数理解析研究所講究録
第1965巻 2015年 135-149

Three-valued Gauss periods and related designs and association schemes

-ガウス周期とそれに関連するデザインおよびアソシエーションスキーム-

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

概 要

ガウス周期 (およびガウス和) の概念は, (古典的) 整数論における概念であるが, 組合せ論との相性も非常によい. 特に, この論文では, 三種の値を取るガウス周期についての分類についての部分的な結果と, デザインやアソシエーションスキームとの関連についての新しい結果について概説する.

1 導入

この論文は, Tao Feng (Zhejiang University) と Qing Xiang (University of Delaware) との共同研究によるものである. いくつか証明を省く命題があるが, 詳しくは論文 [3] を参照していただきたい.

この論文では, 以下の表記を用いることとする. p を素数, f を正整数とする. $\mathbb{F}_q$ で位数 $q=p^f$ の有限体とし, $\xi_p=e^{\frac{2\pi i}{p}}$ を 1 の原始 p 乗根とする. ここで,

$$\psi\colon \mathbb{F}_q \to \mathbb{C}^*, \qquad \psi(x)=\xi_p^{\mathrm{Tr}_{q/p}(x)}$$

は, $\mathbb{F}_q$ の 1 つの加法的な指標を定めるが, これを $\mathbb{F}_q$ の標準指標と呼ぶ. また, 一つの乗法的指標 $\chi\colon \mathbb{F}_q^* \to \mathbb{C}^*$ に対し,

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

なる指標和をガウス和とよぶ. また, ガウス和の概念は, 以下で定義するガウス周期の概念と密接な関係にある. $N>1$ を $N|(q-1)$ なる整数とし, $\mathbb{F}_q$ の原始根 γ を一つ固定する. このとき,

[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) 25800093, 基盤研究 (C) 24540013) の補助を受けています.

$C_a^{(N,q)} = \gamma^a\langle\gamma^N\rangle$ $(0 \le a \le N-1)$ を $\mathbb{F}_q$ の位数 N の円分剰余類とよぶ. また, 指標和

$$\eta_a = \sum_{x \in C_a^{(N,q)}} \psi(x),\ 0 \le a \le N-1$$

をガウス周期とよぶ.

ガウス和やガウス周期の概念は, ガウスによって導入された (古典的な) 整数論的概念であるが, 組合せ論においてもしばしば登場し, 特に, 差集合, 巡回符号, 強正則ケーリーグラフ, アソシエーションスキーム等 [1, 2, 5, 6] がある. 二種の値を取るガウス周期に関しては論文 [6] で扱われ, $N \mid \frac{p^f-1}{p-1}$ なる場合に, 二種の値を取るための必要十分条件が与えられている. しかし, その条件は (p, f, N) を exact に与えるものではなかった. 一方で, 彼らは, 以下のような予想を立てている.

予想 1.1. ([6]) $N \mid \frac{p^f-1}{p-1}$ を仮定する. このとき, ガウス周期が二種の値を取るのは以下の場合に限る:

(1) (部分体の場合) $C_0^{(N,q)}$ が $\mathbb{F}_q$ の部分体の乗法群に一致する場合.

(2) (準原始的な場合) $-1 \in \langle p\rangle \le (\mathbb{Z}/N\mathbb{Z})^*$ なる場合.

(3) (散在的な例) 以下の 11 個の例のうちのいづれか:

$$(p, f, N) = (3,5,11), (5,9,19), (3,12,35), (7,9,37), (11,7,43), (17,33,67)$$
$$(3,53,107), (5,18,133), (41,81,163), (3,144,323), (5,249,499).$$

この論文では, 三種の値をとるガウス周期の分類を部分的に与えることを目標とし, また, 関連するデザインやアソシエーションスキームに関するいくつかの結果について述べる. 特に, ガウス周期の値が等差数列をなし, かつ, 三種のうちの一つの値に関して, その値を取るコセットの数が一つの場合について, 上記の予想と同様の予想を与える. (非常に限られたクラスに対する分類であるが, このクラスはデザインやアソシエーションスキームなどの面白い組合せ構造が関係する組合せ論的に非常に興味深いクラスである.)

2 三種の値を取るガウス周期: 必要条件

ガウス周期 $\eta_a = \psi(\gamma^a C_0^{(N,q)})$ $(a = 0, 1, \ldots, N-1)$ がちょうど異なる 3 つの有理数値 $\alpha_1, \alpha_2, \alpha_3$ を取ると仮定する. $i = 1, 2, 3$ に対し,

$$I_i = \{a \in \mathbb{Z}_N \mid \eta_a = \alpha_i\}$$

とする. 以下, この表記を用いるものとする.

補題 2.1. 以下が成立する.

$$(\alpha_1 I_1 + \alpha_2 I_2 + \alpha_3 I_3)(\alpha_1 I_1^{(-1)} + \alpha_2 I_2^{(-1)} + \alpha_3 I_3^{(-1)}) = q[0] - \frac{q-1}{N}\mathbb{Z}_N. \qquad (2.1)$$

ただし, $I_j^{(-1)} = \{-x \in \mathbb{Z}_N : x \in I_j\}$ とし, 式は群環 $\mathbb{Q}[\mathbb{Z}_N]$ で考えるものとする.

証明: χ を指数 N の乗法的指標とする. このとき,

$$\begin{aligned} G_q(\chi) &= \sum_{i=0}^{N-1} \sum_{x \in C_i^{(N,q)}} \chi(x)\psi(x) \\ &= \eta_0 + \chi(\gamma)\eta_1 + \cdots + \chi(\gamma^{N-1})\eta_{N-1} \\ &= \alpha_1\chi(I_1) + \alpha_2\chi(I_2) + \alpha_3\chi(I_3). \end{aligned}$$

α_i $(1 \leq i \leq 3)$ は有理数を取るので, $\overline{\alpha_i} = \alpha_i$ を満たす. また, ガウス和の性質から

$$(\sum_{i=1}^{3} \alpha_i\chi(I_i))(\sum_{i=1}^{3} \alpha_i\overline{\chi(I_i)}) = G_q(\chi)\overline{G_q(\chi)} = q$$

を満たす. ここで, χ を自明な指標としたとき, $\alpha_1\chi(I_1) + \alpha_2\chi(I_2) + \alpha_3\chi(I_3) = G_q(\chi) = -1$ かつ

$$(\sum_{i=1}^{3} \alpha_i\chi(I_i))(\sum_{i=1}^{3} \alpha_i\overline{\chi(I_i)}) = G_q(\chi)\overline{G_q(\chi)} = 1$$

を満たす. このとき, Inversion formula より, 結果を得る. □

補題 2.1 より, I_i の濃度は $\alpha_1, \alpha_2, \alpha_3$ を使って表されることがわかる.

補題 2.2. ガウス周期 η_a $(0 \leq a \leq N-1)$ が三種の有理数値 $\alpha_1, \alpha_2, \alpha_3$ を取ると仮定する. このとき, 以下が成立する.

$$\begin{aligned} |I_1| &= -\frac{\alpha_2\alpha_3(q-1) + k(q-k+\alpha_2+\alpha_3)}{k(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)}, \\ |I_2| &= -\frac{\alpha_1\alpha_3(q-1) + k(q-k+\alpha_1+\alpha_3)}{k(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)}, \\ |I_3| &= -\frac{\alpha_1\alpha_2(q-1) + k(q-k+\alpha_1+\alpha_2)}{k(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)}. \end{aligned}$$

ここで, $k = \frac{q-1}{N}$ とする.

証明: I_j らは $\mathbb{Z}_N$ を分割しているので, 明らかに $|I_1| + |I_2| + |I_3| = N$. また, $\psi(\mathbb{F}_q^*) = -1$ より, $\alpha_1 I_1 + \alpha_2 I_2 + \alpha_3 I_3 = -1$. 更に, 式 (2.1) の $[0]$ の係数を比べて $\alpha_1^2|I_1| + \alpha_2^2|I_2| + \alpha_3^2|I_3| = q-k$ を得る. この連立方程式を $|I_j|$ $(j = 1, 2, 3)$ について解いて, 結果を得る. □

以下に三種の値を取るための必要条件を与える.

命題 2.3. ガウス周期 η_a $(0 \leq a \leq N-1)$ が 3 つの有理数値 $\alpha_1, \alpha_2, \alpha_3$ を取ると仮定し, $t > 0$ かつ $\gcd(u, v) = 1$ に対し, $\alpha_1 - \alpha_2 = -tu < 0$, $\alpha_3 - \alpha_2 = tv > 0$ とおく. このとき, t は p のベキで, かつ, 2 つの正整数 r, s, $0 < r, s < N$ が存在し,

(i) $t(-ur + vs) \equiv -1 \pmod{N}$;

(ii) $(N-1)q + t^2(-ur + vs)^2 = Nt^2(u^2r + v^2s)$;

が成立する. 特に, t は, 指数 N の全ての非自明な乗法的指標 χ に対し, $G_q(\chi)$ を割る最大の p ベキである.

証明: 関数 $\sigma : \mathbb{Z}_N \to \mathbb{C}$ を $\sigma(a) = \eta_a - \alpha_2$ で定める. σ の離散フーリエ変換 $\widehat{\sigma} : \widehat{\mathbb{Z}}_N \to \mathbb{C}$ は,

$$\widehat{\sigma}(\chi) = \frac{1}{\sqrt{N}} \sum_{a=0}^{N-1} \sigma(a)\chi(\gamma^a)$$

で与えられる. ここで, $\widehat{\mathbb{Z}}_N$ は $\mathbb{Z}_N$ の指標群とする. ただし, $\widehat{\mathbb{Z}}_N$ は $\mathbb{F}_q^*$ の指数 N の指標のなす群 $C_0^{\perp}$ と同一視してよい. このとき,

$$\widehat{\sigma}(\chi) = \begin{cases} \frac{1}{\sqrt{N}} G_q(\chi), & \chi \text{が非自明のとき;} \\ -\frac{1}{\sqrt{N}} - \alpha_2\sqrt{N}, & \chi \text{が自明のとき.} \end{cases}$$

仮定より, $\sigma(a) \in \{0, -tu, tv\}$ に注意. $\chi \in \widehat{\mathbb{Z}}_N$ が非自明であるとき,

$$G_q(\chi) = \sum_{a=0}^{N-1} \eta_a \chi(\gamma^a) = \sum_{a=0}^{N-1} (\eta_a - \alpha_2)\chi(\gamma^a) = t(-u\chi(I_1) + v\chi(I_3))$$

となる. よって, $t \,|\, G_q(\chi)$ を得て, $t = p^\theta$ と書ける.

一方,

$$\eta_a = \frac{1}{N} \sum_{\chi \in C_0^{\perp}} G_q(\chi)\chi^{-1}(\gamma^a)$$

より,

$$\sigma(\overline{\gamma}^a) = \frac{1}{N} \sum_{\chi \in (C_0^{\perp})^*} G_q(\chi)(\chi^{-1}(\gamma^a) - \chi^{-1}(\gamma^e)) \tag{2.2}$$

を得る. ここで, α_2 はある e で η_e と書けることを使っている. 今, t' を $G_q(\chi)$ $(\chi \in (C_0^{\perp})^*)$ を割る最大の p ベキとすると, (2.2) は $\gcd(N, t') = 1$ より, $t = t'$ を意味する.

さらに, $\widehat{\sigma}$ の定義より, $r = |I_1|$, $s = |I_3|$ $(0 < r, s < N)$ に対し,

$$\widehat{\sigma}(\chi_0) = \frac{1}{\sqrt{N}} \sum_{a=0}^{N-1} \sigma(a) = \frac{t(-ur + vs)}{\sqrt{N}}$$

と書ける. よって, $-\frac{1}{\sqrt{N}} - \frac{N}{\sqrt{N}}\alpha_2 = \frac{t(-ur+vs)}{\sqrt{N}}$ を得, $t(-ur + vs) \equiv -1 \pmod{N}$ が得られる.

また, σ の定義より, $\sum_{a=0}^{N-1} \sigma(a)\overline{\sigma(a)} = t^2(u^2r + v^2s)$ を得るが, 一方で,

$$\sum_{\chi \in C_0^{\perp}} \widehat{\sigma}(\chi)\overline{\widehat{\sigma}(\chi)} = \frac{1}{N} \sum_{\chi \in (C_0^{\perp})^*} G_q(\chi)\overline{G_q(\chi)} + \frac{t^2(-ur + vs)^2}{N} = \frac{1}{N}((N-1)q + t^2(-ur + vs)^2)$$

を得る. パーセバルの公式から,

$$(N-1)q + t^2(-ur + vs)^2 = Nt^2(u^2r + v^2s)$$

を得る. □

2.1 Circulant weighing matrix

論文 [6] では, ガウス周期 $\eta_a = \psi(\gamma^a C_0)$ $(0 \le a \le N-1)$ が 2 つの値 α_1, α_2 を取るとき, 集合 $I_i = \{a \in \mathbb{Z}_N \,|\, \eta_a = \alpha_i\}$ $(i = 1, 2)$ がそれぞれ $\mathbb{Z}_N$ で差集合になることを示している. この章では, 3 つの値を取る場合にどのような組合せ構造が現れるかを調べることにする. 以下の結果は, 前章の結果を組み合わせて直ちに得られる.

補題 2.4. ガウス周期 η_a $(0 \le a \le N-1)$ が 3 つの有理数値 $\alpha_1, \alpha_2, \alpha_3$ を取り, かつ, 等差的, つまり, $\alpha_1 - \alpha_2 = -t < 0$ かつ $\alpha_3 - \alpha_2 = t > 0$ を満たすとする. このとき,

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

を満たし, さらに,

$$(I_1 - I_3)(I_1 - I_3)^{(-1)} = \frac{q}{t^2} \cdot 1 + \frac{\alpha_2^2 N + 2\alpha_2 - k}{t^2}\mathbb{Z}_N \tag{2.3}$$

が群環 $\mathbb{Q}[\mathbb{Z}_N]$ の上で成立する.

この結果は, $-1, 0, 1$ を成分に持つ $\mathrm{N} \times N$ 行列で, 任意の異なる 2 行の内積が一定かつ任意の行の数の和も一定というものを生成できることを意味する. (長さ N のベクトルの I_1 の位置の成分を 1, I_2 の位置の成分を 0, I_3 の位置の成分を -1 とし, その列ベクトルから巡回的に行列を作ればよい.) 特別な場合には, 内積が 0 になり, いわゆる weighing matrix が得られる.

命題 2.5. ガウス周期 η_a $(0 \le a \le N-1)$ が 3 つの有理数値 $\alpha_1, \alpha_2, \alpha_3$ を取り, かつ等差的 $(\alpha_1 - \alpha_2 = -t < 0$ かつ $\alpha_3 - \alpha_2 = t > 0)$ とする. このとき, $I_1 - I_3$ が circulant weighing matrix を成すのは $\alpha_2 = (\sqrt{q} - 1)/N$ かつ q が平方のときであり, かつ, そのときに限る.

証明: q を平方とし, $\alpha_2 = (\sqrt{q} - 1)/N$ とおく. このとき, $\alpha_2^2 N + 2\alpha_2 - k = 0$ より, (2.3) は

$$(I_1 - I_3)(I_1 - I_3)^{(-1)} = \frac{q}{t^2} \cdot [0]$$

と変形される. よって, $I_1 - I_3$ が circulant weighing matrix を与える.

逆に, $I_1 - I_3$ が circulant weighing matrix を生成するためには, $\alpha_2^2 N + 2\alpha_2 - k = 0$ が成り立たなければならない. よって, $\alpha_2 = \frac{\sqrt{q}-1}{N}$, または, $\alpha_2 = -\frac{1+\sqrt{q}}{N}$ が成立. 後者では, $\sqrt{q} \equiv -1 \pmod{N}$ が成立するが, [6] の結果より, ガウス周期は 2 つの値を取る. よって, $\alpha_2 = \frac{\sqrt{q}-1}{N}$ が成立し, また, α_2 は有理数より q は平方数である. □

2.2 関連するアソシエーションスキーム

ガウス周期が二種の値を取る場合については, ガウス周期がケーリーグラフ $Cay(\mathbb{F}_q, C_0^{(N,q)})$ の非自明な固有値になっていることから, $\mathbb{F}_q$ 上の強正則グラフ (つまり, 2 クラスのアソシエーショ

ンスキーム) を得ることができる. この章では, この結果のガウス周期が三種の値を取る場合への自然な類似を考えたい.

定理 2.6. ガウス周期 η_a $(0 \le a \le N-1)$ が3つの有理数値 $\alpha_1, \alpha_2, \alpha_3$ を取ると仮定する. ここで, $t > 0$ に対し, $\alpha_1 - \alpha_2 = -tu < 0$ かつ $\alpha_3 - \alpha_2 = tv > 0$ と置ける. また, $I_i = \{a \in \mathbb{Z}_N \mid \eta_a = \alpha_i\}$ $(i = 1, 2, 3)$ に対し,

$$R_0 = \{0\},\ R_1 = \bigcup_{i \in I_1} C_i^{(N,q)},\ R_2 = \bigcup_{i \in I_2} C_i^{(N,q)},\ R_3 = \bigcup_{i \in I_3} C_i^{(N,q)}$$

とする. このとき, $\gcd(p-1, N) = 1$ または2かつ $|I_1| = 1$ または $|I_3| = 1$ ならば, $(\mathbb{F}_q, \{\mathcal{R}_i\}_{i=0}^3)$ は3クラスのアソシエーションスキームを与える. (ここで, (x, y) が関係 $\mathcal{R}_i$ に属すことを $x - y \in R_i$ で定める.)

証明: $|I_1| = 1$ $(I_1 = \{\ell\})$ と仮定する. 各 I_j は p の積で不変であるので, $\gcd(p-1, N) = 1$ または2より, $\ell = 0$ または $N/2$ が得られる. ここで, $J_1 = I_1 + \ell = \{0\}$, $J_2 = I_2 + \ell$, $J_3 = I_3 + \ell$ とおく. いま, それぞれの $\psi(\gamma^a \bigcup_{i \in I_i} C_i)$ が $a \in J_i$ $(i = 1, 2, 3)$. に応じて値が決まることを示せばよい.

(i) $I_1 = \{\ell\}$ より,

$$\psi(\gamma^a \bigcup_{i \in I_1} C_i) = \eta_{\ell+a} = \begin{cases} \alpha_1, & \text{if } a \in J_1; \\ \alpha_2, & \text{if } a \in J_2; \\ \alpha_3, & \text{if } a \in J_3. \end{cases}$$

(ii) 次に $\psi(\gamma^a \bigcup_{i \in I_2} C_i)$ を計算する. I_2 の特性関数 $f_2 : \mathbb{Z}_N \to \{0, 1\}$ は

$$f_2(x) = \frac{(\eta_x - \alpha_1)(\eta_x - \alpha_3)}{(\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)}$$

で与えられるので,

$$\begin{aligned} \psi(\gamma^a \bigcup_{i \in I_2} C_i) &= \sum_{x \in \mathbb{Z}_N} f_2(x) \psi(\gamma^{a+x} C_0) \\ &= \frac{1}{(\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)} \sum_{x \in \mathbb{Z}_N} \eta_{a+x}(\eta_x - \alpha_1)(\eta_x - \alpha_3) \end{aligned}$$

を得る. また,

$$\sum_{x \in \mathbb{Z}_N} \eta_x = -1$$

は明らか. さらに,

$$\begin{aligned} \sum_{x \in \mathbb{Z}_N} \eta_{a+x}\eta_x &= \frac{1}{N^2} \sum_{x \in \mathbb{Z}_N} (\sum_{\chi} G_q(\chi)\chi^{-1}(\gamma^{x+a}))(\sum_{\chi'} G_q(\chi')\chi'^{-1}(\gamma^x)) \\ &= \frac{1}{N} \sum_{\chi} G_q(\chi) G_q(\chi^{-1}) \chi^{-1}(\gamma^a) \\ &= \frac{1}{N}(1 + q \sum_{\chi \neq \chi_0} \chi^{-1}(-\gamma^a)) = \begin{cases} \frac{1-q}{N}, & \text{if } a \notin J_1; \\ \frac{1+q(q-2)}{N}, & \text{if } a \in J_1; \end{cases} \end{aligned}$$

が指標の直交性から得られる. よって, $\sum_{x\in\mathbb{Z}_N}\eta_{x+a}\eta_x^2$ を計算すれば十分である. ここで, $\tau(x)=(\eta_x-\alpha_2)/t$ とおいて, 代わりに $\sum_{x\in\mathbb{Z}_N}\tau(x+a)\tau(x)^2$ を計算することにする.

補題 2.1 より,

$$(-uI_1+vI_3)(-uI_1+vI_3)^{(-1)}=(k^*-\lambda^*)\cdot[0]+\lambda^*\mathbb{Z}_N$$

がある k^* と λ^* で成立する. 任意の $a\in\mathbb{Z}_N$ に対し, $\sum_{x\in\mathbb{Z}_N}\tau(x+a)\tau(x)$ は $(-uI_1+vI_3)(-uI_1+vI_3)^{(-1)}$ における $a\in\mathbb{Z}[\mathbb{Z}_N]$ の係数より, 以下を得る:

$$\sum_{x\in\mathbb{Z}_N}\tau(x+a)\tau(x)=\begin{cases}k^*, & \text{if } a=0;\\ \lambda^*, & \text{if } a\neq 0.\end{cases}$$

一方, $I_1=\{\ell\}$ より,

$$\sum_{x\in\mathbb{Z}_N}\tau(x+a)\tau(x)=-u\tau(\ell+a)+\sum_{x\in I_3}v\tau(x+a)$$

が成立しているので,

$$\sum_{x\in I_3}v\tau(x+a)=u\tau(\ell+a)+\begin{cases}k^*, & \text{if } a=0;\\ \lambda^*, & \text{if } a\neq 0;\end{cases}$$

が得られる. ここで, $a\neq 0$ のとき,

$$\begin{aligned}\sum_{x\in\mathbb{Z}_N}\tau(x+a)\tau(x)^2&=u^2\tau(\ell+a)+v\sum_{x\in I_3}v\tau(x+a)\\&=u^2\tau(\ell+a)+v(\lambda^*+u\tau(\ell+a))\\&=\begin{cases}v\lambda^*, & \text{if } \tau(\ell+a)=0, \text{ i.e., } a\in I_2+\ell=J_2;\\ v\lambda^*+u^2v+v^2u, & \text{if } \tau(\ell+a)=v, \text{ i.e., } a\in I_3+\ell=J_3;\end{cases}\end{aligned}$$

を得る. 同様に, $a=0$ のとき,

$$\sum_{x\in\mathbb{Z}_N}\tau(x+a)\tau(x)^2=-u^3+|I_3|v^3.$$

これらより, $\psi(\gamma^a\bigcup_{j\in I_2}C_j)$ は $a\in J_i$ に応じて一定の値を取る.

(iii) $\psi(\gamma^a\bigcup_{j\in I_3}C_j)$ についての計算は,

$$-1-\psi(\gamma^a\bigcup_{j\in I_1}C_j)-\psi(\gamma^a\bigcup_{j\in I_2}C_j)$$

で得られるので, $\psi(\gamma^a\bigcup_{j\in I_3}C_j)$ は $a\in J_i$ に応じて一定の値を取る.

これらより $|I_1|=1$ の場合の結果が得られる. $|I_3|=1$ の場合も同様である. □

3 三種の値を取るガウス周期: 十分条件

この章では, 命題 2.3 がいつ十分になるのかについて調べることにする.

命題 3.1. 以下の条件を満たす正整数 u, v, r, s が存在するとする.

(i) $t(-ur+vs) \equiv -1 \pmod{N}$;

(ii) $(N-1)q + t^2(-ur+vs)^2 = Nt^2(u^2r+v^2s)$.

ここで, t は全ての $G_q(\chi)$ $(\chi \in (C_0^{\perp})^* = (C_0)^{\perp} \setminus \{\chi_0\})$ を割る最大の p ベキとする. また, 連立方程式

$$\begin{cases} \sum_{x\in\mathbb{N}} x(x-1)t_x + \sum_{x\in\mathbb{N}} x(x+1)t_{-x} = u(u+1)r + v(v-1)s \\ \sum_{x\in\mathbb{N}} x(x+1)t_x + \sum_{x\in\mathbb{N}} x(x-1)t_{-x} = u(u-1)r + v(v+1)s \end{cases}$$

の非負整数解 $(t_x)_{x\in\mathbb{Z}\setminus\{0\}}$ が, 異なる整数 i_1, i_2 に対し, $x = i_1$ または i_2 のとき $t_x \neq 0$, そのほかのとき 0 とする. また, $t_{i_1} + t_{i_2} < N$ とする. このとき, ガウス周期 $\eta_a = \psi(\gamma^a C_0)$ $(0 \leq a \leq N-1)$ は 3 つの値をもつ.

証明: $y = \frac{-t(-ur+vs)-1}{N}$ とおく. 写像 $\tau : \mathbb{Z}_N \to \mathbb{C}$ を

$$\tau(a) = \frac{\psi(\gamma^a C_0) - y}{t}$$

で定義する. このとき,

$$\psi(\gamma^a C_0) + \frac{1}{N} = \frac{1}{N} \sum_{\chi\in(C_0^{\perp})^*} G_q(\chi)\chi^{-1}(\gamma^a)$$

より, $t \mid G_q(\chi)$ と仮定 (i) を使って, $\tau(a) \in \mathbb{Z}$ を得る. τ の離散フーリエ変換は,

$$\widehat{\tau}(\chi) = \frac{1}{\sqrt{N}} \sum_{a\in\mathbb{Z}_N} \tau(a)\chi(\gamma^a) = \begin{cases} \frac{1}{t\sqrt{N}} G_q(\chi), & \chi \text{が非自明のとき;} \\ \frac{-ur+vs}{\sqrt{N}}, & \chi \text{が自明のとき;} \end{cases}$$

で与えられる. パーセバルの公式より,

$$\sum_{a\in\mathbb{Z}_N} \tau(a)^2 = \sum_{\chi\in C_0^{\perp}} \widehat{\tau}(\chi)\overline{\widehat{\tau}(\chi)} = (N-1)\frac{q}{Nt^2} + \frac{(-ur+vs)^2}{N}.$$

仮定 (ii) より,

$$\sum_{a\in\mathbb{Z}_N} \tau(a)^2 = u^2r + v^2s \tag{3.1}$$

を得る. 一方,

$$\sum_{a\in\mathbb{Z}_N} \tau(a) = -ur + vs \tag{3.2}$$

は明らか. 式 (3.1) と (3.2) は, 以下のように変形される:

$$\sum_{x\in\mathbb{N}} x^2 t_x + \sum_{x\in\mathbb{N}} x^2 t_{-x} = u^2 r + v^2 s,\ \sum_{x\in\mathbb{N}} x t_x - \sum_{x\in\mathbb{N}} x t_{-x} = -ur + vs.$$

ここで, $t_x = |\{a \in \mathbb{Z}_N \,|\, \tau(a) = x\}|$ $(x \in \mathbb{N})$ である. このとき,

$$\sum_{x\in\mathbb{N}} x(x-1)t_x + \sum_{x\in\mathbb{N}} x(x+1)t_{-x} = u(u+1)r + v(v-1)s \tag{3.3}$$

と

$$\sum_{x\in\mathbb{N}} x(x+1)t_x + \sum_{x\in\mathbb{N}} x(x-1)t_{-x} = u(u-1)r + v(v+1)s \tag{3.4}$$

が得られる. 仮定より, 上記の式の非負整数解 $(t_x)_{x\in\mathbb{Z}\setminus\{0\}}$ が, $x = i_1$ または i_2 のとき $t_x \neq 0$, そのほかの $x \neq i_1, i_2$ のとき $t_x = 0$ を満たす. これより, $\tau(a) \in \{0, i_1, i_2\}$ がすべての $a \in \mathbb{Z}_N$ で成立. よって, $\eta_a = \psi(\gamma^a C_0)$ $(0 \le a \le N-1)$ はちょうど 3 つの値をとる. □

系 3.2. 以下の条件を満たす正整数 u, v, r, s が存在するとする.

(i) $t(-ur + vs) \equiv -1 \pmod{N}$;

(ii) $(N-1)q + t^2(-ur + vs)^2 = Nt^2(u^2 r + v^2 s)$.

ここで, t はすべての $G_q(\chi)$ $(\chi \in (C_0^{\perp})^* = (C_0)^{\perp} \setminus \{\chi_0\})$ を割る最大の p ベキとする. このとき, $u = v = r = 1$ かつ $s + 1 < N$, または, $u = v = s = 1$ かつ $r + 1 < N$ ならば, ガウス周期 $\eta_a = \psi(\gamma^a C_0)$ $(0 \le a \le N-1)$ は異なる 3 つの値をとり, 特に, 等差的である.

証明: $u = v = s = 1$ と仮定する. ($u = v = r = 1$ の場合も証明は同様である.) 式 (3.4) は

$$\sum_{x\in\mathbb{N}} x(x+1)t_x + \sum_{x\in\mathbb{N}\setminus\{1\}} x(x-1)t_{-x} = 2$$

に変形される. 連立方程式

$$\begin{cases} \sum_{x\in\mathbb{N}\setminus\{1\}} x(x-1)t_x + \sum_{x\in\mathbb{N}} x(x+1)t_{-x} = 2r \\ \sum_{x\in\mathbb{N}} x(x+1)t_x + \sum_{x\in\mathbb{N}\setminus\{1\}} x(x-1)t_{-x} = 2 \end{cases}$$

の非負整数解 $(t_x)_{x\in\mathbb{Z}\setminus\{0\}}$ は $t_1 = 1$, $t_{-1} = r$, その他の x に対し $t_x = 0$ を満たすか, $t_{-2} = 1$, $t_{-1} = r - 3$, その他の x に対し $t_x = 0$ を満たす. さらに, $\tau(a) \in \{0, -1, 1\}$ または $\tau(a) \in \{0, -1, -2\}$ である. よって, ガウス周期 η_a $(a \in \mathbb{Z}_N)$ は等差的な 3 つの値を取る. □

さらなる一般的な十分条件については, 論文 [3] を参照していただきたい.

4 三種の値を取るガウス周期: 例

この章では, 三種の値を取るガウス周期の例を与える.

4.1 Conic からの例

$L=\mathbb{F}_{p^f}$, $F=\mathbb{F}_{p^{3f}}$, $E=\mathbb{F}_{p^{6f}}$ とする. γ と ω を F と E の原始根で, $\gamma=\mathrm{Norm}_{E/F}(\omega)$ を満たすものとする. $N=\frac{p^{3f}-1}{p^f-1}$ とすると, $C_0^{(N,p^{3f})}=L^*<F^*$ である. このとき, F でのガウス周期は, $\mathrm{Tr}_{F/L}(\gamma^a)=0$ のとき $\eta_a=\psi(\gamma^a C_0^{(N,F)})=p^f-1$, さもなければ -1 であることに注意する.

$$S:=\{i\in\mathbb{Z}_N:\mathrm{Tr}_{F/L}(\gamma^i)=0\}$$

とすると, $|S|=p^f+1$ は明らか. 今, $\mathbb{Z}_N$ を $PG(2,p^f)$ の点集合と同一視し, S は $PG(2,p^f)$ の直線とみることができる (Singer 差集合である).

このとき, E における指数 N の乗法的指標に対するガウス和は, よく知られた Hasse-Davenport のリフトの公式から, S^2 を $\mathbb{Z}[\mathbb{Z}_N]$ 上で計算すれば良いことがわかる. この各係数が三種の値のみを取ることを見れば十分である. 任意の $a\in\mathbb{Z}_N$ に対し, S^2 における $[a]$ の係数は,

$$\{i\in\mathbb{Z}_N:\mathrm{Tr}_{F/L}(\gamma^{-i})=0,\mathrm{Tr}_{F/L}(\gamma^{i+a})=0\}=\mathcal{Q}\cap(S-a).$$

である. ここで, $\mathcal{Q}=\{i\in\mathbb{Z}_N:\mathrm{Tr}_{F/L}(\gamma^{-i})=0\}$, $S-a=\{x-a\mid x\in S\}$ とする. $\mathcal{Q}$ は $PG(2,p^f)$ の Conic であり, $S-a$ は直線を成すことに注意する. よって, 有限幾何でよく知られているように, $|\mathcal{Q}\cap(S-a)|=0,1,$ または 2 となり, ガウス周期 $\psi(\omega^a C_0^{(N,E)})$ $(0\le a\le N-1)$ はちょうど 3 つの値 $\alpha_1=p^{2f}+p^f-1$, $\alpha_2=p^f-1$, $\alpha_3=-p^{2f}+p^f-1$ をとることがわかる. また, 命題 2.5 より, circulant weighing matrix が得られることになる. (この circulant weighing matrix は系列としては新しくないが, ガウス周期から得られるという意味で面白い結果であると思われる.)

注意として, p が偶数の場合は, 集合 I_j らによる E^* の自然な分割が 3 クラスのアソシエーションスキームを成すことが既に [4] で示されている.

4.2 二種のガウス周期を取る場合からの例

$F=\mathbb{F}_{p^f}$, $E=\mathbb{F}_{p^{fe}}$ $(e>2)$ とし, $k|(p^f-1)$ とする. $N=(p^f-1)/k$, $N'=(p^{fe}-1)/k$ とすると, $C_0^{(N,F)}=C_0^{(N',E)}$ は明らか

今, ガウス周期 $\eta_a=\psi(\gamma^a C_0^{(N,F)})$ $(0\le a\le N-1)$ が, $S\subseteq\mathbb{Z}_N$ に対し, $a\in S$ かどうかで二種の値 α_1,α_2 を取ると仮定する. ここで γ は F の原始根である. ψ',ψ を E と F の標準加法的指標とすると,

$$\begin{aligned}\psi'(\omega^a C_0^{(N',E)})&=\sum_{x\in C_0^{(N,p^f)}}\xi_p^{\mathrm{Tr}_{p^f/p}(x\cdot(\mathrm{Tr}_{E/F}(\omega^a)))}=\psi(\mathrm{Tr}_{E/F}(\omega^a)C_0^{(N,p^f)})\\&=\begin{cases}k, & \text{if } \mathrm{Tr}_{E/F}(\omega^a)=0;\\ \alpha_1, & \text{if } \mathrm{Tr}_{E/F}(\omega^a)=\gamma^b \text{ and } b\in S;\\ \alpha_2, & \text{if } \mathrm{Tr}_{E/F}(\omega^a)=\gamma^b \text{ and } b\in\mathbb{Z}_N\setminus S;\end{cases}\end{aligned}$$

が得られる. ここで, ω は E の原始根とする. よって, ガウス周期 $\psi'(\omega^a C_0^{(N',E)})$ $(0 \le a \le N'-1)$ は三種の値 k, α_1, α_2 をとる. また, $C_0^{(N,F)}$, $F^* \setminus C_0^{(N,F)}$, $E^* \setminus F^*$ は 3 クラスのアソシエーションスキームを与える.

4.3 3つの1次元部分空間の和集合からの例

$q \equiv 1 \pmod 3$ とし, γ を $\mathbb{F}_{q^3}$ での位数 $k = 3(q-1)$ の元とする. また, $N = \frac{q^3-1}{k}$ とする. このとき, γ の $\mathbb{F}_q$ 上での最小多項式の次数は 3 である. このとき, $1, \gamma, \gamma^2$ は $\mathbb{F}_q$ 上線形独立で, さらに, $C_0^{(N,q^3)} = \langle\gamma\rangle = \{\lambda \cdot 1 \mid \lambda \in \mathbb{F}_q^*\} \cup \{\lambda \cdot \gamma \mid \lambda \in \mathbb{F}_q^*\} \cup \{\lambda \cdot \gamma^2 \mid \lambda \in \mathbb{F}_q^*\}$ と書ける. このとき, $\mathbb{F}_{q^3}$ の任意の非自明な指標 ψ' に対し,

$$\psi'(C_0^{(N,q^3)}) = \begin{cases} -3, & \psi'|_{\mathbb{F}_q}, \psi'|_{\mathbb{F}_q\gamma}, \psi'|_{\mathbb{F}_q\gamma^2} \text{ がすべて非自明のとき;} \\ -3+q, & \psi'|_{\mathbb{F}_q}, \psi'|_{\mathbb{F}_q\gamma}, \psi'|_{\mathbb{F}_q\gamma^2} \text{ のちょうど一つが自明のとき;} \\ -3+2q, & \psi'|_{\mathbb{F}_q}, \psi'|_{\mathbb{F}_q\gamma}, \psi'|_{\mathbb{F}_q\gamma^2} \text{ のちょうど2つが自明のとき;} \end{cases}$$

を得る. よって, ガウス周期 η_a $(0 \le a \le N-1)$ は等差的な 3 つの値 $\alpha_1 = -3, \alpha_2 = -3+q, \alpha_3 = -3+2q$ をもつ. 補題 2.4 より,

$$|I_1| = \frac{(q-1)^2}{3}, |I_2| = q-1, |I_3| = 1$$

を得る. また, $|I_3| = 1$ なので, 定理 2.6 より, $\bigcup_{i \in I_j} C_i^{(N,q3)}$ $(j = 1, 2, 3)$ は 3 クラスのアソシエーションスキームを与える.

4.4 部分体の積からの例

e, f を $e/\gcd(e,f) = 3$ を満たす正整数とし, $q = p^{\mathrm{lcm}(e,f)} = p^{3f}$, $C_0^{(N,q)}$ を $\mathbb{F}_q^*$ の $\mathbb{F}_{p^e}^*$ と $\mathbb{F}_{p^f}^*$ によって生成される部分群とする. このとき,

$$|C_0^{(N,q)}| = (p^e - 1)(p^f - 1)/(p^\ell - 1)$$

は明らかである. (ここで, $\ell = \gcd(e,f)$, $N = \frac{(p^{3f}-1)(p^\ell-1)}{(p^e-1)(p^f-1)}$ とする.) γ を $\mathbb{F}_q$ の原始根とする. このとき,

$$\psi(\gamma^a C_0^{(N,q)}) = \frac{1}{p^\ell - 1} \sum_{x \in \mathbb{F}_{p^e}^*} \sum_{y \in \mathbb{F}_{p^f}^*} \xi_p^{\mathrm{Tr}_{p^f}(y\mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a))} = \frac{1}{p^\ell - 1} \sum_{x \in \mathbb{F}_{p^e}^*} (p^f \delta_{\mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a)} - 1)$$

となる. ただし,

$$\delta_{\mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a)} = \begin{cases} 1, & \text{if } \mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a) = 0; \\ 0, & \text{otherwise;} \end{cases}$$

とする. また, ここで

$$W_a := \{x \in \mathbb{F}_{p^e} \mid \mathrm{Tr}_{p^{3f}/p^f}(x\gamma^a) = 0\}$$

とし, $s_a = |W_a|$ とすると,

$$\psi(\gamma^a C_0^{(N,q)}) = \frac{p^f(s_a - 1) - (p^e - 1)}{p^\ell - 1} = \frac{p^f s_a - p^f - p^e + 1}{p^\ell - 1}$$

が得られる. 一方, W_a は $\mathbb{F}_{p^e}$ の $\mathbb{F}_{p^\ell}$ 上の部分空間を成すので, $s_a = 1, p^\ell, p^{2\ell}, p^{3\ell} = p^e$ が得られる. $\mathbb{F}_{p^e}$ の $\mathbb{F}_{p^\ell}$ 上の基底は, $\mathbb{F}_{p^{3f}}$ の $\mathbb{F}_{p^f}$ 上の基底を成すことに注意すると, $W_a = \mathbb{F}_{p^e}$ はあり得ないことがわかる. よって, ガウス周期 $\psi(\gamma^a C_0^{(N,q)})$ $(0 \le a \le N-1)$ はちょうど3つの値

$$\alpha_1 = \frac{1-p^e}{p^\ell - 1},\ \alpha_2 = p^f + \frac{1-p^e}{p^\ell - 1},\ \alpha_3 = p^f(p^\ell + 1) + \frac{1-p^e}{p^\ell - 1}$$

をとる. 補題 2.2 より,

$$|I_1| = \frac{p^{3\ell} + p^{2f} - p^{2\ell+f} - p^{\ell+f}}{1 + p^\ell + p^{2\ell}},\ |I_2| = p^f - p^\ell,\ |I_3| = 1$$

が得られる. また, $|I_3| = 1$ より, 定理 2.6 を使って, $\bigcup_{i \in I_j} C_i^{(N,q)}$ $(j = 1, 2, 3,)$ が3クラスのアソシエーションスキームを成すことがわかる.

4.5 指数2型のガウス和からの例

今, 指数2型, つまり $[\mathbb{Z}_N^* : \langle p \rangle] = 2$ を仮定する. この場合, 位数 N の乗法的指標 χ に対するガウス和 $G_q(\chi)$ は [7] などで完全に計算されている. 論文 [2] では, 指数2型のガウス周期について, 特別な場合に計算している. 以下の結果は, 論文 [2] の定理 4.1 と定理 5.1 である.

定理 4.1. (i) ([2, 定理 4.1]) $N = p_1 \equiv 3 \pmod 4$ を $p_1 > 3$ なる素数とし, p を $\gcd(p, N) = 1$ かつ $\mathrm{ord}_N(p) = (N-1)/2$ を満たす素数とする. また, $f = (p_1 - 1)/2$ に対し, $q = p^f$ とおく. このとき, ガウス周期 $\psi(\gamma^a C_0^{(N,q)})$ $(a = 0, 1, \ldots, N-1)$ は高々3つの値

$$\alpha_1 = \frac{-2 + p^{\frac{f-h}{2}} b(p_1 - 1)}{2p_1},\ \alpha_2 = \frac{-2 + p^{\frac{f-h}{2}} c p_1 - p^{\frac{f-h}{2}} b}{2p_1},\ \alpha_3 = \frac{-2 - p^{\frac{f-h}{2}} c p_1 - p^{\frac{f-h}{2}} b}{2p_1} \tag{4.1}$$

をとる. ここで, h は $\mathbb{Q}(\sqrt{-p_1})$ の類数で, b と c は $b, c \not\equiv 0 \pmod p$, $4p^h = b^2 + p_1 c^2$, $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$ で決まる整数とする.

(ii) ([2, 定理 5.1]) p_1 と p_2 を such that $p_1 \equiv 1 (\mathrm{mod}\ 4)$ and $p_2 \equiv 3 (\mathrm{mod}\ 4)$ なる素数とし, $N = p_1 p_2$ とおく. p を $\mathrm{ord}_{p_1}(p) = p_1 - 1$, $\mathrm{ord}_{p_2}(p) = p_2 - 1$, $\mathrm{ord}_{p_1 p_2}(p) = (p_1-1)(p_2-1)/2$ を満たす素数とする. また, $f = (p_1 - 1)(p_2 - 1)/2$ に対し, $q = p^f$ とおく. このとき, ガウス周期 $\psi(\gamma^a C_0^{(N,q)})$ $(a = 0, 1, \ldots, N-1)$ は高々5つの値

$$\alpha_1 = \frac{-1 + \frac{1}{2} p^{\frac{f-h}{2}} (b + c p_1 p_2)}{N},\ \alpha_2 = \frac{-1 + p^{\frac{f}{2}} (-\frac{1}{2} b p^{\frac{-h}{2}} (-1 + p_1) + p_1)}{N},$$
$$\alpha_3 = \frac{-1 + \frac{1}{2} p^{\frac{f-h}{2}} (b - c p_1 p_2)}{N},\ \alpha_4 = \frac{-1 + p^{\frac{f}{2}} (-\frac{1}{2} b p^{\frac{-h}{2}} (-1 + p_2) - p_2)}{N},$$
$$\alpha_5 = \frac{-1 + p^{\frac{f}{2}} (p_1 + \frac{1}{2} b p^{\frac{-h}{2}} (-1 + p_1)(-1 + p_2) - p_2)}{N}$$

をとる．ここで，h は $\mathbb{Q}(\sqrt{-p_1p_2})$ の類数で，b と c は $b, c \not\equiv 0 \pmod{p}$, $4p^h = b^2 + p_1p_2c^2$, $bp^{\frac{f-h}{2}} \equiv 2 \pmod{p_1p_2}$ で決まる整数とする．

この定理より，直ちに以下が得られる．

命題 4.2. (i) 定理 4.1 (i) の表記のもとで，ガウス周期 $\psi(\gamma^a C_0^{(N,q)})$ $(a = 0, 1, \ldots, N-1)$ がちょうど3つの等差的な値を取るための必要十分条件は，$p_1 + 9 = 4p^h$ かつ $\pm 3p^{(f-h)/2} \equiv -2 \pmod{p_1}$ となることである．

(ii) 定理 4.1 (ii) の表記のもとで，$4p^{\frac{h}{2}} \equiv 0 \pmod{p_1 + p_2}$ かつ $2p^{\frac{f}{2}}(p_1 - p_2)/(p_1 + p_2) \equiv 2 \pmod{p_1p_2}$ のとき，ガウス周期 $\psi(\gamma^a C_0^{(N,q)})$ $(a = 0, 1, \ldots, N-1)$ は高々3つの値をとる．特に，ちょうど3つの等差的な値を取るための必要十分条件は，$p_1p_2 + 9 = 4p^h$ かつ $\pm 3p^{(f-h)/2} \equiv 2 \pmod{p_1p_2}$ となることである．

証明: (i) 定理 4.1 (i) の計算から，$\alpha_1, \alpha_2, \alpha_3$ が等差的であるための必要十分条件は，明らかに $b = \pm 3c$ である．$b, c \not\equiv 0 \pmod{p}$ より，$b = \pm 3c$ は $c \in \{-1, 1\}$ かつ $b = \pm 3$ と同値である．よって，結果を得る．

(ii) $4p^{\frac{h}{2}} \equiv 0 \pmod{p_1 + p_2}$ かつ $2p^{\frac{f}{2}}(p_1 - p_2)/(p_1 + p_2) \equiv 2 \pmod{p_1p_2}$ と仮定する．また，

$$b = \frac{2p^{\frac{h}{2}}(p_1 - p_2)}{p_1 + p_2}, \quad c = \pm\frac{4p^{\frac{h}{2}}}{p_1 + p_2}$$

とおく．b と c は整数で，必然的に $4p^h = b^2 + p_1p_2c^2$ と $bp^{\frac{f-h}{2}} \equiv 2 \pmod{p_1p_2}$ を満たす．$b = \frac{2p^{\frac{h}{2}}(p_1-p_2)}{p_1+p_2}$ かつ $c = \frac{4p^{\frac{h}{2}}}{p_1+p_2}$ のとき，$\alpha_1 = \alpha_2$ かつ $\alpha_3 = \alpha_4$ で，$b = \frac{2p^{\frac{h}{2}}(p_1-p_2)}{p_1+p_2}$ かつ $c = -\frac{4p^{\frac{h}{2}}}{p_1+p_2}$ のとき，$\alpha_1 = \alpha_4$ かつ $\alpha_2 = \alpha_3$ が成り立つ．どちらの場合も，ガウス周期 $\psi(\gamma^a C_0^{(N,q)})$ $(a = 0, 1, \ldots, N-1)$ は高々3つの値 $\alpha_1, \alpha_3, \alpha_5$ を取る．特に，これら $\alpha_1, \alpha_3, \alpha_5$ が等差的であるための必要十分条件は，明らかに $p_1 - p_2 = \pm 6$ (つまり，$b = \pm 3c$) である．$b, c \not\equiv 0 \pmod{p}$ より，条件 $b = \pm 3c$ は $c \in \{-1, 1\}$ かつ $b = \pm 3$ に同値である．よって，結果を得る． □

例 4.3. 命題 4.1 (i) の条件を満たす (p_1, p, h) について，$p_1 \leq 20000$ の範囲で計算機によって調べた結果，以下の5つを発見した: $(p_1, p, h) = (11, 5, 1), (23, 2, 3), (43, 13, 1), (67, 19, 1), (163, 43, 1)$. また，命題 4.1 (ii) の条件を満たす (p_1, p_2, p, h) について，$p_1p_2 \leq 20000$ の範囲で計算機によって調べた結果，以下の2つを発見した: $(p_1, p_2, p, h) = (5, 11, 2, 4), (11, 17, 7, 2)$.

4.6 計算機からの例

$p < 300$, $p^f < 2^{25}$, $3 < N < 1001$, $(p-1)|k = \frac{p^f-1}{N}$ という制限の下で，計算機を用いて調べた結果，表1に挙げた例を得た．この表では，すでに前章で得られた例は除いて挙げている．表の読み方についてであるが，例えば1行目の -7^{10} は，ガウス周期として -7 が10回出現することを意味している．AP の列は，ガウス周期が等差的であるとき ○，さもなければ × で記してある．また，AS の列は，集合 $I_j = \{a \in \mathbb{Z}_N : \psi(C_a^{(N,q)}) = \alpha_j\}$ $(j = 1, 2, 3)$ が3クラスのアソシエーションスキームを与えるかどうかを記している．さらに，系 3.2 はある条件下で，

p	f	N	ガウス周期の値	AP	AS	p	f	N	ガウス周期の値	AP	AS
11	3	19	$-7^{10}, 4^{6}, 15^{3}$	○	×	53	3	409	$-7^{358}, 46^{48}, 99^{3}$	○	×
7	7	29	$-414, -71^{21}, 272^{7}$	○	○	139	3	499	$-39^{378}, 100^{102}, 239^{19}$	○	×
29	3	67	$-13^{43}, 16^{18}, 45^{6}$	○	×	137	3	511	$-37^{391}, 100^{102}, 237^{18}$	○	×
37	3	67	$-21^{39}, 16^{18}, 53^{10}$	○	×	109	3	571	$-21^{471}, 88^{90}, 197^{10}$	○	×
23	3	79	$-7^{58}, 16^{18}, 39^{3}$	○	×	67	3	651	$-7^{586}, 60^{62}, 127^{3}$	○	×
2	11	89	$-9^{11}, -1^{56}, 7^{22}$	○	○	11	6	703	$-21^{591}, 100^{102}, 221^{10}$	○	×
5	6	93	$-7^{70}, 18^{20}, 43^{3}$	○	×	149	3	721	$-31^{586}, 118^{120}, 267^{15}$	○	×
37	3	201	$-7^{166}, 30^{32}, 67^{3}$	○	×	11	6	777	$-19^{661}, 102^{113}, 343^{3}$	×	×
67	3	217	$-21^{159}, 46^{48}, 113^{10}$	○	×	5	9	829	$-19^{712}, 106^{108}, 231^{9}$	○	×
2	18	219	$-19^{163}, 45^{47}, 109^{9}$	○	×	107	3	889	$-13^{787}, 94^{96}, 201^{6}$	○	×
61	3	291	$-13^{235}, 48^{50}, 109^{6}$	○	×	79	3	903	$-7^{826}, 72^{74}, 151^{3}$	○	×
79	3	301	$-21^{231}, 58^{60}, 137^{10}$	○	×	17	6	921	$-91^{676}, 198^{200}, 487^{45}$	○	×
83	3	367	$-19^{292}, 64^{66}, 147^{9}$	○	×	3	12	949	$-7^{870}, 74^{76}, 155^{3}$	○	×
11	6	399	$-37^{295}, 84^{86}, 205^{18}$	○	×	113	3	991	$-13^{883}, 100^{102}, 213^{6}$	○	×

表 1: $p < 300$, $p^f < 2^{25}$, $6 < N < 1001$, $N|\frac{p^f-1}{p-1}$ という制限の下での計算機による結果.

十分大きな N に対しても計算機での探索を可能にする. 実際, 以下のように系 3.2 の条件 ((i) $t(vs-ur)+1 \equiv 0 \pmod N$, (ii) $(N-1)q+t^2(vs-ur)^2 = (u^2r+v^2s)t^2N$, (iii) $u=v=1$ かつ $r=1$ または $s=1$) を満たす (p,f,N) を探索できる: g と h を $g=s-r$ と $h=r+s$ で定めると, $h=|g|+2$ は明らか. このとき,

(1) 任意の正整数 N, h $(1<h<N)$ に対し, $(Nh-(h-2)^2)/(N-1)$ を計算する (q/t^2 の値を知るため).

(2) この値が素数ベキ p^w のとき, N を法とする p の位数を計算し, f' とおく. さらに, 任意の非自明な指数 N の指標 χ に対し, すべての $G_{pf'}(\chi)$ を割る最大の p ベキを $p^{\theta'}$ とする.

(3) $f'-2\theta'$ が w を割るか調べる. このとき, $d=w/(f'-2\theta')$, $t=p^{\theta}=p^{d\theta'}$ とし, $(h-2)t+1 \equiv 0 \pmod N$ または $-(h-2)t+1 \equiv 0 \pmod N$ が成立するかを調べる.

このアルゴリズムで, $N<5000$ の範囲で計算機によって調べた結果, 以下の 3 つの新しい例を得た

$$(p,f,N,\theta) = (7,7,29,3), (13,13,53,6), (2,36,247,15). \tag{4.2}$$

定理 2.6 より, これらの場合はどれも 3 クラスのアソシエーションスキームを与えることもわかる.

二種の値をとるガウス周期の分類に関する予想 1.1 の類似として, 以下の予想を与える.

予想 4.4. $N\,|\,\frac{p^f-1}{p-1}$ のもとで, ガウス周期 $\psi(\gamma^a C_0^{(N,q)})$ $(a=0,1,\ldots,N-1)$ が等差的な 3 つの有理数値を持ち, かつ, $|I_1|=1$ または $|I_3|=1$ となる場合は, 章 4.3 の場合か, 例 4.3 の 7 つの場合か, (4.2) の 3 つの場合に限る.

5 まとめ

この論文では, 三種の値をとるガウス周期の分類に試み, 部分的であるが二種の値をとるガウス周期と同種の予想を導くことができた. 最後に現時点で分かっている, 三種の値をとるガウス周期の例 (無限系列) を表 2 に与えておく. (CW の列は, $I_1 - I_3$ が circulant weighing matrix を与えるか否かを示している. 記号 $\star$ は部分的に条件を満たす例を含んでいることを意味する.)

パラメータ	AP	AS	CW	参照
$p=2, q=p^{6f}, N=\frac{p^{3f}-1}{p^f-1}$	○	○	○	章 4.1
p odd, $q=p^{6f}, N=\frac{p^{3f}-1}{p^f-1}$	○	×	○	章 4.1
$q=p^{3f}, N=\frac{p^{3f}-1}{p^f-1}$, $\mathrm{ord}_{3(p^f-1)}(p^f)=3$	○	○	×	章 4.3
$q=p^{fe}$, $\frac{p^{fe}-1}{N} \mid p^f-1$, $\frac{(p^f-1)N}{p^{fe}-1} \mid \frac{p^f-1}{p-1}$, $Cay(\mathbb{F}_q, C_0^{(\frac{(p^f-1)N}{p^{fe}-1}, p^f)})$ is an SRG	$\star$	○	×	章 4.2
$q=p^{\mathrm{lcm}(e,f)}=p^{3f}$, $e/\gcd(e,f)=3$, $C_0^{(N,q)}=\mathbb{F}_{p^e}^* \cdot \mathbb{F}_{p^f}^*$	×	○	×	章 4.4
$q=p^f$, $N=p_1$, $[\mathbb{Z}_N^*, \langle p\rangle]=2$, $f=e(N-1)/2$ for any $e \in \mathbb{N}$	$\star$	○	×	章 4.5
$q=p^f$, $N=p_1p_2$, $[\mathbb{Z}_N^* : \langle p\rangle]=2$, $f=(p_1-1)(p_2-1)/2$	$\star$	○	×	章 4.5

表 2: 三種の値をとるガウス周期の例

参考文献

[1] R. Evans, H. D. L. Hollmann, C. Krattenthaler, Q. Xiang, Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets, *J. Combin. Theory, Ser. A*, **87** (1999), 74–119.

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

[3] T. Feng, K. Momihara, Q. Xiang, Three-valued Gauss periods, circulant weighing matrices and association schemes, `ArXiv:1409.8350`.

[4] T. Feng, K. Momihara, Three-class association schemes from cyclotomy, *J. Combin. Theory, Ser. A*, **120** (2013), 1202–1215.

[5] R. J. McEliece, Irreducible cyclic codes and Gauss sums. Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: *Theory of designs, finite geometry and coding theory*, in: Math. Centre Tracts, vol. 55, Math. Centrum, Amsterdam, 1974, pp. 179–196.

[6] B. Schmidt, C. White, All two-weight irreducible cyclic codes?, *Finite Fields Appl.*, **8** (2002), 1–17.

[7] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Ser. A*, **53** (2010), 2525–2542.