数理解析研究所講究録
第1844巻 2013年 153-163

強正則グラフ$Cay(\mathbb{F}_q, D)$と相対ガウス和の有理性について

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

概 要

Schmidt-White [14] にある11個の散在型の強正則グラフや有限体の部分体の乗法群から得られる自明な強正則グラフから出発して, 新たなパラメータで強正則グラフを構成したい. この論文では, その構成法の提示と関連する相対ガウス和の計算を行う.

キーワード: 強正則グラフ, ガウス和, 相対ガウス和

1 導入

この論文では, 位数qの有限体$\mathbb{F}_q$上のケーリーグラフ$Cay(\mathbb{F}_q, D)$を考え, どのようなうまい$D \subseteq \mathbb{F}_q$に対し, $Cay(\mathbb{F}_q, D)$が強正則グラフを成すかを考えたい. 特に, Dが$\mathbb{F}_q$の乗法部分群であるとき, 対応する強正則グラフは円分的であるとよぶ. 例えば, よく知られたPaleyグラフはパラメータ$(v, k, \lambda, \mu) = (4t+1, 2t, t-1, t)$を持つ円分的強正則グラフである. 今後, pを素数, fを正整数, $q := p^f$, kを$q-1$を割る正整数, γを$\mathbb{F}_q$の一つの原始根とする. また, $C_i^{(k,q)} = \gamma^i\langle\gamma^k\rangle$ $(0 \le i \le k-1)$と表記する. これらのコセットを円分類と呼ぶことにする.

円分的強正則グラフの存在性について以下の予想が知られている.

予想 1.1. *([14])* kを$k \mid \frac{p^f-1}{p-1}$を満たす正整数とし, $C_0^{(k,p^f)} = -C_0^{(k,p^f)}$を仮定する. このとき, $Cay(\mathbb{F}_{p^f}, C_0^{(k,p^f)})$は以下のいずれかである.

(1) *(部分体型)* $d \mid f$なるdに対し, $C_0^{(k,p^f)} = \mathbb{F}_{p^d}^*$,

(2) *(準原始型)* $-1 \in \langle p\rangle \le (\mathbb{Z}/k\mathbb{Z})^*$,

(3) *(散在型)* $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0^{(k,p^f)})$は表 *1* の *11* 個のいずれか.

[1]〒 860-8555, 熊本県熊本市黒髪 2-40-1, 熊本大学教育学部数学科, Email: momihara@educ.kumamoto-u.ac.jp
この研究は, 科学研究費補助金 (研究活動スタートアップ 23840032) の補助を受けています.

表 1: 11 個の散在型

No.	k	p	f	$e := [(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle]$
1	11	3	5	2
2	19	5	9	2
3	35	3	12	2
4	37	7	9	4
5	43	11	7	6
6	67	17	33	2
7	107	3	53	2
8	133	5	18	6
9	163	41	81	2
10	323	3	144	2
11	499	5	249	2

この予想に関する最近の進展については, F. Wu の論文 [15] を参照されたい. 最近, 論文 [5, 6, 7] の中で, 表 1 にある No. 1, 5, 8 以外の 8 個の強正則グラフをある種の無限系列に拡張することに成功している. ただし, 得られた強正則グラフは円分的でなく, いくつかの円分類をうまく規則的に取ることによって得られた. また, その証明は, 次の章に定義する指数 2 型や 4 型のガウス和と呼ばれる古典的な指標和の計算に基づいて行われている. ここでの 2 や 4 という数字は, 表にあるパラメータ e の 2 や 4 に対応している. しかし, 指数が 6 以上のガウス和の完全な計算は, 現状では非常に困難であると思われるため, 表 1 にある No. 5, 8 といった指数 6 型のガウス和の計算が必要であろうケースは, これまでの手法では一般化は難しいと思われる.

この論文では, 表 1 の例や部分体型の円分的強正則グラフをある種の無限系列に拡張するためには, 実はガウス和の計算に基づく必要はなく, 相対ガウス和と呼ばれる指標和の計算がより本質的であることを示し, 特にその計算に基づいて表 1 の No. 5 や部分体型の円分的強正則グラフを含んだいくつかの新しい強正則グラフの無限系列を得た.

2 相対ガウス和の有理性

この論文では, 素数 p_1 に対し, $k = p_1^m$ と仮定する. これより, 表 1 の No. 8 などは除外されることになる. No. 8 も含めた一般の状況に対する結果については [12] を参照されたい.

2.1 準備

$\mathbb{F}_q$ の標準加法的指標 ψ と $\mathbb{F}_q$ のある乗法的指標 χ に対し, 指標和

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

をガウス和と呼ぶ. ここでは, 以下のガウス和の計算に関するよく知られた性質を用いる.

(i) χ が非自明のとき, $G_f(\chi)\overline{G_f(\chi)} = q$.

(ii) p を $\mathbb{F}_q$ の標数とする. このとき, $G_f(\chi^p) = G_f(\chi)$.

(iii) $G_f(\chi^{-1}) = \chi(-1)\overline{G_f(\chi)}$.

(iv) χ が自明のとき, $G_f(\chi) = -1$.

(v) $\sigma_{a,b}(G_f(\chi)) = \chi^{-a}(b)G_f(\chi^a)$. ここで, k を χ の位数とし, $\sigma_{a,b}$ を $\gcd(a,k) = \gcd(b,p) = 1$ に対し, $\sigma_{a,b}(\zeta_k) = \zeta_k^a$ かつ $\sigma_{a,b}(\zeta_p) = \zeta_p^b$ で決まる $\mathbb{Q}(\zeta_{kp})$ の自己同型とする.

これまで, 小さな位数 k に対し, ガウス和の計算が行われてきた. 例えば, 位数 2 の場合のガウス和の計算は古くから知られている. また, 準原始的な場合 (すなわち $-1 \in \langle p \rangle \leq (\mathbb{Z}/k\mathbb{Z})^*$ なる場合) に対しても, ガウス和の値は完全に決定されており, また, これらの計算に基づいて様々な組合せ構造の存在性が示されてきた. 様々な結果および歴史については, [2] を参照されたい. 一方, 最近活発に研究されているケースは, 指数 e 型と呼ばれるケースであり, 以下のようなものである: $e = [(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle]$ とする. また, p の $\mathbb{Z}/k\mathbb{Z}$ における位数 $\phi(k)/e$ を f と書く. この f に対し, $\mathbb{F}_{p^f}$ 上のガウス和 $G_f(\chi_k)$ を指数 e 型と呼ぶ. ここで, χ_k は $\mathbb{F}_{p^f}$ の位数 k の乗法的指標とする. 特に, $e = 2, 4$ の場合は, このガウス和はほとんどの場合で値が決定している ([1, 4, 9, 10, 11, 18]). しかしながら, $e > 4$ の場合については, その計算は困難であるように思え, また, 可能だとしても非常に複雑であることが予想される (指数 4 の場合にすでに非常に複雑である). そこで, ガウス和を扱う代わりに, 相対ガウス和とよばれる指標和を用いる.

f, f' を $f \mid f'$ を満たす正整数とし, χ' を $\mathbb{F}_{p^{f'}}$ の乗法的指標, χ を χ' の $\mathbb{F}_{p^f}$ への制限とする. このとき,

$$\vartheta(\chi', \chi) := \frac{G_{f'}(\chi')}{p^{\frac{f'-f}{2}} G_f(\chi)}$$

を相対ガウス和と呼ぶ. $p^{\frac{f'-f}{2}}$ で割るのは, χ' と χ が非自明のときの $\vartheta(\chi', \chi)$ の絶対値が 1 となるようにするためである. 今, いつ $\vartheta(\chi', \chi) = 1$ が成立するのかに関心がある. 相対ガウス和の概念は, 山本 [16] が初めて定義した概念で, あるクラスのアダマール行列の構成のために用いられた.

最後に次の章の準備として, 以下の 3 つの結果を挙げておく.

定理 2.1. *(Davenport-Hasse のリフトの公式 [2])* χ を $\mathbb{F}_q = \mathbb{F}_{p^f}$ の非自明な乗法的指標とし, χ' を χ の $\mathbb{F}_{q'} = \mathbb{F}_{p^{fs}}$ へのリフトとする. このとき, 以下が成立する.

$$G_{fs}(\chi') = (-1)^{s-1}(G_f(\chi))^s.$$

定理 2.2. *(Davenport-Hasse の積の公式 [2])* η を $\mathbb{F}_q = \mathbb{F}_{p^r}$ の位数 $\ell > 1$ の乗法的指標とする. $\mathbb{F}_q$ の非自明な乗法的指標 χ に対し, 以下が成立する.

$$G_f(\chi) = \frac{G_f(\chi^\ell)}{\chi^\ell(\ell)} \prod_{i=1}^{\ell-1} \frac{G_f(\chi\eta^i)}{G_f(\eta^i)}.$$

補題 2.3. *([16])* χ' を $\mathbb{F}_{p^{f'}}$ の位数 k' の乗法的指標とし, χ を χ' の $\mathbb{F}_{p^f}$ への制限とする. ここで, f, f' は $f \mid f'$ を満たすものとする. χ が $\mathbb{F}_{p^f}$ で非自明ならば, 以下が成立する.

$$p^{\frac{f-f'}{2}}\vartheta_p(\chi', \chi) = \sum_{\mathrm{Tr}_{p^{f'}/p^f}(x)=1} \chi'(x).$$

2.2 相対ガウス和

この章では, 以下の表記を用いる.

- 素数 p_1 に対し, $k = p_1^m$ とする.
- f を p の k を法とする位数とし, $q = p^f$ とする.
- ζ_s で 1 の原始 s 乗根を表記する.
- $K := \mathbb{Q}(\zeta_k), M := K(\zeta_p) = \mathbb{Q}(\zeta_k, \zeta_p)$.
- O_K, O_M を K, M それぞれの整数環とする.
- $j \in (\mathbb{Z}/k\mathbb{Z})^*$ に対し, $\sigma_j \in \mathrm{Gal}(M/\mathbb{Q}(\zeta_p))$ を $\sigma_j(\zeta_k) = \zeta_k^j$ で定める.

P を O_K の p の上の素イデアルとすると, O_M の素イデアル $\mathfrak{p}$ が存在して, O_M では $PO_M = \mathfrak{p}^{p-1}$ と分解される. 今, $P_j = \sigma_j(P)$, $\mathfrak{p}_j = \sigma_j(\mathfrak{p})$ とすると, $P_jO_M = \mathfrak{p}_j^{p-1}$ が成立している. 今, T を $(\mathbb{Z}/k\mathbb{Z})^*/\langle p \rangle$ の代表系とすると, $pO_K = \prod_{j\in T} P_j$ が成立しており, よって, $pO_M = \prod_{j\in T} \mathfrak{p}_j^{p-1}$ が従う.

χ_P で素イデアル P に付随する $O_K/P(\simeq \mathbb{F}_{p^f})$ の Teichmüller 指標を表記する. 今後, この指標を $\mathbb{F}_{p^f}$ の位数 k の指標として使う.

定理 2.4. *(Stickelberger's relation [2, 8])* k を正整数とし, p を $\gcd(p, k) = 1$ を満たす素数, f を p の k を法とする位数とする. このとき, O_M の P の上の素イデアル $\mathfrak{p}$ に対し,

$$G_f(\chi_P^{-1})O_M = \mathfrak{p}^{(p-1)\sum_{t\in T}\sum_{i=0}^{f-1}\langle tp^i/k\rangle\sigma_t^{-1}} \subseteq O_M$$

が成立する. ここで, $\langle x \rangle$ は有理数 x に対し, 整数部分の切り捨てを意味する.

また, $G_f(\chi^a)G_f(\chi^{-a}) = \pm p^f$ より,

$$G_f(\chi_P)O_M = \mathfrak{p}^{(p-1)(f\sum_{t\in T}\sigma_t - \sum_{t\in T}\sum_{i=0}^{f-1}\langle tp^i/k\rangle\sigma_t^{-1})}$$

も成立する.

以後, p_1 を奇素数, $h = p_1$, $k = p_1^m$, $k' = p_1^{m+1}$ とし, p が h, k, k' のどれを法としても指数が e であると仮定する. また, $q = p^f = p^{p_1^{m-1}(p_1-1)/e}$, $q' = p^{f'} = p^{p_1^m(p_1-1)/e}$ とおく. O_K, $O_{K'}$, O_M, $O_{M'}$, O_L, $O_{L'}$ をそれぞれ $\mathbb{Q}(\zeta_k)$, $\mathbb{Q}(\zeta_{k'})$, $\mathbb{Q}(\zeta_k, \zeta_p)$, $\mathbb{Q}(\zeta_{k'}, \zeta_p)$, $\mathbb{Q}(\zeta_{p^f-1})$, $\mathbb{Q}(\zeta_{p^{f'}-1})$ の整数環と

し, $P \subseteq O_K$ を p の上の素イデアル, $\mathfrak{p} \subseteq O_M$ を P の上の素イデアルとする. また, $\mathfrak{p}' \subseteq O_{M'}$ を $\mathfrak{p}$ の上の素イデアルとし, $P' = \mathfrak{p}' \cap O_{K'}$ とおく.

T' を $(\mathbb{Z}/k'\mathbb{Z})^*/\langle p \rangle$ の代表系とすると, $\{\sigma_j(P)(=: P_j) \mid j \in T\}$ と $\{\sigma'_j(P)(=: P'_j) \mid j \in T'\}$ の間には自然な1対1対応 $P_j = P'_j \cap O_K$ がある. ここで, $\sigma'_j \in \mathrm{Gal}(\mathbb{Q}(\zeta_{k'p})/\mathbb{Q}(\zeta_p))$ は $\sigma'_j(\zeta_{k'}) = \zeta_{k'}^j$ を満たすものとする. 今, $pO_K = \prod_{j \in T} P_j$ の両辺に $O_{K'}$ を掛けると, $pO_{K'} = \prod_{j \in T'} P'_j$ に注意して, $P_j O_{K'} = P'_j$ を得る. さらに, $O_{M'}$ を $P_j O_{K'} = P'_j$ の両辺に掛けて, $P_j O_{M'} = P'_j O_{M'} = \mathfrak{p}'^{p-1}_j$ を得る. ここで $\mathfrak{p}'_j \subseteq O_{M'}$ は P'_j の上の素イデアルとする. 一方, $P_j O_{M'} = \mathfrak{p}_j^{p-1} O_{M'}$ より, $\mathfrak{p}_j O_{M'} = \mathfrak{p}'_j$ が得られる.

$\mathfrak{P} \subseteq O_L$ と $\mathfrak{P}' \subseteq O_{L'}$ それぞれ P と P' の上の素イデアルとする. このとき, $O_L/\mathfrak{P} = \{\alpha + \mathfrak{P} \mid \alpha \in O_K/P\}$, および, $\alpha \in O_K$ に対し

$$\chi_{\mathfrak{P}}^{\frac{p^f-1}{k}}(\alpha + \mathfrak{P}) = \chi_P(\alpha + P)$$

が成立していることに注意する. よって,

$$G_f(\chi_{\mathfrak{P}}^{a\frac{p^f-1}{k}}) = G_f(\chi_P^a)$$

が従う. また, $O_L/\mathfrak{P}$ の代表系として $\{0\} \cup \{\zeta_{p^f-1}^i \mid 0 \le i \le p^f - 1\}$ が取れ,

$$\chi_{\mathfrak{P}}(\zeta_{p^f-1}^i + \mathfrak{P}) = \zeta_{p^f-1}^i$$

が成立している. よって, $\alpha \in (\zeta_{p^f-1} + \mathfrak{P}) \cap O_K$ と $\beta \in (\zeta_{p^{f'}-1} + \mathfrak{P}') \cap O_{K'}$ に対し,

$$\begin{aligned} \chi_P(\alpha^i + P) &= \chi_{\mathfrak{P}}(\zeta_{p^f-1}^{\frac{p^f-1}{k}i} + \mathfrak{P}) = \chi_{\mathfrak{P}'}^{\frac{p^f-1}{k}}(\zeta_{p^{f'}-1}^{\frac{p^{f'}-1}{p^f-1}i} + \mathfrak{P}') \\ &= \chi_{\mathfrak{P}'}^{p_1}(\zeta_{p^{f'}-1}^{\frac{p^{f'}-1}{kp_1}i} + \mathfrak{P}') = \chi_{P'}^{p_1}(\beta^i + P') \end{aligned} \tag{2.1}$$

が成立する. ここで, $\alpha + P$ と $\beta + P'$ は O_K/P と $O_{K'}/P'$ の原始根になっていることに注意する.

補題 2.5. $\chi_{P'}$ と χ_P を P' と P に付随する *Teichmüller* 指標とする. このとき,

$$(\vartheta(\chi_{P'}, \chi_P) :=) \frac{G_{f'}(\chi_{P'})}{p^{\frac{\phi(k)(p_1-1)}{2e}} G_f(\chi_P)}$$

は1の $2k'$ 乗根.

証明: まず, $\vartheta(\chi_{P'}, \chi_P) \in \mathbb{Q}(\zeta_{k'})$ をみる. $(p^{f'}-1)/k' \equiv (p^f-1)/k \pmod{p^f-1}$ より,

$$\chi_{\mathfrak{P}'}^{\frac{p^{f'}-1}{k'}}(\zeta_{p^f-1} + \mathfrak{P}') = \chi_{\mathfrak{P}}^{\frac{p^f-1}{k}}(\zeta_{p^f-1} + \mathfrak{P})$$

が成立するので, χ_P は $\chi_{P'}$ の $\mathbb{F}_{p^f}$ への制限である. よって, 補題 2.3 より, $\vartheta(\chi_{P'}, \chi_P) \in \mathbb{Q}(\zeta_{k'})$ が従う.

$[a]_k$ で $[a]_k \equiv a \pmod{k}$, $0 \leq [a]_k \leq k-1$ を満たす整数とする. このとき

$$k\sum_{i=0}^{f-1}\left\langle \frac{tp^i}{k} \right\rangle = \sum_{i=0}^{f-1}[tp^i]_k$$

は明らか. 一方, これは以下のように変形できる.

$$\begin{aligned}\sum_{x\in\langle p\rangle\leq(\mathbb{Z}/k\mathbb{Z})^*}[tx]_k &= \sum_{y=0}^{\frac{k}{h}-1}\sum_{z\in\langle p\rangle\leq(\mathbb{Z}/h\mathbb{Z})^*} hy+[tz]_h \\ &= k(\frac{k}{h}-1)\phi(h)/2e + \frac{k}{h}\sum_{z\in\langle p\rangle\leq(\mathbb{Z}/h\mathbb{Z})^*}[tz]_h.\end{aligned}$$

ここで, $T \pmod{h}$ は $(\mathbb{Z}/h\mathbb{Z})^*/\langle p\rangle$ の代表系になっていることに注意する. よって,

$$\sum_{i=0}^{f-1}\left\langle \frac{tp^i}{k} \right\rangle = \frac{\phi(k)-\phi(h)}{2e} + \frac{1}{h}\sum_{z\in\langle p\rangle\leq(\mathbb{Z}/h\mathbb{Z})^*}[tz]_h$$

を得る. 同様に

$$\sum_{i=0}^{f'-1}\left\langle \frac{tp^i}{k'} \right\rangle = \frac{\phi(k')-\phi(h)}{2e} + \frac{1}{h}\sum_{z\in\langle p\rangle\leq(\mathbb{Z}/h\mathbb{Z})^*}[tz]_h$$

が得られる. 定理 2.4 より,

$$G_{f'}(\chi_{P'})O_{M'} = \mathfrak{p}'^{(p-1)((f'-\frac{\phi(k')-\phi(h)}{2e})\sum_{t\in T'}\sigma_t - \sum_{t\in T'}(\frac{1}{h}\sum_{z\in\langle p\rangle\leq(\mathbb{Z}/h\mathbb{Z})^*}[tz]_h)\sigma_t^{-1})}$$

が得られ, また $\mathfrak{p}O_{M'} = \mathfrak{p}'$ に注意して,

$$G_f(\chi_P)O_{M'} = \mathfrak{p}'^{(p-1)((f-\frac{\phi(k)-\phi(h)}{2e})\sum_{t\in T'}\sigma_t - \sum_{t\in T'}(\frac{1}{h}\sum_{z\in\langle p\rangle\leq(\mathbb{Z}/h\mathbb{Z})^*}[tz]_h)\sigma_t^{-1})}$$

を得る. よって, $pO_{M'} = \mathfrak{p}'^{(p-1)\sum_{i\in T'}\sigma_t}$ より, $p^{\frac{\phi(k')-\phi(k)}{2e}}G_f(\chi_P)O_{M'} = G_{f'}(\chi_{P'})O_{M'}$, つまり, $\vartheta(\chi_{P'},\chi_P)$ は $O_{M'}$ の単数であることがわかる. 一方, $\vartheta(\chi_{P'},\chi_P) \in \mathbb{Q}(\zeta_{k'})$ より, $O_{K'}$ の単数である. さらには, $\vartheta(\chi_{P'},\chi_P)$ の $O_{K'}$ における共役はすべて絶対値 1 をもつ. よって, $\vartheta(\chi_{P'},\chi_P)$ は 1 の $2k'$ 乗根である. □

補題 2.6. $d = 2\gcd(k', p-1)$ とすると, 以下が成立する.

$$\vartheta(\chi_{P'},\chi_P)^d = 1.$$

証明: σ を $\sigma(\zeta_{pk'}) = \zeta_{pk'}^{k'\ell+p}$ で決まる $\mathrm{Gal}(\mathbb{Q}(\zeta_p, \zeta_{k'})/\mathbb{Q}(\zeta_p))$ の元とする. ここで, ℓ は k' の p を法とする逆元とする. ψ' と ψ を $\mathbb{F}_{q'}$ と $\mathbb{F}_q$ の標準加法的指標とする. このとき, 以下を得る.

$$\begin{aligned}
\sigma\left(\frac{G_{f'}(\chi_{P'})}{G_f(\chi_P)}\right) &= \sigma\left(\frac{\sum_{\alpha\in\mathbb{F}_{q'}}\psi'(\alpha)\chi_{P'}(\alpha)}{\sum_{\beta\in\mathbb{F}_q}\psi(\beta)\chi_P(\beta)}\right) \\
&= \frac{\sum_{\alpha\in\mathbb{F}_{q'}}\psi'((k'\ell+p)\alpha)\chi_{P'}^{k'\ell+p}(\alpha)}{\sum_{\beta\in\mathbb{F}_q}\psi((k'\ell+p)\beta)\chi_P^{k'\ell+p}(\beta)} \\
&= \frac{\sum_{\alpha\in\mathbb{F}_{q'}}\psi'(\alpha)\chi_{P'}^{p}(\alpha)}{\sum_{\beta\in\mathbb{F}_q}\psi(\beta)\chi_P^{p}(\beta)} \\
&= \frac{G_{f'}(\chi_{P'}^p)}{G_f(\chi_P^p)} = \frac{G_{f'}(\chi_{P'})}{G_f(\chi_P)},
\end{aligned}$$

つまり, $\sigma(\vartheta(\chi_{P'}, \chi_P)) = \vartheta(\chi_{P'}, \chi_P)$. 一方, 補題 2.5 より, ある s が存在して $\vartheta(\chi_{P'}, \chi_P)^2 = \zeta_{k'}^s$ と書けるので,

$$\sigma(\vartheta(\chi_{P'}, \chi_P)^2) = \vartheta(\chi_{P'}, \chi_P)^{2(k'\ell+p)} = \vartheta(\chi_{P'}, \chi_P)^{2p}$$

が従う. よって, $\vartheta(\chi_{P'}, \chi_P)^{2(p-1)} = 1$ を得る. さらに, $\vartheta(\chi_{P'}, \chi_P)^{2k'} = 1$ と組み合わせて, $\vartheta(\chi_{P'}, \chi_P)^{2\gcd(k', p-1)} = 1$ を得る. □

以下の定理がこの章の主定理である.

定理 2.7. $\gcd(k', p-1) = 1$ であるとき, $\vartheta(\chi_{P'}, \chi_P) = 1$ が成立する.

証明: 補題 2.6 より, $\vartheta(\chi_{P'}, \chi_P) = -1$ または 1 が成立している. 今, $p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P)\vartheta(\chi_{P'}, \chi_P)$ の $\lambda := 1 - \zeta_{p_1^{m+1}}$ を法とした値を計算する. $p^{\frac{\phi(k)(p_1-1)}{2e}} \equiv 1 \pmod{\lambda}$ と $G_{f'}(\chi_{P'}) \equiv -1 \pmod{\lambda}$ は $G_{f'}(\chi_{P'})$ の定義から明らか. 一方,

$$\begin{aligned}
G_{f'}(\chi_{P'}) &= p^{\frac{\phi(k')-\phi(k)}{2e}} G_f(\chi_P)\vartheta(\chi_{P'}, \chi_P) \\
&\equiv -\vartheta(\chi_{P'}, \chi_P) \pmod{\lambda}
\end{aligned}$$

を得る. ここで、もし $\vartheta(\chi_{P'}, \chi_P) = -1$ ならば, $p_1 \mid 2$ となって矛盾が得られる. □

注意 2.8. 定理 *2.2* より, ガロア群の作用を考えれば, $\gcd(a, k') = 1$ なる任意の a に対し, $\vartheta(\chi_{P'}^a, \chi_P^a) = 1$ は明らか.

系 2.9. $\gcd(k', p-1) = 1$ のとき, $p_1^m \nmid t$ でない任意の t に対し, $\vartheta(\chi_{P'}^t, \chi_P^t) = 1$ が成立する.

証明: $\gcd(a, k) = 1$ なる a に対し, $t = a \cdot \gcd(t, k)$ とおく. r' と r をそれぞれ, $k'/\gcd(t, k')(=: u')$ と $k/\gcd(t, k)(=: u)$ を法とする p の位数とする. このとき, $r' = rp_1$ と $u' = up_1$ は明らか. 今, $J = \mathbb{Q}(\zeta_u)$, $J' = \mathbb{Q}(\zeta_{u'})$, $H = \mathbb{Q}(\zeta_{p^r-1})$, $H' = \mathbb{Q}(\zeta_{p^{r'}-1})$, $R = P \cap O_J$, $R' = P' \cap O_{J'}$, $\mathfrak{R} = \mathfrak{P} \cap O_H$, $\mathfrak{R}' = \mathfrak{P}' \cap O_{H'}$ とおく. このとき,

$$\chi_{\mathfrak{R}}^{a\frac{p^r-1}{u}}(\zeta_{p^f-1}^{i\frac{p^f-1}{p^r-1}} + \mathfrak{R}) = \chi_{\mathfrak{P}}^{a\frac{p^f-1}{u}}(\zeta_{p^f-1}^i + \mathfrak{P}) = \chi_{\mathfrak{P}}^{\frac{p^f-1}{k}t}(\zeta_{p^f-1}^i + \mathfrak{P})$$

より, $\chi_{\mathfrak{P}}^{\frac{p^f-1}{k}t}$ は, $\mathbb{F}_{p^f}$ への $\chi_{\mathfrak{R}}^{a\frac{p^r-1}{u}}$ のリフトである. 同様に, $\chi_{\mathfrak{P}'}^{\frac{p^{f'}-1}{k'}t}$ は $\mathbb{F}_{p^{f'}}$ への $\chi_{\mathfrak{R}'}^{a\frac{p^{r'}-1}{u'}}$ のリフトである. ここで, Davenport-Hasse のリフトの公式より以下を得る.

$$\begin{aligned}\vartheta(\chi_{P'}^t,\chi_P^t) &= \frac{G_{f'}(\chi_{P'}^t)}{p^{\frac{\phi(k')-\phi(k)}{2e}}G_f(\chi_P^t)} = \frac{G_{f'}(\chi_{\mathfrak{P}'}^{\frac{p^{f'}-1}{k'}t})}{p^{\frac{\phi(k')-\phi(k)}{2e}}G_f(\chi_{\mathfrak{P}}^{\frac{p^f-1}{k}t})}\\ &= \frac{(-1)^{f'/r'-1}(G_{r'}(\chi_{\mathfrak{R}'}^{a\frac{p^{r'}-1}{u'}}))^{f'/r'}}{(-1)^{f/r-1}p^{\frac{\phi(k')-\phi(k)}{2e}}(G_r(\chi_{\mathfrak{R}}^{a\frac{p^r-1}{u}}))^{f/r}}\\ &= \frac{1}{p^{\frac{\phi(k')-\phi(k)}{2e}}}\cdot\left(\frac{G_{r'}(\chi_{R'}^a)}{G_r(\chi_R^a)}\right)^{f/r}.\end{aligned}$$

さらに, 定理 2.7 より, 上の値は

$$\frac{1}{p^{\frac{\phi(k')-\phi(k)}{2e}}}\cdot\left(p^{\frac{r'-r}{2}}\vartheta(\chi_{R'},\chi_R)\right)^{f/r}=1$$

となり主張が得られた. □

3 強正則グラフの構成法

q をある素数冪とし, $C_i^{(k,q)}=\gamma^i\langle\gamma^k\rangle$, $0\le i\le k-1$ を $\mathbb{F}_q$ の位数 k の円分類とする. このとき, $\mathbb{F}_q$ の部分集合 $D=\bigcup_{i\in I}C_i^{(k,q)}$ がある強正則グラフの連結集合 (組合せデザインの理論では部分差集合の概念に一致する) であることをチェックするには, 指標和 $\psi(aD):=\sum_{x\in D}\psi(ax)$ をすべての $a\in\mathbb{F}_q^*$ に対し計算し, これらがちょうど二つの値を取ることを示せばよい. ここで, ψ は $\mathbb{F}_q$ の標準加法的指標とする. (この強正則グラフをなすための必要十分条件については [3, p. 134] などを参照されたい.)

ここで, $\psi(aD)$ は指標の直交性から以下のようにガウス和を使って表せる.

$$\psi(aD)=\frac{1}{k}\sum_{\chi\in C_0^\perp}G(\chi^{-1})\sum_{i\in I}\chi(a\gamma^i).$$

上の式において, $C_0^\perp$ は $\mathbb{F}_{p^f}$ 上で自明な乗法的指標からなる群とする.

この章でも, 前章と同様に以下のことを仮定する. p_1 を奇素数とし, $h=p_1$, $k=p_1^m$, $k'=p_1^{m+1}$, p を h,k,k' のいずれを法としても指数が e である素数とする. このとき, 以下が成立する.

定理 3.1. p と p_1 は $\gcd(p_1,p-1)=1$ を満たすと仮定する. ここで, $f=\phi(k)/e$, $f'=\phi(k')/e$, $q=p^f$, $q'=p^{f'}$ とし, $\mathbb{F}_q$ および $\mathbb{F}_{q'}$ の部分集合として

$$D=\bigcup_{i=0}^{p_1^{m-1}-1}C_i^{(p_1^m,q)},\ D'=\bigcup_{i=0}^{p_1^m-1}C_i^{(p_1^{m+1},q')}$$

とおく. このとき, $Cay(\mathbb{F}_q,D)$ が強正則であれば, $Cay(\mathbb{F}_{q'},D')$ も強正則である.

証明: $|\{\psi(\gamma^a D)\,|\,a=0,1,\ldots,q-2\}|=2$ を仮定して, $|\{\psi'(\omega^a D')\,|\,a=0,1,\ldots,q'-2\}|=2$ を示せば十分である. ここで, ψ,ψ' は $\mathbb{F}_q,\mathbb{F}_{q'}$ の標準加法的指標, γ,ω は $\mathbb{F}_q,\mathbb{F}_{q'}$ の原始根とする. ここで, 一般性を失うことなく γ と ω は (2.1) の α と β に対し, $\gamma=\alpha+P\in O_K/P$ と $\omega=\beta+P'\in O_{K'}/P'$ の形をしていると仮定できる. このとき, $\chi^u_{P'}(\omega^{p_1})=\chi^u_P(\gamma)$ が従う.

定理を証明するために,

$$p_1^{m+1}\cdot\psi'(\omega^a D')=\sum_{u=0}^{p_1^{m+1}-1}G_{f'}(\chi_{P'}^{-u})\sum_{i=0}^{p_1^{m-1}-1}\sum_{j=0}^{p_1-1}\chi^u_{P'}(\omega^{a+ip_1+j})$$

を計算すれば十分である. ここで, $a=0,1,\ldots,k'-1$ とする.

$u=0$ に対し,

$$G_{f'}(\chi^0_{P'})\sum_{i=0}^{p_1^{m-1}-1}\sum_{j=0}^{p_1-1}\chi^0_{P'}(\omega^{a+ip_1+jk/p_1^{e_1}})=-p_1^m$$

を得る.

$u=p_1^m v$ かつ $v\not\equiv 0\,(\mathrm{mod}\ p_1)$ のとき,

$$G_{f'}(\chi_{P'}^{-p_1^{e_1}v})\sum_{i=0}^{p_1^{m-1}-1}\sum_{j=0}^{p_1-1}\chi_{P'}^{p_1^{e_1}v}(\omega^{a+ip_1+jk/p_1^{e_1}})=0$$

を得る.

残りの場合, つまり, $p_1^m\nmid u$ のとき, ある $0\le v_1\le p_1-1$ と $1\le v_2\le p_1^m-1$ で $u=p_1^m v_1+v_2$ と書ける. ここで, 各 $a\in\{0,1,\ldots,k'-1\}$ に対し, ただ一つ $j\in\{0,1,\ldots,p_1-1\}$ があって, $p_1\,|\,a+j$ が成立し, その j に対し $a+j=p_1 j_a$ とおく. このとき, 任意の $0\le v_1,v_1'\le p_1-1$ に対し, $G_{f'}(\chi_{P'}^{p_1^m v_1+v_2})=G_{f'}(\chi_{P'}^{p_1^m v_1'+v_2})$ より,

$$\begin{aligned}&\sum_{v_1=0}^{p_1-1}\sum_{v_2=1}^{p_1^m-1}G_{f'}(\chi_{P'}^{-p_1^m v_1-v_2})\sum_{i=0}^{p_1^{m-1}-1}\sum_{j=0}^{p_1-1}\chi_{P'}^{p_1^m v_1+v_2}(\omega^{a+ip_1+j})\\ =\ & p_1\sum_{v_2=1}^{p_1^m-1}G_{f'}(\chi_{P'}^{-v_2})\sum_{i=0}^{p_1^{m-1}-1}\chi^{v_2}_{P'}(\omega^{p_1(j_a+i)}).\end{aligned}$$

ここで, 系 2.9 より, $G_{f'}(\chi_{P'}^{-v_2})=p^{\frac{\phi(k')-\phi(k)}{2e}}G_f(\chi_P^{-v_2})$ が成立していることに注意. また, $\chi^{v_2}_{P'}(\omega^{p_1(j_a+i)})=\chi^{v_2}_P(\gamma^{j_a+i})$ も成立しているから, 上の値は

$$p_1 p^{\frac{\phi(k')-\phi(k)}{2e}}\sum_{v_2=1}^{p_1^m-1}G_f(\chi_P^{-v_2})\sum_{i=0}^{p_1^{m-1}-1}\chi^{v_2}_P(\gamma^{j_a+i})$$

と変形できる. このようにして,

$$p_1^{m+1}\cdot\psi'(\omega^a D')+p_1^m=p_1 p^{\frac{\phi(k')-\phi(k)}{2e}}\sum_{v_2=1}^{k-1}G_f(\chi_P^{-v_2})\sum_{i=0}^{p_1^{m-1}-1}\chi^{v_2}_P(\gamma^{j_a+i})\qquad(3.1)$$

が得られるが, 我々の仮定より,

$$|\{\psi(\gamma^a D) \mid a = 0, 1, \ldots, k-1\}| = 2$$

であったから, (3.1) の値もちょうど 2 つである. □

例 3.2. 表 *1* の *No. 2, 4, 5, 6, 7, 9, 11* および表 *2* のすべての (p_1, p, e) に対し, $Cay(\mathbb{F}_{p^f}, C_0^{(p_1, p^f)})$ は強正則グラフである. 特に, 表 *2* は部分体型の例である. これらの例では, 帰納法から, 任意の m で $[(\mathbb{Z}/p_1^m\mathbb{Z})^* : \langle p \rangle] = e$ が成立しているので, 定理 *3.1* より, 任意の m に対し, $D = \bigcup_{i=0}^{p_1^{m-1}-1} C_i^{(p_1^m, p^f p_1^{m-1})}$ と定めると, $Cay(\mathbb{F}_{p^f p_1^{m-1}}, D)$ は強正則である. このようにして, 多くの新しい強正則グラフの無限系列が得られた.

表 2: 部分体型の例

p_1	p	f	$e = [(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle]$
7	2	2	2
13	3	3	4
31	2	5	6
31	5	3	10
73	2	9	8
127	2	7	18
307	17	3	102
757	3	9	84
1093	3	7	156
1723	41	3	574

この論文では, 論文 [12] の部分的な結果について, その要約とより簡潔な証明を与えた. より一般的な結果については [12] を参照されたい. また, 最近, ここで与えた結果とは別に, 円分的強正則グラフを利用して, skew Hadamard 型の差集合を構成することに成功した. 可換群上の skew Hadamard 型の差集合の存在性については, 基本可換群上でしかも平方剰余型の差集合しかないという予想があったが, 我々の構成法で, その予想の反例を与えることに成功した. 詳しくは論文 [13] を参照されたい.

参考文献

[1] L. D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, *DSN Progr. Rep.*, **16** (1973), 128–131.

[2] B. Berndt, R. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.

[3] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, course notes, available at `http://homepages.cwi.nl/~aeb/math/ipm.pdf`

[4] K. Q. Feng, J. Yang, S. X. Luo, Gauss sums of index 4: (1) cyclic case, *Acta Math. Sin. (Engl. Ser.),* **21** (2005), 1425–1434.

[5] T. Feng, Q. Xiang, Strongly regular graphs from union of cyclotomic classes, to appear in *J. Combin. Theory* (B).

[6] T. Feng, K. Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, ArXiv: 1201.0701.

[7] G. Ge, Q. Xiang, T. Yuan, Construction of strongly regular Cayley graphs using index four Gauss sums, ArXiv: 1201.0702.

[8] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory, 2nd ed.,* Graduate Texts in Mathematics 84, 1998.

[9] P. Langevin, Calcus de certaines sommes de Gauss, 1990. *J. Number Theory,* **63** (1997), 59–64.

[10] O. D. Mbodj, Quadratic Gauss sums, *Finite Fields Appl.,* **4** (1998), 347–361.

[11] P. Meijer, M. van der Vlugt, The evaluation of Gauss sums for characters of 2-power order, *J. Number Theory,* **100** (2003), 381–395.

[12] K. Momihara, Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums, ArXiv:1202.6414.

[13] K. Momihara, Skew Hadamard difference sets from cyclotomic strongly regular graphs, ArXiv:1207.2197.

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

[15] F. Wu, Constructions of strongly regular graphs using even index Gauss sums, preprint.

[16] K. Yamamoto, On congruences arising from relative Gauss sums, in: *Number Theory and Combinatorics, Japan, 1984*, World Scientific Pub., 1985, pp. 423–446.

[17] J. Yang, S. X. Luo, K. Q. Feng, Gauss sums of index 4: (1) non-cyclic case, *Acta Math. Sin. (Engl. Ser.),* **22** (2006), 833–844.

[18] 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.