数理解析研究所講究録 第2086巻 2018年 29-44

Construction of strongly regular Cayley graphs based on three-valued Gauss periods

–3 値のガウス周期に基づく強正則ケーリーグラフの構成について–

熊本大学 教育学部　　籾原　幸二*
Koji Momihara
Faculty of Education, Kumamoto University

概 要

この論文では, 3 つの値を取るガウス周期の新しい系列を発見するとともに, それに基づく強正則ケーリーグラフの新たな構成法を与える. 特に, 今回得られた結果は, [3] の結果のある種の一般化としてみなすことができ, 強正則グラフの新たな無限系列を与えるものである. この論文は, 論文 [21] の要約である.

1　導入

この論文では, いくつか証明を省く命題があるが, 詳しくは論文 [21] を参照していただきたい.

v 頂点上の k-正則単純グラフ Γ が, 以下の条件を満たすとき, パラメータ (v,k,λ,μ) を持つ強正則グラフであるという: 任意の 2 頂点 x,y に対し,

$$|\{z\in V(\Gamma):(x,z),(y,z)\in E(\Gamma)\}|=\begin{cases}\lambda, & (x,y)\in E(\Gamma)\text{ のとき},\\ \mu, & (x,y)\notin E(\Gamma)\text{ のとき}.\end{cases}$$

ある k-正則グラフが強正則であるための必要十分条件は, そのグラフの隣接行列の固有値が, k 以外にちょうど 2 種類となることである [4, Theorem 9.1.2].

この論文では, ケーリーグラフのみ扱うこととする. G を有限可換群とし, D を逆元について閉じた $G\setminus\{0_G\}$ の部分集合とする. ここで, 0_G は G の単位元とする. 今, ケーリーグラフ $\mathrm{Cay}(G,D)$ を以下のように定める: 頂点は G の要素と同一視し, $x-y\in D$ のときのみ, 2 つの頂点 x,y が隣接するものとする. D を連結集合とよぶ. $\mathrm{Cay}(G,D)$ の固有値は, $\psi(D)$, $\psi\in\widehat{G}$ で与えられる. ここで, $\widehat{G}$ は G の指標群とする. 先ほどの強正則グラフの固有値に関する特徴付けより, ケーリーグラフ $\mathrm{Cay}(G,D)$ が強正則グラフであるためには, $\psi(D)$, $\psi\in\widehat{G}\setminus\{\psi_0\}$ が

[1] 〒 860-8555, 熊本県熊本市黒髪 2-40-1, 熊本大学教育学部, Email: momihara@educ.kumamoto-u.ac.jp
この研究は, 科学研究費補助金 (若手研究 (B) 17K14236, 基盤研究 (B) 15H03636) の補助を受けています.

ちょうど 2 つとなることが必要十分である．ただし，ψ_0 は単位指標とする．強正則ケーリーグラフの基本的性質については，[19] を参照していただきたい．

今回，強正則ケーリーグラフの構成問題を扱うが，最も効果的な方法の一つとして知られているのが，有限体の乗法部分群を利用することである．q を素数ベキとし，$\mathbb{F}_q$ を位数 q の有限体を表す．ω を $\mathbb{F}_q$ の原始根とし，N を $q-1$ を割る自然数とする．今，

$$C_i^{(N,q)} = \omega^i \langle \omega^N \rangle,\ 0 \leq i \leq N-1$$

と定める．これらは，しばしば位数 N の円分剰余類と呼ばれる．今回得られた強正則グラフは，端的に言えば，いくつかの円分剰余類の和集合を連結集合に持つケーリーグラフとして実現される．これまでに知られている，円分剰余類を用いたいくつか構成法については，[6, 10, 12, 14, 16, 20] およびその参考文献を参照していただきたい．

一方，有限体上の強正則グラフは，有限幾何のいくつかの問題とも関連している．特に，m-ovoid や i-tight set と呼ばれる有限幾何学における構造があるが，それらは有限体上の 2 次形式の零点の部分集合であり，射影空間で捉えたとき，特別な超平面らとの交差数がちょうど 2 種類となることが知られている．射影空間の次元や 2 次形式の型によって，それらの集合を連結集合にもつ有限体上のケーリーグラフが強正則となることが知られている．これまでの結果については [1, 2, 5, 7, 9, 11, 17, 18, 24] を参照していただきたい．特に，最近，Bamberg, Lee, Xiang および著者は，論文 [3] において，elliptic 型の 2 次形式の零点集合の部分集合としての $\frac{q+1}{2}$-ovoid(および対応する強正則グラフ) を構成した．これは，一般化四角形の双対性を利用すれば，Hermitian 曲面の hemisystem と呼ばれる幾何構造と同値であることが知られている．著者たちは，特に $\mathbb{F}_{q^6}$ 上で，位数 $4(q^2+q+1)$ の円分剰余類を用いて構成を行ったが，その背後には，2 つの値を持つガウス周期と対応する Singer 差集合の分割があり，この論文では，この手法が 3 つの値をもつガウス周期の場合にも適用できることを概説する．特に，以下の 2 つの強正則ケーリーグラフの無限系列を得た．

定理 1.1. *以下の場合に，パラメータ $(q^6, r(q^3+1), q^3+r^2-3r, r^2-r)$ を持つ，$(\mathbb{F}_{q^6}, +)$ 上の強正則ケーリーグラフが存在する:*

(i) $M = 3$ かつ $q \equiv 7 \pmod{24}$,

(ii) $M = 7$ かつ $q \equiv 11, 51 \pmod{56}$.

ここで，$r = M(q^2-1)/2$ とする．

上定理において，$M = 1$ かつ $q \equiv 3 \pmod 4$ の場合にも，強正則グラフが得られるが，この場合は [3] で扱われた．よって，今回の我々の結果は，[3] の結果の一般化であるとみなすことができる．

2　ガウス周期と有限体上のケーリーグラフ

有限体 $\mathbb{F}_q$ の乗法的指標 χ と加法的標準指標 $\psi_{\mathbb{F}_q}$ に対し, 指標和

$$G_q(\chi)=\sum_{x\in\mathbb{F}_q^*}\chi(x)\psi_{\mathbb{F}_q}(x)$$

をガウス和と呼ぶ. ガウス和の基本的性質, 計算方法に関しては [15] を参照されたい.

有限体 $\mathbb{F}_{q^m}$ の位数 N のガウス周期とは,

$$\psi_{\mathbb{F}_{q^m}}(C_i^{(N,q^m)}):=\sum_{x\in C_i^{(N,q^m)}}\psi_{\mathbb{F}_{q^m}}(x),\ \ 0\le i\le N-1$$

で定義される N 個の数値のことである. 指標の直交性より, 位数 N のガウス周期は, ガウス和の線形結合で表現される:

$$\psi_{\mathbb{F}_{q^m}}(C_i^{(N,q^m)})=\frac{1}{N}\sum_{j=0}^{N-1}G_{q^m}(\chi_N^j)\chi_N^{-j}(\omega^i),\ \ 0\le i\le N-1. \tag{2.1}$$

ここで, χ_N は $\mathbb{F}_{q^m}$ の位数 N の乗法的指標とする. また, ω は, $\mathbb{F}_{q^m}$ の原始根とする.

定理 2.1. ([26, Theorem 1]) χ を $\mathbb{F}_{q^m}$ の非自明な乗法的指標, χ' をその $\mathbb{F}_q$ への制限とする. L を $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ の個別代表系で, 特に $\mathrm{Tr}_{q^m/q}$ による像が 0 または 1 となるものから成るとする. (ここで, $\mathrm{Tr}_{q^m/q}$ は $\mathbb{F}_{q^m}$ から $\mathbb{F}_q$ へのトレース関数とする.) 今, L を

$$L_0=\{x\in L:\mathrm{Tr}_{q^m/q}(x)=0\},\quad L_1=\{x\in L:\mathrm{Tr}_{q^m/q}(x)=1\}$$

と分解とする. このとき, 以下が成立する.

$$\sum_{x\in L_1}\chi(x)=\begin{cases}G_{q^m}(\chi)/G_q(\chi'), & \chi'\text{ が非自明のとき},\\ -G_{q^m}(\chi)/q, & \chi'\text{ が自明のとき}.\end{cases}$$

集合 $S=\{i\,(\mathrm{mod}\ \frac{q^m-1}{q-1}):\omega^i\in L_0\}$ は, Singer 差集合と呼ばれる. ここで, $|S|=(q^{m-1}-1)/(q-1)$ である. $N\,|\,(q^m-1)/(q-1)$ であるとき, χ_N の $\mathbb{F}_q$ への制限は自明となる. この場合, 式 (2.1) と定理 2.1 より, 以下を得る.

$$\begin{aligned}\psi_{\mathbb{F}_{q^m}}(C_i^{(N,q^m)})&=-\frac{1}{N}+\frac{1}{N}\sum_{j=1}^{N-1}G_{q^m}(\chi_N^j)\chi_N^{-j}(\omega^i)\\&=-\frac{q^m-1}{N(q-1)}+\frac{q}{N}\sum_{j=0}^{N-1}\sum_{\ell\in S}\chi_N^j(\omega^{\ell-i}).\end{aligned}\tag{2.2}$$

$\overline{S_N}$ を S の N を法とする制限 (多重集合) とする. このとき, 群環 $\mathbb{Z}[\mathbb{Z}_N]$ の元と同一視し,

$$\overline{S_N}=c_0[0]+c_1[1]+\cdots+c_{N-1}[N-1]\in\mathbb{Z}[\mathbb{Z}_N],\ \ c_i\in\mathbb{Z}$$

とする．また，

$$F_N = \{c_i : 0 \le i \le N-1\} \tag{2.3}$$

を $x \in \mathbb{Z}_N$ の $\overline{S_N}$ における重複度の集合とする．さらに，

$$I_\beta = \{i \in \mathbb{Z}_N : c_i = \beta\},\ \beta \in F_N \tag{2.4}$$

とおく．このとき，

$$\overline{S_N} = \sum_{\beta \in F_N} \beta I_\beta \in \mathbb{Z}[\mathbb{Z}_N]. \tag{2.5}$$

が成り立つ．(2.2) から続けて，

$$\psi_{\mathbb{F}_{q^m}}(C_i^{(N,q^m)}) = -\frac{q^m-1}{N(q-1)} + q\beta, \tag{2.6}$$

を得る．特に，$\beta \in F_N$ は $i \in I_\beta$ で定まる．よって，ガウス周期は $\overline{S_N}$ から計算できる．

3　3つの値をとるガウス周期

3.1　3つの値をとるガウス周期の基本

Schmidt と White [25] は，ガウス周期 $\psi_{\mathbb{F}_{q^m}}(C_i^{(N,q^m)})$, $i = 0, 1, \ldots, N-1$ が，2つの値を取る場合について研究を行った．彼らは，q, m, N に関する2つの系列と11個の散在的な例を発見し，また，それらに限るという予想を与えている．論文 [3, 22, 23] では，彼らの結果に基づき，強正則ケーリーグラフを構成した．

また，[25] の研究の自然な一般化として，著者は Feng, Xiang と共に，3つの値をとるガウス周期の分類について研究を行った [13].

q^m を素数ベキとし，$N > 2$ を $(q^m-1)/(q-1)$ を割る正整数とする．ガウス周期 $\psi_{\mathbb{F}_{q^m}}(C_i^{(N,q^m)})$, $0 \le i \le N-1$ がちょうど3つの値 $\alpha_1, \alpha_2, \alpha_3$ を取るとし，特にそれらが，等差数列を成すと仮定する: $\alpha_1 - \alpha_2 = \alpha_2 - \alpha_3 = t > 0$. 式 (2.6) と定義 (2.3) より，

$$F_N = \left\{ (\beta_i :=) \frac{\alpha_i}{q} + \frac{q^m-1}{qN(q-1)} : i = 1, 2, 3 \right\} \tag{3.1}$$

を得る．このとき，$\beta_1, \beta_2, \beta_3$ はまた等差数列を成す．ここで，単純のため，$I_i := I_{\beta_i}$ と書く．ただし，I_{β_i} は (2.4) で定義されている．このとき，I_i の濃度は以下で与えられる．

補題 3.1. ([13, Lemma 2.5]) I_j の濃度について以下が成立する．

$$\begin{aligned}
|I_1| &= \frac{N(\alpha_2^2 - \alpha_2 t + k) + 2\alpha_2 - k - t + 1}{2t^2}, \\
|I_2| &= \frac{N(t^2 - \alpha_2^2 - k) - 1 - 2\alpha_2 + k}{t^2}, \\
|I_3| &= \frac{N(\alpha_2^2 + \alpha_2 t + k) + 2\alpha_2 - k + t + 1}{2t^2},
\end{aligned}$$

ここで，$k := (q^m-1)/N$ とする．

ω を $\mathbb{F}_{q^m}$ の原始根とし, χ を指数 N の非自明な乗法的指標とする. このとき, 定理 2.1 と式 (2.5) より,

$$G_{q^m}(\chi) = q \sum_{i \in \overline{S_N}} \chi(\omega^i) = q \sum_{j=1,2,3} \beta_j \sum_{i \in I_j} \chi(\omega^i) \tag{3.2}$$

を得る. また, 式 (3.1) より, 式 (3.2) の右辺は

$$\sum_{j=1,2,3} \alpha_j \sum_{i \in I_j} \chi(\omega^i) = t \left(2 \sum_{i \in I_1} \chi(\omega^i) + \sum_{i \in I_2} \chi(\omega^i) \right) \tag{3.3}$$

と変形される.

論文 [13] では, 以下 2 つの等差数列をなす 3 値をとるガウス周期の無限系列が得られた:

$$m = 6,\ N = (q^3 - 1)/(q - 1), \tag{3.4}$$

$$m = 3,\ N = (q^3 - 1)/(3(q - 1)),\ q \equiv 1 \pmod 3. \tag{3.5}$$

一方, 上の 2 つの系列以外にも数多くの散在的な例が発見されている [13, Example 4.4, Table 1].

3.2 3 値をとるガウス周期の例

ω を $\mathbb{F}_{q^3}$ の原始根とし, M を $(q^3 - 1)/(q - 1)$ を割る正整数とし, $N = \frac{q^3-1}{M(q-1)}$ とおく.

補題 3.2. 異なる全ての $j_1, j_2, j_3 \in \{0, 1, \ldots, M-1\}$ に対し, $\omega^{j_1 N}, \omega^{j_2 N}, \omega^{j_3 N}$ が $\mathbb{F}_q$ 上線形独立と仮定する. このとき, ガウス周期 $\psi_{\mathbb{F}_{q^3}}(C_i^{(N,q^3)})$, $i = 0, 1, \ldots, N-1$ はちょうど 3 つの値 $-M + 2q, -M + q, -M$ を取る.

証明: $\omega^a \in \mathbb{F}_{q^3}^*$ とする. 3 つもしくはそれ以上の $j \in \{0, 1, \ldots, M-1\}$ に対し, $\mathrm{Tr}_{q^3/q}(\omega^a \omega^{jN}) = 0$ は成立しない. 事実, もし, ある異なる $j_1, j_2, j_3 \in \{0, 1, \ldots, M-1\}$ に対し,

$$\mathrm{Tr}_{q^3/q}(\omega^a \omega^{j_1 N}) = \mathrm{Tr}_{q^3/q}(\omega^a \omega^{j_2 N}) = \mathrm{Tr}_{q^3/q}(\omega^a \omega^{j_3 N}) = 0$$

が成立したとき, $\omega^{j_1 N}, \omega^{j_2 N}, \omega^{j_3 N}$ は線形独立より, すべての $x \in \mathbb{F}_{q^3}$ に対し, $\mathrm{Tr}_{q^3/q}(\omega^a x) = 0$ が成立する. これは不可能である. よって,

$$\begin{aligned}
\psi_{\mathbb{F}_{q^3}}(\omega^a C_0^{(N,q^3)}) &= \sum_{j=0}^{M-1} \psi_{\mathbb{F}_q}(\mathrm{Tr}_{q^3/q}(\omega^a \omega^{jN}) \mathbb{F}_q^*) \\
&= \begin{cases}
-M + 2q, & \text{ちょうど 2 つの } j \in \{0, 1, \ldots, M-1\} \text{ に対し,} \\
& \quad \mathrm{Tr}_{q^3/q}(\omega^a \omega^{jN}) = 0 \text{ が成り立つとき,} \\
-M + q, & \text{ちょうど 1 つの } j \in \{0, 1, \ldots, M-1\} \text{ に対し,} \\
& \quad \mathrm{Tr}_{q^3/q}(\omega^a \omega^{jN}) = 0 \text{ が成り立つとき,} \\
-M, & \mathrm{Tr}_{q^3/q}(\omega^a \omega^{jN}) = 0 \text{ となる } j \text{ が存在しないとき.}
\end{cases}
\end{aligned}$$

□

いま, $\alpha_1 = -M+2q$, $\alpha_2 = -M+q$, $\alpha_3 = -M$ とおく. このとき, 式 (3.1) より, $\beta_1 = 2$, $\beta_2 = 1$, $\beta_3 = 0$ を得る.

$$I_j := \{i \pmod N : 0 \le i \le N-1, \psi_{\mathbb{F}_{q^3}}(C_i^{(N,q^3)}) = \alpha_j\},\ j = 1,2,3 \tag{3.6}$$

と定めると, 補題 3.1 より,

$$|I_1| = \frac{M-1}{2}, |I_2| = q - M + 2, |I_3| = \frac{q^2+q+1}{M} - q + \frac{M-3}{2}.$$

さらに, 式 (2.5) より, Singer 差集合 $S = \{i \pmod{q^2+q+1} : \mathrm{Tr}_{q^3/q}(\omega^i) = 0\}$ の N を法とする制限 (多重集合) は以下のように与えられる:

$$\overline{S_N} = I_1 \cup I_1 \cup I_2 \subseteq \mathbb{Z}_N. \tag{3.7}$$

系 3.3. ([13, Section 4.3]) q を $q \equiv 1 \pmod 3$ なる素数べキとし, $N = (q^2+q+1)/3$ とする. このとき, ガウス周期 $\psi_{\mathbb{F}_{q^3}}(C_i^{(N,q^3)})$, $i = 0,1,\ldots,N-1$ はちょうど 3 つの値 $-3+2q, -3+q, -3$ をとる.

証明: ω^N の最小多項式の次数は 3 である. よって, $1, \omega^N, \omega^{2N}$ は, $\mathbb{F}_q$ 上線形独立である. よって, 補題 3.2 より, 主張が成立する. □

この結果は, 既値の結果 (3.5) を再証明したことになる. 以下に, 3 値をとるガウス周期の新しい系列を与える.

系 3.4. q を $q \equiv 2$ または $4 \pmod 7$ なる奇素数べキとし, $N = (q^2+q+1)/7$ とおく. このとき, ガウス周期 $\psi_{\mathbb{F}_{q^3}}(C_i^{(N,q^3)})$, $i = 0,1,\ldots,N-1$ はちょうど 3 つの値 $-7+2q, -7+q, -7$ をとる.

証明: 各 ω^{jN}, $j = 1,2,\ldots,6$ の最小多項式の次数は 3 である. よって, $1, \omega^{jN}, \omega^{2jN}$ は $\mathbb{F}_q$ 上線形独立である. これは, $j' \equiv 2j \pmod 7$ としたとき, $\omega^{2jN}\mathbb{F}_q^* = \omega^{j'N}\mathbb{F}_q^*$ より, $1, \omega^{jN}, \omega^{j'N}$ は, $\mathbb{F}_q$ 上線形独立である

次に, 全ての $j = 1,2,\ldots,6$ に対し, $1, \omega^{jN}, \omega^{3jN}$ が $\mathbb{F}_q$ 上線形独立であることを示す. これが証明されれば, 上と同様, $j' \equiv 3j \pmod 7$ としたとき, $1, \omega^{jN}, \omega^{j'N}$ が線形独立となる. 今, $1, \omega^{jN}, \omega^{3jN}$ が線形従属であるとすると, ある $a, b \in \mathbb{F}_q^*$ が存在して, $\omega^{3jN} + a\omega^{jN} + b = 0$ と書ける. このとき $f(x) = x^3 + ax + b \in \mathbb{F}_q[x]$ は ω^{jN} の最小多項式である. $\omega^{qjN}, \omega^{q^2jN}$ は $f(x)$ の根であるので, $x^3 + ax + b = (x - \omega^{jN})(x - \omega^{qjN})(x - \omega^{q^2jN})$ となる. 両辺の x^2 の係数を比較して, $\omega^{jN} + \omega^{qjN} + \omega^{q^2jN} = 0$ を得る. $q \equiv 2$ か $4 \pmod 7$ に応じて, $1 + \omega^{j\frac{q^3-1}{7}} + \omega^{3j\frac{q^3-1}{7}} = 0$ または $1 + \omega^{2j\frac{q^3-1}{7}} + \omega^{3j\frac{q^3-1}{7}} = 0$ を得る. $q \equiv 2 \pmod 7$ の場合, $g(x) = x^3 + x + 1$ が $\omega^{j\frac{q^3-1}{7}}$ の最小多項式である. $\omega^{2j\frac{q^3-1}{7}}, \omega^{4j\frac{q^3-1}{7}}$ も $g(x)$ の根であるので, $x^3 + x + 1 = (x - \omega^{j\frac{q^3-1}{7}})(x - \omega^{2j\frac{q^3-1}{7}})(x - \omega^{4j\frac{q^3-1}{7}})$ を得る. 両辺の定数を比較して, $1 = -\omega^{7j\frac{q^3-1}{7}} = -1$ を得るが, これは矛盾である. $q \equiv 4 \pmod 7$ の場合の証明も同様である.

さらに, $1, \omega^{jN}, \omega^{j'N}$ が線形独立であることと, 任意の $t \in \{0,1,\ldots,6\}$ に対し, $\omega^{tN}, \omega^{(j+t)N}$, $\omega^{(j'+t)N}$ が線形独立であることは同値であるから, 全ての異なる $j_1, j_2, j_3 \in \{0,1,\ldots,6\}$ に対し, $\omega^{j_1N}, \omega^{j_2N}, \omega^{j_3N}$ は線形独立である. よって, 補題 3.2 より, 主張が示された. □

4　3値のガウス周期に基づくケーリーグラフの構成

この章では, $\mathbb{F}_{q^m}$ 上で 3 値のガウス周期の存在を仮定して, $(\mathbb{F}_{q^{2m}}, +)$ 上であるケーリーグラフを構成する. もし, 対応する連結集合がある条件を満たせば, 強正則グラフが得られる.

まず, 例から与えることとする.

例 4.1. $q = 7$, $M = 3$ とする. このとき, 系 3.3 で示されたように, ガウス周期 $\psi_{\mathbb{F}_{7^3}}(C_i^{(19,7^3)})$, $i = 0, 1, \ldots, 18$ はちょうど 3 つの値 $\alpha_1 = 11, \alpha_2 = 4$, $\alpha_3 = -3$ をもつ. このとき,

$$\begin{aligned} I_1 =& \{0\}, \\ I_2 =& \{8, 10, 12, 13, 15, 18\}, \\ I_3 =& \{1, 2, 3, 4, 5, 6, 7, 9, 11, 14, 16, 17\} \end{aligned}$$

となる. 今, I_2 の分割 $S_1 = \{8, 12, 18\}, S_2 = \{10, 13, 15\}$ を考え, $S_i'' \equiv 4^{-1} S_i \pmod{19}$, $i = 1, 2$ と定めると, 実際, $S_1'' = \{2, 3, 14\}, S_2'' = \{8, 12, 18\}$ となる. ここで,

$$\begin{aligned} Y &= \{19i + 4j \pmod{76} : (i, j) \in (\{0, 3\} \times S_1'') \cup (\{1, 2\} \times S_2'')\} \\ &\quad \cup \{19i + 4j \pmod{76} : i = 0, 1, 2, 3,\ j \in 4^{-1} I_1 \pmod{19}\} \\ &= \{8, 12, 37, 56, 65, 69, 10, 15, 34, 51, 67, 70, 0, 19, 38, 57\} \end{aligned}$$

と定めると, $\mathbb{F}_{7^6}$ の適当な原始根の選び方に依って, ケーリーグラフ $\mathrm{Cay}(\mathbb{F}_{7^6}, \bigcup_{i \in Y} C_i^{(76,7^6)})$ が強正則グラフとなる.

今, q^m を $q^m \equiv 3 \pmod 4$ を満たす素数ベキとし, ω を $\mathbb{F}_{q^m}$ の原始根とする. さらに, N を $(q^m - 1)/(q - 1)$ を割る奇数とし, $C_i^{(N,q^m)} = \omega^i \langle \omega^N \rangle$, $i = 0, 1, \ldots, N - 1$ と定める. この章では, 常にガウス周期 $\psi_{\mathbb{F}_{q^m}}(C_i^{(N,q^m)})$, $i = 0, 1, \ldots, N - 1$ はちょうど 3 つの有理数値 $\alpha_1, \alpha_2, \alpha_3$ をとり, かつ, $(t :=) \alpha_1 - \alpha_2 = \alpha_2 - \alpha_3 > 0$ を満たすものとする.

$$I_j := \{i \pmod N \mid \psi_{\mathbb{F}_{q^m}}(C_i^{(N,q^m)}) = \alpha_j\}, \quad j = 1, 2, 3$$

とおき, S_1, S_2 を I_2 のある分割とする. また, 例と同じように, let $S_i' \equiv 2^{-1} S_i \pmod N$, $S_i'' \equiv 2^{-1} S_i' \pmod N$, $i = 1, 2$ とおき,

$$X := 2S_1'' \cup (2S_2'' + N) \pmod{2N}, \tag{4.1}$$

$$\begin{aligned} Y_X := &\{Ni + 4j \pmod{4N} : (i, j) \in (\{0, 3\} \times S_1'') \cup (\{1, 2\} \times S_2'')\} \\ &\cup \{Ni + 4j \pmod{4N} : i = 0, 1, 2, 3,\ j \in 4^{-1} I_1 \pmod N\} \end{aligned} \tag{4.2}$$

と定める. このとき, 多重集合として, $X \equiv 2^{-1} I_2 \pmod N$, $Y_X \equiv I_1 \cup I_1 \cup I_1 \cup I_1 \cup I_2 \cup I_2 \pmod N$ が得られる.

あるうまい I_2 の分割 S_1, S_2 が存在すれば, 以下の D_X が $(\mathbb{F}_{q^{2m}}, +)$ 上の強正則ケーリーグラフ連結集合を与える.

命題 4.2. 上の表記のもと,

$$D_X := \bigcup_{i\in Y_X} C_i^{(4N,q^{2m})}, \tag{4.3}$$

と定める. ただし, $C_i^{(4N,q^{2m})} = \gamma^i\langle\gamma^{4N}\rangle$, $i = 0,1,\ldots,4N-1$ とし, また, γ は $\mathbb{F}_{q^{2m}}$ の原始根で, $\gamma^{q^m+1} = \omega$ となるものとする. また, $a \in \mathbb{Z}_{4N}$ に対し, $b \equiv 4^{-1}a \pmod N$, $c \equiv 2b \pmod{2N}$ と定める. このとき, D_X の指標値は以下で与えられる:

$$\begin{aligned}\psi_{\mathbb{F}_{q^{2m}}}(\gamma^a D_X) =& \frac{\rho_{q^m}\delta_a q^m}{2G_{q^m}(\eta)}\left(2\psi_{\mathbb{F}_{q^m}}(\omega^c\bigcup_{\ell\in X}C_\ell^{(2N,q^m)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c\bigcup_{\ell\in 2^{-1}I_2}C_\ell^{(N,q^m)})\right)\\ &+\frac{(q^m-1)(2|I_1|+|I_2|)}{2N} + \begin{cases} -q^m, & a\in I_1 \pmod N \text{ のとき},\\ -\frac{q^m}{2}, & a\in I_2 \pmod N \text{ のとき},\\ 0, & a\in I_3 \pmod N \text{ のとき}.\end{cases}\end{aligned} \tag{4.4}$$

ここで, η は, $\mathbb{F}_{q^m}$ の位数 2 の乗法的指標, ρ_{q^m} は, $q^m \equiv 7 \pmod 8$ または $q^m \equiv 3 \pmod 8$ に応じて, $\rho_{q^m} = 1$ または -1 とおく. さらに, δ_a は

$$\delta_a = \begin{cases} 1, & a\equiv 0,1 \pmod 4 \text{ かつ } N\equiv 1 \pmod 4, \text{ または},\\ & a\equiv 0,3 \pmod 4 \text{ かつ } N\equiv 3 \pmod 4 \text{ のとき},\\ -1, & a\equiv 2,3 \pmod 4 \text{ かつ } N\equiv 1 \pmod 4, \text{ または},\\ & a\equiv 1,2 \pmod 4 \text{ かつ } N\equiv 3 \pmod 4 \text{ のとき}\end{cases}$$

と定める.

この命題は, この論文の鍵となる重要な物であるが, 煩雑な計算が含まれるため, 省略する. 詳細は, 論文 [21] を参照されたい.

注意 4.3. 式 (4.1) において, X が

$$\begin{aligned}&2\psi_{\mathbb{F}_{q^m}}(\omega^c\bigcup_{\ell\in X}C_\ell^{(2N,q^m)}) - \psi_{\mathbb{F}_{q^m}}(\omega^c\bigcup_{\ell\in 2^{-1}I_2}C_\ell^{(N,q^m)})\\ =&\begin{cases}\pm G_{q^m}(\eta), & c\in 2^{-1}I_2 \pmod N \text{ のとき},\\ 0, & c\notin 2^{-1}I_2 \pmod N \text{ のとき},\end{cases}\end{aligned} \tag{4.5}$$

を満たすとき, 式 (4.5) を式 (4.4) へ代入し, D_X がちょうど 2 つの非自明な指標値 $(q^m-1)(2|I_1|+|I_2|)/2N$ と $-q^m+(q^m-1)(2|I_1|+|I_2|)/2N$ を取ることが分かる. これは, ケーリーグラフ $\mathrm{Cay}(\mathbb{F}_{q^{2m}}, D_X)$ が強正則となることを意味している. また, この場合, 強正則グラフのパラメータは, $(v,k,\lambda,\mu) = (q^{2m}, r(q^m+1), q^m+r^2-3r, r^2-r)$, $r = (|I_2|+2|I_1|)(q^m-1)/2N$ と定まる.

5 注意 4.3 の条件を満たす集合 X について

5.1 $\mathrm{PG}(2,q)$ の conic のある分割

この章では, [8, 11] で発見された $\mathrm{PG}(2,q)$ の conic のある分割について概説する.

q を奇素数ベキとし, ω を $\mathbb{F}_{q^3}$ の原始根とする. $\mathbb{F}_{q^3}$ を $\mathbb{F}_q$ 上の 3 次元線形空間とみなすことで, $\mathbb{F}_{q^3}$ を $\mathrm{PG}(2,q)$ の対応するアフィン空間とみなす. $\mathrm{PG}(2,q)$ の点は, $\langle\omega^i\rangle := \omega^i\mathbb{F}_q^*$, $0 \le i \le q^2+q$ と書ける. また, $\mathrm{PG}(2,q)$ の直線は

$$L_c := \{\langle x\rangle : \mathrm{Tr}_{q^3/q}(\omega^c x) = 0\},\ \ 0 \le c < q^2+q+1 \tag{5.1}$$

と書ける.

非退化な二次形式 $Q : \mathbb{F}_{q^3} \to \mathbb{F}_q$, $Q(x) := \mathrm{Tr}_{q^3/q}(x^2)$ を考える. このとき, $\mathcal{Q} = \{\langle\omega^i\rangle : Q(\omega^i) = 0\}$ は $\mathrm{PG}(2,q)$ の conic と呼ばれる. $|\mathcal{Q}| = q+1$ であり, $\mathrm{PG}(2,q)$ の各直線 L は $\mathcal{Q}$ と $0,1,2$ 点のいずれかで交わる.

$\mathbb{Z}_{q^2+q+1}$ の部分集合

$$W_{\mathcal{Q}} := \{i \pmod{q^2+q+1} : Q(\omega^i) = 0\} = \{d_0, d_1, \ldots, d_q\} \tag{5.2}$$

を考える. ここで, 要素には適当な順序を付けている. このとき, 明らかに

$$\mathcal{Q} = \{\langle\omega^{d_i}\rangle : 0 \le i \le q\}$$

である. さらに, Singer 差集合 $S = \{i \pmod{q^2+q+1} : \mathrm{Tr}_{q^3/q}(\omega^i) = 0\}$ に対し, $W_{\mathcal{Q}} \equiv 2^{-1}S \pmod{q^2+q+1}$ が成立する.

今, $D_1 := \bigcup_{i\in W_{\mathcal{Q}}} C_i^{(q^2+q+1,q^3)}$ とし, また,

$$W_s := \{i \pmod{q^2+q+1} : \mathrm{Tr}_{q^3/q}(\omega^{2i}) \in C_0^{(2,q)}\},$$
$$W_n := \{i \pmod{q^2+q+1} : \mathrm{Tr}_{q^3/q}(\omega^{2i}) \in C_1^{(2,q)}\}$$

と定める. このとき, 以下が成立する.

補題 5.1. ([3, 式 (3.5)]) 集合 D_1 は, 以下のちょうど 3 つの非自明な指標値を取る:

$$\psi_{\mathbb{F}_{q^3}}(\omega^c D_1) = \begin{cases} -1, & c \pmod{q^2+q+1} \in W_{\mathcal{Q}} \text{ のとき}, \\ -1+\epsilon q, & c \pmod{q^2+q+1} \in W_s \text{ のとき}, \\ -1-\epsilon q, & c \pmod{q^2+q+1} \in W_n \text{ のとき}. \end{cases}$$

ここで, ϵ は $q \equiv 1 \pmod 4$ または $3 \pmod 4$ に応じて, $\epsilon = 1$ または -1 と定める.

今, D_1 の分割を考える. $d_0 \in W_{\mathcal{Q}}$ を任意に固定し,

$$\mathcal{X}_{\mathcal{Q}} := \{\omega^{d_i}\mathrm{Tr}_{q^3/q}(\omega^{d_0+d_i}) : 1 \le i \le q\} \cup \{2\omega^{d_0}\} \tag{5.3}$$

および

$$X_{\mathcal{Q}} := \{\log_\omega(x) \pmod{2(q^2+q+1)} : x \in \mathcal{X}_{\mathcal{Q}}\} \tag{5.4}$$

と定める. このとき, 明らかに, $X_{\mathcal{Q}} \equiv W_{\mathcal{Q}} \pmod{q^2+q+1}$ が成立する. ここで, $X_{\mathcal{Q}}$ の重要な性質を述べる.

補題 5.2. ([11, Lemma 3.4]) X_Q において, d_0 の代わりに他の d_i を用いたとき, 結果の集合 X'_Q は, $X'_Q \equiv X_Q$ または $X_Q + (q^2+q+1) \pmod{2(q^2+q+1)}$ を満たす.

集合 $X_Q \subseteq \mathbb{Z}_{2(q^2+q+1)}$ は, $|E_1| + |E_2| = q+1$ を満たすある $E_1, E_2 \subseteq \mathbb{Z}_{q^2+q+1}$ が存在し,

$$X_Q = 2E_1 \cup (2E_2 + (q^2+q+1)) \pmod{2(q^2+q+1)} \tag{5.5}$$

となる. このとき, $2(E_1 \cup E_2) \equiv W_Q \pmod{q^2+q+1}$ かつ $4(E_1 \cup E_2) \equiv S \pmod{q^2+q+1}$ が成立する. 今, D_1 の分割

$$D_{1,1} := \bigcup_{i \in X_Q} C_i^{(2(q^2+q+1),q^3)} \quad \text{and} \quad D_{1,2} := \bigcup_{i \in X_Q + (q^2+q+1)} C_i^{(2(q^2+q+1),q^3)}$$

を考えると, 以下の定理が成立する.

定理 5.3. ([11, Theorem 3.7, Remark 3.8], [3, Theorem 3.4]) $D_{1,1}$ は, 以下のちょうど 4 つの非自明な指標値を取る:

$$\psi_{\mathbb{F}_{q^3}}(\omega^c D_{1,1}) = \begin{cases} \frac{-1+\epsilon\eta(2)G_{q^3}(\eta)}{2}, & c \pmod{q^2+q+1} \in W_Q \text{ かつ} \\ & \quad c \pmod{2(q^2+q+1)} \in X_Q \text{ のとき}, \\ \frac{-1-\epsilon\eta(2)G_{q^3}(\eta)}{2}, & c \pmod{q^2+q+1} \in W_Q \text{ かつ} \\ & \quad c \pmod{2(q^2+q+1)} \in X_Q + (q^2+q+1) \text{ のとき}, \\ \frac{-1+\epsilon q}{2}, & c \pmod{q^2+q+1} \in W_s \text{ のとき}, \\ \frac{-1-\epsilon q}{2}, & c \pmod{q^2+q+1} \in W_n \text{ のとき}. \end{cases}$$

ここで, η は $\mathbb{F}_{q^3}$ の位数 2 の乗法的指標とする.

5.2 Conic の分割の商について

q を素数ベキとし, M を q^2+q+1 を割る正整数とし, $N = \frac{q^2+q+1}{M}$ と定める. 今, ガウス周期 $\psi_{\mathbb{F}_{q^3}}(C_i^{(N,q^3)})$, $i = 0, 1, \ldots, N-1$ がちょうど 3 つの値 $-M+2q, -M+q, -M$ を取ると仮定する. 3.2 章において, そのような例 (無限系列) を二つ与えた.

X_Q を (5.5) で定めた $\mathbb{Z}_{2(q^2+q+1)}$ の部分集合とし, W_Q を (5.2) で定めた集合とする. このとき $X_Q \equiv W_Q \equiv 2^{-1}S \pmod{q^2+q+1}$ であった. X_Q の N を法とした制限は, (3.7) で見たように, 多重集合として $\overline{S_N} = 2^{-1}(I_1 \cup I_1 \cup I_2)$ となる. いま, X_Q の $2N$ を法とした制限 $\overline{X_Q}$ が, 多重集合になるかどうかに興味がある. ここで, 群 G のある多重集合が, 重複度が 1 以下の単なる集合であるとき, pure であると呼ぶ.

ここで,

$$X_i := \{x \pmod{2N} : x \in X_Q, x \pmod{N} \in 2^{-1}I_i\}, \ i = 1, 2 \tag{5.6}$$

と定めると, $X_1 \equiv 2^{-1}(I_1 \cup I_1) \pmod{N}$ かつ $X_2 \equiv 2^{-1}I_2 \pmod{N}$ は明らか. さらに, $\overline{X_Q} = X_1 \cup X_2$ も明らかである. X_2 は $\mathbb{Z}_{2N}$ 上で pure であるが, X_1 が $\mathbb{Z}_{2N}$ 上 pure でないかもしれない. よって, $\overline{X_Q}$ が $\mathbb{Z}_{2N}$ 上 pure であることと, X_1 が pure であることは同値である.

補題 5.4. X_1 が, $\mathbb{Z}_{2N}$ 上 *pure* であるとき, 以下が成立する*:*

$$\begin{aligned}&2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in X_2} C_\ell^{(2N,q^3)}) - \psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in 2^{-1}I_2} C_\ell^{(N,q^3)})\\ =&2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in \overline{X_{\mathcal{Q}}}} C_\ell^{(2N,q^3)}) - \psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in 2^{-1}(I_1\cup I_1\cup I_2)} C_\ell^{(N,q^3)}).\end{aligned}$$

証明:

$$A := 2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in \overline{X_{\mathcal{Q}}}} C_\ell^{(2N,q^3)}) - 2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in X_2} C_\ell^{(2N,q^3)})$$

を計算する. $\overline{X_{\mathcal{Q}}} = X_1 \cup X_2$ より,

$$A = 2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in X_1} C_\ell^{(2N,q^3)}) \tag{5.7}$$

は明らか. また, $X_1 \equiv 2^{-1}(I_1 \cup I_1) \pmod N$ であるので, 補題の仮定より, X_1 のある部分集合 T が存在し,

$$X_1 = T \cup (T+N)$$

かつ

$$T \cap (T+N) = \emptyset$$

と書ける. ここで, $T \equiv 2^{-1}I_1 \pmod N$ を満たす. このとき, (5.7) から続けて,

$$\begin{aligned}A =& 2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in T}(C_\ell^{(2N,q^3)} \cup C_{\ell+N}^{(2N,q^3)}))\\ =& 2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in 2^{-1}I_1} C_\ell^{(N,q^3)})\\ =& \psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in 2^{-1}(I_1\cup I_1\cup I_2)} C_\ell^{(N,q^3)}) - \psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in 2^{-1}I_2} C_\ell^{(N,q^3)})\end{aligned}$$

を得る. よって, 主張が得られる. □

命題 5.5. 補題 *5.4* の仮定の下, 以下が成立する*:*

$$2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in X_2} C_\ell^{(2N,q^3)}) - \psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in 2^{-1}I_2} C_\ell^{(N,q^3)}) = \begin{cases} \pm G_{q^3}(\eta), & c \in 2^{-1}I_2 \pmod N \text{ のとき,}\\ 0, & c \notin 2^{-1}I_2 \pmod N \text{ のとき.}\end{cases}$$

証明: 補題 5.4 より,

$$B := 2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in \overline{X_{\mathcal{Q}}}} C_\ell^{(2N,q^3)}) - \psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in 2^{-1}(I_1\cup I_1\cup I_2)} C_\ell^{(N,q^3)})$$

を計算すれば十分である. ここで,

$$B_1 := 2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell\in \overline{X_{\mathcal{Q}}}} C_\ell^{(2N,q^3)}) = 2\sum_{h=0}^{M-1} \psi_{\mathbb{F}_{q^3}}(\omega^{c+2hN} \bigcup_{\ell\in X_{\mathcal{Q}}} C_\ell^{(2(q^2+q+1),q^3)})$$

と

$$B_2 := \psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell \in 2^{-1}(I_1 \cup I_1 \cup I_2)} C_\ell^{(N,q^3)}) = \sum_{h=0}^{M-1} \psi_{\mathbb{F}_{q^3}}(\omega^{c+hN} \bigcup_{\ell \in W_{\mathcal{Q}}} C_\ell^{(q^2+q+1,q^3)})$$

は明らかである. このとき, 定理 5.3 より,

$$\begin{aligned} B_1 = &(-1+\epsilon\eta(2)G_{q^3}(\eta)) \cdot |X_{\mathcal{Q}} \cap (2N\mathbb{Z}_{2(q^2+q+1)} + c)| \\ &+ (-1-\epsilon\eta(2)G_{q^3}(\eta)) \cdot |(X_{\mathcal{Q}} + (q^2+q+1)) \cap (2N\mathbb{Z}_{2(q^2+q+1)} + c)| \\ &+ (-1+\epsilon q) \cdot |W_s \cap (N\mathbb{Z}_{q^2+q+1} + c)| + (-1-\epsilon q) \cdot |W_n \cap (N\mathbb{Z}_{q^2+q+1} + c)| \end{aligned}$$

を得る. 一方, 補題 5.1 より,

$$\begin{aligned} B_2 = &-|W_{\mathcal{Q}} \cap (N\mathbb{Z}_{q^2+q+1} + c)| \\ &+ (-1+\epsilon q) \cdot |W_s \cap (N\mathbb{Z}_{q^2+q+1} + c)| + (-1-\epsilon q) \cdot |W_n \cap (N\mathbb{Z}_{q^2+q+1} + c)| \end{aligned}$$

を得る. ここで,

$$\begin{aligned} x_0 :&= |X_{\mathcal{Q}} \cap (2N\mathbb{Z}_{2(q^2+q+1)} + c)|, \\ x_1 :&= |(X_{\mathcal{Q}} + (q^2+q+1)) \cap (2N\mathbb{Z}_{2(q^2+q+1)} + c)| \end{aligned}$$

と定めると, $x_0 + x_1 = |W_{\mathcal{Q}} \cap (N\mathbb{Z}_{q^2+q+1} + c)|$ より,

$$B = B_1 - B_2 = \epsilon\eta(2)G_{q^3}(\eta)(x_0 - x_1) \tag{5.8}$$

を得る. 仮定より, X_1 は $\mathbb{Z}_{2N}$ 上 pure であるから, $X_{\mathcal{Q}}$ の $2N$ を法とする制限 $\overline{X_{\mathcal{Q}}}$ も $\mathbb{Z}_{2N}$ 上 pure である. よって, $x_0, x_1 \in \{0,1\}$ である. 特に,

$$\begin{aligned} (x_0,x_1) = (1,1) &\Leftrightarrow\ c \in 2^{-1}I_1 \pmod N, \\ (x_0,x_1) = (0,1),(1,0) &\Leftrightarrow\ c \in 2^{-1}I_2 \pmod N, \\ (x_0,x_1) = (0,0) &\Leftrightarrow\ c \in 2^{-1}I_3 \pmod N \end{aligned}$$

が成立する. (5.8) から続けて,

$$B = \begin{cases} \pm G_{q^3}(\eta), & c \in 2^{-1}I_2 \pmod N \text{ のとき}, \\ 0, & c \notin 2^{-1}I_2 \pmod N \text{ のとき} \end{cases}$$

を得る. よって, 主張が示された. □

注意 5.6. X_2 が $\mathbb{Z}_{2N}$ 上の *pure* であり, $X_2 \equiv 2^{-1}I_2 \pmod N$ を満たすことに注意する. このとき, 命題 *5.5* は, もし X_1 が $\mathbb{Z}_{2N}$ 上 *pure* であれば, X_2 が注意 *4.3* の条件 (4.5) を $m = 3$, $X = X_2$ として満たすことを意味している.

5.3 X_1 が $\mathbb{Z}_{2N}$ 上 pure となるための条件

3.2 章で示したように, $M=3$ または 7 に対し, $N=(q^2+q+1)/M$ とするとき, ガウス周期 $\psi_{\mathbb{F}_{q^3}}(C_i^{(N,q^3)})$, $i=0,1,\dots,N-1$ はちょうど 3 つの値 $-M+2q, -M+q, -M$ をとる. 注意 5.6 を適用するために, X_1 が $\mathbb{Z}_{2N}$ 上 pure になるかどうかを調べる必要がある, この章では, 以下の結果を証明する.

結果 5.1.

(i) q を $q\equiv 1 \pmod 3$ なる素数ベキで, $M=3$ とする. もし, $q\equiv 7$ または $13 \pmod{24}$ であれば, X_1 は $\mathbb{Z}_{2N}$ 上 *pure* となる.

(ii) q を $q\equiv 2$ *or* $4 \pmod 7$ なる素数ベキで, $M=7$ とする. もし, $q\equiv 11, 37, 51$ または $53 \pmod{56}$ であれば, X_1 は $\mathbb{Z}_{2N}$ 上 *pure* となる.

$u\in W_Q$ かつ $u \pmod N \in 2^{-1}I_1$ と仮定する. $W_Q \equiv 2^{-1}(I_1\cup I_1\cup I_2) \pmod N$ であるので, ちょうど一つ $\ell_u\in\{1,2,\dots,M-1\}$ が存在し, $u+\ell_u N$ もまた W_Q に属す. W_Q の定義 (5.2) より, $\mathrm{Tr}_{q^3/q}(\omega^{2u})=\mathrm{Tr}_{q^3/q}(\omega^{2u+2\ell_u N})=0$ が成り立つ. これらの式から,

$$\omega^{2uq^2}=-(\omega^{2u}+\omega^{2uq}), \tag{5.9}$$

$$\omega^{2uq}=-\frac{\omega^{2u-\frac{2\ell_u(q^3-1)}{M}}(1-\omega^{\frac{2(q+1)\ell_u(q^3-1)}{M}})}{1-\omega^{\frac{2q\ell_u(q^3-1)}{M}}} \tag{5.10}$$

が成立する. $u \pmod N \in 2^{-1}I_1$ となる $u\in W_Q$ に対し,

$$g_M(\omega^u)=\mathrm{Tr}_{q^3/q}(\omega^{2u+\ell_u N})\omega^{\ell_u N}$$

と定める. $\mathcal{X}_Q$ の定義 (5.3) と補題 5.2 より, $2\omega^u, g_M(\omega^u)\omega^u \in \mathcal{X}_Q$ または $2\omega^{u+(q^2+q+1)}$, $g_M(\omega^u)\omega^{u+(q^2+q+1)}\in\mathcal{X}_Q$ と仮定できる. よって, X_1 が $\mathbb{Z}_{2N}$ 上 pure であることと, $\eta(2)\neq\eta(g_M(\omega^u))$ が $u \pmod N\in 2^{-1}I_1$ を満たすすべての $u\in W_Q$ で成立することは同値である. ここで, η は $\mathbb{F}_{q^3}$ の位数 2 の乗法的指標とする.

補題 5.7. 上記の表記の下, 以下が成立する.

$$\eta(g_M(\omega^u))=\eta(-1)\eta(1-\omega^{\frac{\ell_u(q+1)(q^3-1)}{M}})\eta(1-\omega^{\frac{2\ell_u q(q^3-1)}{M}}).$$

証明: $g_M(\omega^u)$ の定義と条件 (5.9) より,

$$\begin{aligned} g_M(\omega^u) &= \omega^{2\ell_u N}(\omega^{2u}+\omega^{2uq+\frac{\ell_u(q^3-1)}{M}}+\omega^{2uq^2+\frac{\ell_u(q+1)(q^3-1)}{M}}) \\ &= \omega^{2\ell_u N}(\omega^{2u}(1-\omega^{\frac{\ell_u(q+1)(q^3-1)}{M}})+\omega^{2uq+\frac{\ell_u(q^3-1)}{M}}(1-\omega^{\frac{\ell_u q(q^3-1)}{M}})) \end{aligned} \tag{5.11}$$

を得る. また, (5.10) を (5.11) へ代入して,

$$(5.11)=-\omega^{2\ell_u N}\omega^{2u-\frac{\ell_u(q^3-1)}{M}}\frac{(1-\omega^{\frac{\ell_u(q^3-1)}{M}})(1-\omega^{\frac{\ell_u(q+1)(q^3-1)}{M}})(1-\omega^{\frac{\ell_u q(q^3-1)}{M}})}{1-\omega^{\frac{2\ell_u q(q^3-1)}{M}}} \tag{5.12}$$

が得られる．ここで，$\eta(1-\omega^{\frac{\ell_u(q^3-1)}{M}})=\eta(1-\omega^{\frac{\ell_u q(q^3-1)}{M}})$ より，

$$\eta(g_M(\omega^u))=\eta(-1)\eta(1-\omega^{\frac{\ell_u(q+1)(q^3-1)}{M}})\eta(1-\omega^{\frac{2\ell_u q(q^3-1)}{M}})$$

を得る． □

命題 5.8. q を $q\equiv 1\,(\mathrm{mod}\ 6)$ なる素数ベキとし，η を $\mathbb{F}_{q^3}$ の位数 2 の乗法的指標とする．このとき，

$$\eta(g_3(\omega^u))=\begin{cases} 1, & q\equiv 1\,(\mathrm{mod}\ 12)\text{ のとき},\\ -1, & q\equiv 7\,(\mathrm{mod}\ 12)\text{ のとき}\end{cases}$$

が成立する．

証明: 補題 5.7 より，

$$\begin{aligned}\eta(g_3(\omega^u))&=\eta(-1)\eta(1-\omega^{\frac{2\ell_u(q^3-1)}{3}})\eta(1-\omega^{\frac{2\ell_u(q^3-1)}{3}})\\&=\eta(-1)=\begin{cases} 1, & q\equiv 1\,(\mathrm{mod}\ 12)\text{ のとき},\\ -1, & q\equiv 7\,(\mathrm{mod}\ 12)\text{ のとき}\end{cases}\end{aligned}$$

を得る． □

平方剰余の相互法則の補助法則より，$\eta(2)\neq\eta(g_3(\omega^u))$ であるための必要十分条件は，$q\equiv 7$ または $13\,(\mathrm{mod}\ 24)$ である．よって，結果 5.1 (i) が得られる．

命題 5.9. q を $q\equiv 9$ または $11\,(\mathrm{mod}\ 14)$ を満たす素数ベキとする．また，η を $\mathbb{F}_{q^3}$ の位数 2 の乗法的指標とする．このとき，

$$\eta(g_7(\omega^u))=1$$

が成立する．

証明: 補題 5.7 より，

$$\eta(g_7(\omega^u))=\eta(-1)\eta(1-\omega^{\frac{\ell_u(q+1)(q^3-1)}{7}})\eta(1-\omega^{\frac{2\ell_u q(q^3-1)}{7}}) \tag{5.13}$$

であるが，この右辺を，(i) $q\equiv 9\,(\mathrm{mod}\ 14)$ の場合と (ii) $q\equiv 11\,(\mathrm{mod}\ 14)$ の場合に分けて決定する．

(i) $q\equiv 9\,(\mathrm{mod}\ 14)$ の場合，$1-\omega^{\frac{\ell_u(q+1)(q^3-1)}{7}}=1-\omega^{\frac{3\ell_u(q^3-1)}{7}}$ かつ $1-\omega^{\frac{2\ell_u q(q^3-1)}{7}}=-\omega^{\frac{4\ell_u(q^3-1)}{7}}(1-\omega^{\frac{3\ell_u(q^3-1)}{7}})$ である．このとき，(5.13) から続けて，$\eta(g_7(\omega^u))=1$ を得る．

(ii) $q\equiv 11\,(\mathrm{mod}\ 14)$ の場合，$1-\omega^{\frac{\ell_u(q+1)(q^3-1)}{7}}=1-\omega^{\frac{5\ell_u(q^3-1)}{7}}$ かつ $1-\omega^{\frac{2\ell_u q(q^3-1)}{7}}=-\omega^{\frac{\ell_u(q^3-1)}{7}}(1-\omega^{\frac{6\ell_u(q^3-1)}{7}})$ である．ここで，

$$\eta(1-\omega^{\frac{6\ell_u(q^3-1)}{7}})=\eta(1-\omega^{\frac{6q^2\ell_u(q^3-1)}{7}})=\eta(1-\omega^{\frac{5\ell_u(q^3-1)}{7}})$$

に注意し，(5.13) から続けて，$\eta(g_7(\omega^u))=1$ を得る． □

平方剰余の相互法則の補助法則より, $\eta(2) = -1$ であるための必要十分条件は, $q \equiv 3$ または $5 \pmod 8$ である. よって, 結果 5.1 (ii) を得る.

最後に, 命題 5.5, 注意 4.3, 注意 5.6, さらに, $q^m \equiv 3 \pmod 4$ の場合の結果 5.1 (i), (ii) を組み合わせることで, 定理 1.1 (i) および (ii) の主張が従う.

参考文献

[1] J. Bamberg, S. Kelly, M. Law, T. Penttila, Tight sets and m-ovoids of finite polar spaces, *J. Combin. Theory Ser. A* **114**, 1293–1314, (2007).

[2] J. Bamberg, M. Law, T. Penttila, Tight sets and m-ovoids of generalised quadrangles, *Combinatorica* **29**, 1–17, (2009).

[3] J. Bamberg, M. Lee, K. Momihara, Q. Xiang, A new family of hemisystems of the Hermitian surface, *Combinatorica*, DOI: 10.1007/s00493-016-3525-4.

[4] A.E. Brouwer, W.H. Haemers, *Spectra of Graphs*, Springer, Universitext, 2012.

[5] A.A. Bruen, K. Drudge, The construction of Cameron-Liebler line classes in PG$(3, q)$, *Finite Fields Appl.* **5**, 35–45, (1999).

[6] R. Calderbank, W.M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.* **18**, 97–122, (1986).

[7] A. Cossidente, T. Penttila, Hemisystems on the Hermitian surface, *J. London Math. Soc.* **72**, 731–741, (2005).

[8] J. De Beule, J. Demeyer, K. Metsch, M. Rodgers, A new family of tight sets in $\mathcal{Q}^+(5, q)$, *Des. Codes Cryptogr.* **78**, 655–678, (2016).

[9] K. Drudge, *Extremal sets in projective and polar spaces*, PhD thesis, The University of Western Ontario, 1998.

[10] T. Feng, Q. Xiang, Strongly regular graphs from unions of cyclotomic classes, *J. Combin. Theory Ser. B* **102** 982–995, (2012).

[11] T. Feng, K. Momihara, Q. Xiang, Cameron-Liebler line classes with parameter $x = \frac{q^2-1}{2}$, *J. Combin. Theory Ser. A* **133**, 307–338, (2015).

[12] T. Feng, K. Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, *Combinatorica* **35**, 413–434, (2015).

[13] T. Feng, K. Momihara, Q. Xiang, Three-valued Gauss periods, circulant weighing matrices and association schemes, *J. Algebraic Combin.* **43**, 851–875, (2016).

[14] G. Ge, Q. Xiang, T. Yuan, Construction of strongly regular Cayley graphs using index four Gauss sums, *J. Algebraic Combin.* **37**, 313–329, (2013).

[15] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.

[16] J.H. van Lint, A. Schrijver, Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica* **1**, 63–73, (1981).

[17] D. Luyckx, J.A. Thas, The uniqueness of the 1-system of $\mathcal{Q}^-(7,q)$, q odd, *J. Combin. Theory Ser. A* **98**, 253–267, (2002).

[18] D. Luyckx, J.A. Thas, The uniqueness of the 1-system of $\mathcal{Q}^-(7,q)$, q even, *Discrete Math.* **294**, 133–138, (2005).

[19] S.L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4**, 221–261, (1994).

[20] K. Momihara, Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums, *Europ. J. Combin.* **34**, 706–723, (2013).

[21] K. Momihara, Construction of strongly regular Cayley graphs based on three-valued Gauss periods, arXiv: 1705.07623.

[22] K. Momihara, Q. Xiang, Lifting constructions of strongly regular Cayley graphs, *Finite Fields Appl.* **26**, 86–99, (2014).

[23] K. Momihara, Q. Xiang, Strongly regular Cayley graphs from partitions of subdifference sets of the Singer difference sets, to appear in *Finite Fields Appl.*

[24] B. Segre, Forme e geometrie hermitiane, con particolare riguardo al caso finito, *Ann. Mat. Pura Appl.* **70**, 1–201, (1965).

[25] B. Schmidt, C. White, All two-weight irreducible cyclic codes?, *Finite Fields Appl.* **8**, 321–367, (2002).

[26] K. Yamamoto, M. Yamada. Williamson Hadamard matrices and Gauss sums, *J. Math. Soc. Japan* **37**, 703–717, (1985).