (0,1,0,0,0,1,1), \\ (0,0,1,1,0,1,0), & (1,0,1,0,0,0,1), \\ (0,0,0,1,1,0,1). & \end{array}$$

よって，

$$\begin{cases} X = \{1,2,3,4,5,6,7\}, \\ \mathcal{B}(H_3) = \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}\}, \end{cases}$$

が得られるが，$(X, \mathcal{B}(H_3))$ は例 3.1 の $(X, \mathcal{B})$ に一致するので，$(X, \mathcal{B}(H_3))$ は 2-$(7,3,1)$ design である．

3.2 拡大平方剰余符号から得られる組合せデザイン

$\mathbb{F}_q$ 上の長さ $p+1$ の拡大平方剰余符号 $\widetilde{Q}_{q,p+1}$ から得られる組合せデザインについて，以下の事実が知られている．

(1) $\ell \in \mathbb{N}$ に対して，$(\widetilde{Q}_{q,p+1})_\ell$ $(\neq \emptyset)$ は 2-design である．

(2) $p \equiv -1 \pmod 4$ のとき，$\ell \in \mathbb{N}$ に対して，$(\widetilde{Q}_{q,p+1})_\ell$ $(\neq \emptyset)$ は 3-design である．

(3) $p \equiv 1 \pmod 4$ のとき，$(\widetilde{Q}_{q,p+1})_\ell$ は一般に 3-design ではない．

これらは，次のように導かれる．$\widetilde{Q}_{q,p+1}$ の座標を $\{1,\ldots,p-1,p,\infty\}$ とラベルづけし，$X = \{1,\ldots,p-1,p,\infty\}$ とおく．このとき，

(0) $\mathrm{Aut}(\widetilde{Q}_{q,p+1}) \supset PSL_2(p)$，ここで，
$\mathrm{Aut}(C) = \{\sigma \in S_n \mid C^\sigma = C\}$, $C^\sigma = \{(c_{\sigma(1)},\ldots,c_{\sigma(n)}) \mid (c_1,\ldots,c_n) \in C\}$.

(1) $PSL_2(p)$ は 2-homogeneous である．
（つまり，$\forall A, B \in \binom{X}{2}$, $\exists \sigma \ni PSL_2(p)$ $\sigma(A) = B$.）
よって，$\ell \in \mathbb{N}$ に対して, $(\widetilde{Q}_{q,p+1})_\ell$ $(\neq \emptyset)$ は 2-design である．

(2) $p \equiv -1 \pmod 4$ のとき，$PSL_2(p)$ は 3-homogeneous である．
（つまり，$\forall A, B \in \binom{X}{3}$, $\exists \sigma \ni PSL_2(p)$ $\sigma(A) = B$.）
よって，$p \equiv -1 \pmod 4$ のとき，$\ell \in \mathbb{N}$ に対して, $(\widetilde{Q}_{q,p+1})_\ell$ $(\neq \emptyset)$ は 3-design である．

(3) $p \equiv 1 \pmod 4$ のとき，$PSL_2(p)$ は 3-homogeneous ではなく，以下が成り立つ：
$\exists \theta \in X$

$$\binom{X}{3} = PSL_2(p)\{\infty, 0, -1\} \sqcup PSL_2(p)\{\infty, 0, \theta\}.$$

ここで，$|PSL_2(p)\{\infty, 0, -1\}| = |PSL_2(p)\{\infty, 0, \theta\}|$.
よって，$p \equiv 1 \pmod 4$ のとき，$(\widetilde{Q}_{q,p+1})_\ell$ $(\neq \emptyset)$ は一般に 3-design ではない．

4 Jacobi 多項式と調和重さ多項式

Jacobi 多項式，調和重さ多項式はいずれも，符号が t-design であるかどうかを判定することができる．

定義 4.1 (Jacobi 多項式). C を $\mathbb{F}_q$ 上の長さ n の符号とし， $T \subset [n] := \{1, \ldots, n\}$ とする．このとき，Jacobi 多項式を以下のように定義する [7]:

$$J_{C,T}(w, z, x, y) := \sum_{c \in C} w^{m_0(c)} z^{m_1(c)} x^{n_0(c)} y^{n_1(c)},$$

ただし，
$$\begin{aligned} m_0(c) &= |\{j \in T \mid c_j = 0\}|, \\ m_1(c) &= |\{j \in T \mid c_j \neq 0\}|, \\ n_0(c) &= |\{j \in [n] \setminus T \mid c_j = 0\}|, \\ n_1(c) &= |\{j \in [n] \setminus T \mid c_j \neq 0\}|. \end{aligned}$$

任意の $T \subset [n]$ $(|T| = t)$ に対して，$J_{C,T} + J_{C^{\perp,*},T}$ $(* : E, H)$ が一意的に定まるとき，任意の $\ell \in \mathbb{N}$ に対して $C_\ell \cup (C^{\perp,*})_\ell$ $(* : E, H)$ は t-design となる．

定義 4.2 (離散調和関数). $\Omega = [n]$, $X = 2^\Omega$, $X_k = \binom{X}{k}$ に対し，

$$\mathbb{R}X = \{\sum_{x \in X} c_i x \mid \forall i, c_i \in \mathbb{R}\}, \quad \mathbb{R}X_k = \{\sum_{x \in X_k} c_i x \mid \forall i, c_i \in \mathbb{R}\},$$

$$f = \sum_{z \in X_k} f(z) z, \quad \widetilde{f}(u) = \sum_{z \in X_k, z \subset u} f(z), \quad \gamma(z) = \sum_{y \in X_{k-1}, y \subset z} y,$$

と定義する．任意の $z \in X_k$，$k \in [n]$ に対し，離散調和関数の空間を以下のように定義する：

$$\mathrm{Harm}_k = \ker(\gamma|_{\mathbb{R}X_k}).$$

定義 4.3 (調和重さ多項式,[4]). $\mathbb{F}_q$ 上の長さ n の符号 C，$f \in \mathrm{Harm}_k$ に対し， 調和重さ多項式を以下のように定義する．

$$w_{C,f}(x,y) = \sum_{c \in C} \widetilde{f}(c) x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)}.$$

定理 4.1 ([3]). C_ℓ $(\neq \emptyset)$ が t-design であることと，任意の $f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)} (1 \leq k \leq t)$ について $\sum_{c \in C_\ell} \widetilde{f}(c) = 0$ が成り立つことは同値である．

任意の $f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)}$ に対して，$w_{C,f} + w_{C^{\perp,*},f} = 0$ $(* : E, H)$ のとき，任意の $\ell \in \mathbb{N}$ に対して $C_\ell \cup (C^{\perp,*})_\ell$ $(* : E, H)$ は t-design となる．

5 主結果 – 符号の複数のシェルが t-design をなす条件 –

5.1 拡大平方剰余符号と t-design

定理 5.1 ([1]). C を $\mathbb{F}_q$ 上の長さ n の isodual 符号，$X := \{1, \ldots, n\}$，$G = \mathrm{Aut}(C)$，$\sigma \in S_n$ を $C^{\perp,*} = C^\sigma$ $(* : E, H)$ を満たす置換とする．また， G が $\binom{X}{t}$ に作用し， G が

$$\binom{X}{t} = GT_1 \sqcup GT_2 \quad （ただし， \ (GT_1)^\sigma = GT_2）$$

のように軌道分解されるとする．このとき，以下が成り立つ．

(1) 任意の $T \in \binom{X}{t}$ について, $J_{C,T} + J_{C^{\perp,*},T}$ $(* : E, H)$ が一意に定まる．

(2) 任意の次数 t の離散調和関数 f に対して，$w_{C,f} + w_{C^{\perp,*},f} = 0$ $(* : E, H)$.

Isodual 符号として，$\mathbb{F}_q$ 上の長さ $p+1$ の拡大平方剰余符号 $\widetilde{Q}_{q,p+1}$ を考えると，以下の系が得られる：

系 5.1 ([1]). p を，q が p を法として平方剰余となるような奇素数とし，$\widetilde{Q}_{q,p+1}$ を $\mathbb{F}_q$ 上の長さ $p+1$ の拡大平方剰余符号とする．このとき，$\ell \in \mathbb{N}$ に対して,

$$(\widetilde{Q}_{q,p+1})_\ell \cup ((\widetilde{Q}_{q,p+1})^{\perp,*})_\ell \ (\neq \emptyset), \ (* : E, H)$$

は 3-design である．

補題 5.1 ([1]). p を奇素数とし，$\widetilde{Q}_{r^2,p+1}$ を $\mathbb{F}_{r^2}$ 上の長さ $p+1$ の拡大平方剰余符号とする．$p \equiv 1 \pmod 4$ かつ r が p を法として平方剰余でないとき，$\widetilde{Q}_{r^2,p+1}$, $\widetilde{Q}_{r^2,p+1}^{\perp,H}$ の生成行列は、$\widetilde{Q}_{r^2,p+1}$ の部分符号の生成行列 G を用いて，以下のように与えられる：

$$\begin{array}{c|c} \begin{array}{cccc} 0 & 1 & \cdots & p-1 \end{array} & \infty \\ \hline G & \begin{array}{c} 0 \\ \vdots \\ 0 \end{array} \\ \hline \begin{array}{cccc} 1 & 1 & \cdots & 1 \end{array} & k \end{array}.$$

ここで，それぞれの生成行列における k の値を k_1, k_2 とすると，

(i) $k_1 = k_2 = 1$ ($p \equiv -1 \pmod r$ のとき),

(ii) $k_1 = -m$, $k_2 = 1$ ($p \equiv m \pmod r$, $m \neq -1$ のとき).

したがって，次が得られる：

$$\begin{aligned}\forall \ell \in \mathbb{N},\ \mathcal{B}((\widetilde{Q}_{r^2,p+1})_\ell) &:= \{\mathrm{supp}(x) \mid x \in (\widetilde{Q}_{r^2,p+1})_\ell\} \\ &= \{\mathrm{supp}(x) \mid x \in (\widetilde{Q}^{\perp,H}_{r^2,p+1})_\ell\} =: \mathcal{B}((\widetilde{Q}^{\perp,H}_{r^2,p+1})_\ell).\end{aligned}$$

第 3.2 節の自己同型群の可移性の議論から，$p \equiv -1 \pmod 4$ のとき，$\ell \in \mathbb{N}$ に対して，$(\widetilde{Q}_{q,p+1})_\ell$ $(\neq \emptyset)$ は 3-design であることが導かれる．しかし，系 5.1 と補題 5.1 から導かれる次の定理は，この議論から従わず，また，多くの場合が Assmus–Mattson の定理 [8] からも従わない：

定理 5.2 ([1]). p を奇素数とし，$\widetilde{Q}_{r^2,p+1}$ を $\mathbb{F}_{r^2}$ 上の長さ $p+1$ の拡大平方剰余符号とする．このとき，$p \equiv 1 \pmod 4$ かつ r が p を法として平方剰余でないとき，$\ell \in \mathbb{N}$ に対して，$(\widetilde{Q}_{r^2,p+1})_\ell$ $(\neq \emptyset)$ は 3-design である．

系 5.2 ([1]). p を奇素数とし，$\widetilde{Q}_{r^2,p+1}$ を $\mathbb{F}_{r^2}$ 上の長さ $p+1$ の拡大平方剰余符号とする．

(1) $p \equiv -3 \pmod 8$ のとき，$\ell \in \mathbb{N}$ に対して，$(\widetilde{Q}_{4,p+1})_\ell$ $(\neq \emptyset)$ は 3-design である．

(2) $p \equiv 5 \pmod{12}$ のとき，$\ell \in \mathbb{N}$ に対して，$(\widetilde{Q}_{9,p+1})_\ell$ $(\neq \emptyset)$ は 3-design である．

5.2 m 乗剰余符号と t-design

定理 5.3 ([2]). C を $\mathbb{F}_q$ 上の長さ n の符号，$X := \{1, \dots, n\}$ とし，G を $\mathrm{Aut}(C)$ の部分群とする．また，G が $\binom{X}{t}$ に作用し，G が

$$\binom{X}{t} = GT_1 \sqcup \cdots \sqcup GT_s$$

のように s 個の軌道に分解されるとする．ここで，$\sigma \in S_n$ は，$(GT_i)^\sigma = GT_{i+1}$ $(1 \le i \le s-1)$, $(GT_s)^\sigma = GT_1$, $o(\sigma) = s$ を満たす．このとき，以下が成り立つ．

(1) 任意の $T \in \binom{X}{t}$ について，$J_{C,T} + J_{C^\sigma,T} + \cdots + J_{C^{\sigma^{s-1}},T}$ が一意に定まる．

(2) 任意の次数 t の離散調和関数 f に対して，$w_{C,f} + w_{C^\sigma,f} + \cdots + w_{C^{\sigma^{s-1}},f} = 0$.

$\mathbb{F}_q$ 上の長さ p の m 乗剰余符号のシェル $(\mathrm{PR}_q^m(p))_\ell$ は，1-design であることが一般に知られているが，符号 C として $\mathrm{PR}_q^m(p)$ を考えると，以下の系が得られる：

系 5.3 ([2]). $\mathrm{PR}_q^m(p)$ を $\mathbb{F}_q$ 上の長さ p の m 乗剰余符号とする．このとき，$\ell \in \mathbb{N}$ に対して，

$$(\mathrm{PR}_q^m(p))_\ell \cup (\mathrm{PR}_q^m(p))_\ell^\sigma \cup \cdots \cup (\mathrm{PR}_q^m(p))_\ell^{\sigma^{s-1}} (\neq \emptyset)$$

は 2-design である．

参考文献

[1] M. Awada, Infinite series of 3-designs in the extended quadratic residue code, submitted.

[2] M. Awada, R. Ishikawa, T. Miezaki, and Y. Tanaka, A criterion for determining whether multiple shells support a t-design, submitted.

[3] M. Awada, T. Miezaki, A. Munemasa, and H. Nakasora, A note on t-designs in isodual codes, *Finite Fields and Their Applications* **95** (2024), 102366.

[4] C. Bachoc, Harmonic weight enumerators of nonbinary codes and MacWilliams identities, *Codes and association schemes* (Piscataway, NJ, 1999), 1-23, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 56, Amer. Math. Soc., Providence, RI, 2001.

[5] A. Bonnecaze and P. Solé, The extended binary quadratic residue code of length 42 holds a 3-design, *J. Combin. Des.* **29** (2021), no. 8, 528–532.

[6] R. Ishikawa, Exceptional designs in some extended quadratic residue codes, *J. Combin. Des.* 31 (2023), no. 10, 496–510.

[7] M. Ozeki, On the notion of Jacobi polynomials for codes. *Math. Proc. Cambridge Philos. Soc.* **121** (1997), no. 1, 15–30.

[8] K. Tanabe, A new proof of the Assmus-Mattson theorem for non-binary codes, *Des. Codes Cryptogr.* **22** (2001), no. 2, 149–155.