A large family of strongly regular Cayley graphs from three-valued Gauss periods

Koji Momihara (Kumamoto University)

momihara@educ.kumamoto-u.ac.jp

22-Aug-2019

I will report that

there exists an infinite family of strongly regular Cayley graphs on $(\mathbb{F}_q^6, +)$ with either of the following parameters

$$(q^6, r(q^3+1), -q^3+r^2+3r, r^2+r)$$

or

$$(q^6, r(q^3-1), q^3+r^2-3r, r^2-r),$$

where $r = (q^2-1)M/2$.

The family includes geometrically important classes of SRGs.

Collaborators

J. Bamberg T. Feng M. Lee Q. Xiang

Strongly regular graphs and geometric substructures

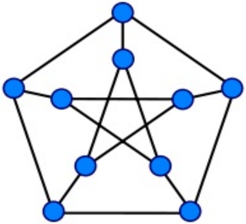
Strongly regular graph

Definition: strongly regular graph

A (v, k, λ, μ) *strongly regular graph* (SRG) is a k-regular graph (V, E) with v vertices satisfying

- for $\forall x, y \in V$ s.t. $xy \in E$, $|\{z \mid xz \in E; yz \in E\}| = \lambda$;
- for $\forall x, y \in V$ s.t. $xy \notin E$, $|\{z \mid xz \in E; yz \in E\}| = \mu$.

The Petersen graph is a $(10, 3, 0, 1)$ SRG.



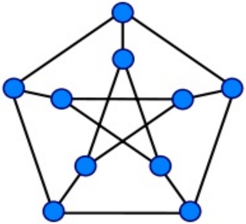
Strongly regular graph

Definition: strongly regular graph

A (v, k, λ, μ) *strongly regular graph* (SRG) is a k-regular graph (V, E) with v vertices satisfying

- for $\forall x, y \in V$ s.t. $xy \in E$, $|\{z \mid xz \in E; yz \in E\}| = \lambda$;
- for $\forall x, y \in V$ s.t. $xy \notin E$, $|\{z \mid xz \in E; yz \in E\}| = \mu$.

The Petersen graph is a $(10, 3, 0, 1)$ SRG.



A connected SRG, not complete or edgeless, is a regular graph having precisely two distinct eigenvalues different from k.

Two types of parameters

Definition

A (v, k, λ, μ)-SRG is called

- *Latin square type* $(+; u, r)$ if
$$(v, k, \lambda, \mu) = (u^2, r(u-1), u + r^2 - 3r, r^2 - r);$$
- *negative Latin square type* $(-; u, r)$ if
$$(v, k, \lambda, \mu) = (u^2, r(u+1), -u + r^2 + 3r, r^2 + r).$$

Two types of parameters

Definition

A (v, k, λ, μ)-SRG is called

- *Latin square type* $(+; u, r)$ if
$$(v, k, \lambda, \mu) = (u^2, r(u-1), u + r^2 - 3r, r^2 - r);$$
- *negative Latin square type* $(-; u, r)$ if
$$(v, k, \lambda, \mu) = (u^2, r(u+1), -u + r^2 + 3r, r^2 + r).$$

Typical examples of SRGs of $+$ type or $-$ type come from hyperbolic or elliptic quadrics of $\mathrm{PG}(2n-1, q)$, respectively.

A SRG of type $(+; u, r)$ and a SRG of type $(-; u, r)$ sometimes act like a twin.

Cayley graph

Definition: Cayley graph

- G: an (additively written) abelian group
- D: a subset of G satisfying $0_G \notin D$ and $D = -D$

A *Cayley graph* $\mathrm{Cay}(G, D)$ is a graph $\Gamma = (G, E)$ s.t. $xy \in E$ iff $x - y \in D$. The set D is called the *connection set* of Γ.

Cayley graph

Definition: Cayley graph

- G: an (additively written) abelian group
- D: a subset of G satisfying $0_G \notin D$ and $D = -D$

A *Cayley graph* $\mathrm{Cay}(G, D)$ is a graph $\Gamma = (G, E)$ s.t. $xy \in E$ iff $x - y \in D$. The set D is called the *connection set* of Γ.

We treat $\mathrm{Cay}(\mathbb{F}_q^6, D)$ s.t. D is $\mathbb{F}_q^*$-invariant.
$\Rightarrow$ $D/\mathbb{F}_q^*$ can be viewed as a set $\mathcal{D}$ of projective points in $\mathrm{PG}(5, q)$.

Finite orthogonal polar spaces

- f: a nondegenerate quadratic form on $\mathbb{F}_q^{d+1}$

An orthogonal polar space $\mathcal{S}$ w.r.t. f is the geometry consisting of totally singular subspaces, which are the subspaces of $\mathbf{PG}(d, q)$ contained in the associated quadric.

Finite orthogonal polar spaces

- f: a nondegenerate quadratic form on $\mathbb{F}_q^{d+1}$

An orthogonal polar space $\mathcal{S}$ w.r.t. f is the geometry consisting of totally singular subspaces, which are the subspaces of $\mathbf{PG}(d, q)$ contained in the associated quadric.

- *Maximals*: subspaces in $\mathcal{S}$ of maximal dimension
- *Rank*: the vector space dimension of maximals
- $P^{\perp}$: the intersection of the tangent hyperplane at P with $\mathcal{S}$

Orthogonal polar spaces in $\mathbf{PG}(5, q)$

We consider orthogonal polar spaces in $\mathbf{PG}(5, q)$:
a hyperbolic quadric $\mathbf{Q}^+(5, q)$ and an elliptic quadric $\mathbf{Q}^-(5, q)$.

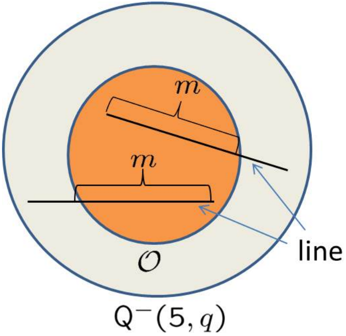
Quadric	rank	#points	quadratic form
$\mathbf{Q}^+(5, q)$	$\mathbf{3}$	$(q^2+1)(q^2+q+1)$	$x_1x_2 + x_3x_4 + x_5x_6$
$\mathbf{Q}^-(5, q)$	$\mathbf{2}$	$(q^3+1)(q+1)$	$f(x_0, x_1) + x_3x_4 + x_5x_6$

m-ovoids

$\mathcal{S}$: a finite (orthogonal) polar space of rank r in $\mathrm{PG}(d, q)$

Definition: m-ovoid

An *m-ovoid* is a set $\mathcal{O}$ of points s.t. every maximal of $\mathcal{S}$ meets $\mathcal{O}$ in exactly m points.

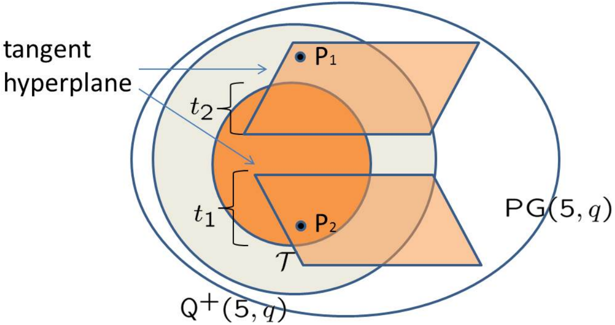


i-tight sets

Definition: i-tight set

A ***i**-tight set* is a set $\mathcal{T}$ of points s.t.

$$|P^\perp \cap \mathcal{T}| = \begin{cases} i\frac{q^{r-1}-1}{q-1} + q^{r-1} (=: t_1) & \text{if } P \in \mathcal{T} \\ i\frac{q^{r-1}-1}{q-1} (=: t_2) & \text{if } P \notin \mathcal{T}. \end{cases}$$



SRGs from m-ovoids and i-tight sets

- $\mathcal{D}$: either a m-ovoid in $\mathbf{Q}^-(5,q)$ or i-tight set in $\mathbf{Q}^+(5,q)$
- $D := \{xy : \langle x\rangle \in \mathcal{D}, y \in \mathbb{F}_q^*\} \subseteq \mathbb{F}_q^6$

J. Bamberg, S. Kelly, M. Law, T. Penttila, Tight sets and m-ovoids of finite polar spaces, **JCTA**, (2007).

SRGs from m-ovoids and i-tight sets

- $\mathcal{D}$: either a m-ovoid in $\mathbf{Q}^-(5,q)$ or i-tight set in $\mathbf{Q}^+(5,q)$
- $D := \{xy : \langle x \rangle \in \mathcal{D}, y \in \mathbb{F}_q^*\} \subseteq \mathbb{F}_q^6$

Proposition: m-ovoid, i-tight set $\Rightarrow$ $\mathrm{Cay}(\mathbb{F}_q^6, D)$ is a SRG

- a m-ovoid in $\mathbf{Q}^-(5,q)$ $\Rightarrow$ a SRG of type $(-; q^3, m(q-1))$
- a i-tight set in $\mathbf{Q}^+(5,q)$ $\Rightarrow$ a SRG of type $(+; q^3, i)$

J. Bamberg, S. Kelly, M. Law, T. Penttila, Tight sets and m-ovoids of finite polar spaces, **JCTA**, (2007).

Why are $\mathbf{Q}^+(5,q)$ and $\mathbf{Q}^-(5,q)$ so important?

Remark

- A i-tight set in $\mathbf{Q}^+(5,q)$ is mapped by the Klein correspondence to a set $\mathcal{L}$ of lines, called a *Cameron-Liebler line class*, in $\mathbf{PG}(3,q)$ s.t. every spread shares exactly i lines with $\mathcal{L}$.

Why are $\mathsf{Q}^+(5,q)$ and $\mathsf{Q}^-(5,q)$ so important?

Remark

- A i-tight set in $\mathsf{Q}^+(5,q)$ is mapped by the Klein correspondence to a set $\mathcal{L}$ of lines, called a *Cameron-Liebler line class*, in $\mathrm{PG}(3,q)$ s.t. every spread shares exactly i lines with $\mathcal{L}$.
- A $\frac{q+1}{2}$-ovoid in $\mathsf{Q}^-(5,q)$ is mapped by the duality of generalized quadrangles to a set $\mathcal{L}$ of lines, called a *hemisystem*, in $\mathsf{H}(3,q^2)$ containing exactly half of the lines on every point.

If a m-ovoid in $\mathsf{Q}^-(5,q)$ exists, then $m=(q+1)/2$.

Strongly regular graphs of type $(\pm; q^3, \frac{q^2-1}{2})$

New m-ovoids and i-tight sets

Theorem by FMX & DDMR

Let $q \equiv 5, 9 \pmod{12}$. There exists a SRG on $(\mathbb{F}_q^6, +)$ of type $(+; q^3, \frac{q^2-1}{2})$, which gives rise to a $\frac{q^2-1}{2}$-tight set in $\mathbf{Q}^+(5, q)$.

T. Feng, K. Momihara. Q. Xiang, Cameron-Liebler line classes with parameters $x = \frac{q^2-1}{2}$, **JCTA**, (2015).

J. De Beule, J. Demeyer, K. Metsch, M. Rodgers, A new family of tight sets in $Q^+(5, q)$, **DCC**, (2016).

J. Bamberg, M. Lee, K. Momihara, Q. Xiang, New hemisystems of the Hermitian surfaces, **Comb**, (2018).

New m-ovoids and i-tight sets

Theorem by FMX & DDMR

Let $q \equiv 5, 9 \pmod{12}$. There exists a SRG on $(\mathbb{F}_q^6, +)$ of type $(+; q^3, \frac{q^2-1}{2})$, which gives rise to a $\frac{q^2-1}{2}$-tight set in **Q**$^+(5, q)$.

Theorem by BLMX

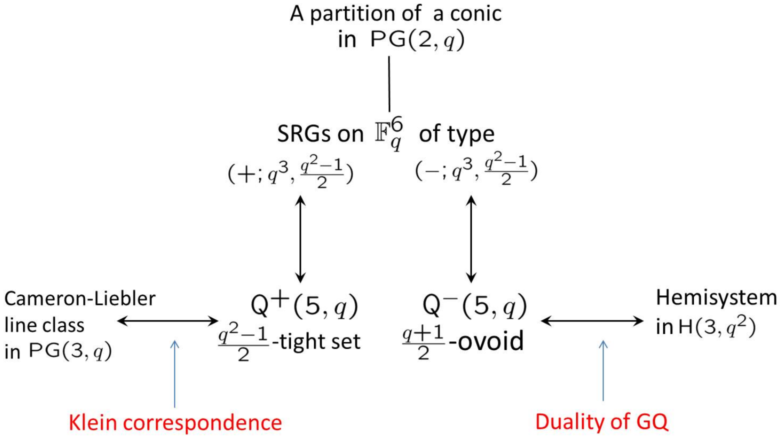
Let $q \equiv 3 \pmod{4}$. There exists a SRG on $(\mathbb{F}_q^6, +)$ of type $(-; q^3, \frac{q^2-1}{2})$, which gives rise to a $\frac{q+1}{2}$-ovoid in **Q**$^-(5, q)$.

T. Feng, K. Momihara. Q. Xiang, Cameron-Liebler line classes with parameters $x = \frac{q^2-1}{2}$, **JCTA**, (2015).

J. De Beule, J. Demeyer, K. Metsch, M. Rodgers, A new family of tight sets in $Q^+(5, q)$, **DCC**, (2016).

J. Bamberg, M. Lee, K. Momihara, Q. Xiang, New hemisystems of the Hermitian surfaces, **Comb**, (2018).

A partition of a conic in $\mathbf{PG(2,}\ q\mathbf{)}$ is behind both constructions.



Conics

- $\mathbf{PG(2,}\boldsymbol{q}\mathbf{)}$: We identify the point set with $\mathbb{F}_{q^3}^*/\mathbb{F}_q^*$ or $\mathbb{Z}_{q^2+q+1}$.
- $f(x) := \mathrm{Tr}_{q^3/q}(x^2)$ defines a nondegenerate quadratic form from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$.

Conics

- $\mathbf{PG(2,}\boldsymbol{q}\mathbf{)}$: We identify the point set with $\mathbb{F}_{q^3}^*/\mathbb{F}_q^*$ or $\mathbb{Z}_{q^2+q+1}$.
- $f(x) := \mathrm{Tr}_{q^3/q}(x^2)$ defines a nondegenerate quadratic form from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$.
- The set $C = \{\langle x \rangle \mid f(x) = 0\} \subseteq \mathbb{F}_{q^3}^*/\mathbb{F}_q^*$ defines a **conic** in $\mathbf{PG(2,}\boldsymbol{q}\mathbf{)}$, i.e., each line meets C in $\mathbf{0}$, $\mathbf{1}$ or $\mathbf{2}$ points.
- T_i, $i = 1, 2$: a “good” partition of

$$I_C = \{i \pmod{q^2+q+1} \mid \mathrm{Tr}_{q^3/q}(\omega^{2i}) = 0\}$$

$\frac{q+1}{2}$-ovoid in $Q^-(5, q)$

Construction by Bamberg-Lee-M.-Xiang (2018)

Let $q \equiv 3 \pmod{4}$ and

$$X = \{Ni + 4j \pmod{4(q^2+q+1)} : \\ (i,j) \in (\{0,3\} \times 2^{-1}T_1) \cup (\{1,2\} \times 2^{-1}T_2)\}.$$

Define

$$D = \bigcup_{i \in X} \gamma^i \langle \gamma^{4(q^2+q+1)} \rangle \subseteq \mathbb{F}_{q^6}.$$

Then, $\mathrm{Cay}(\mathbb{F}_{q^6}, D)$ is a SRG of type $(-; q^3, \frac{q^2-1}{2})$.

Model of an elliptic QF: $f(x) = \mathrm{Tr}_{q^3/q}(x^{q^3+1})$

A partition of the conic C

Definition

For $d_0 \in I_C = \{d_i : i = 0, 1, \ldots, q\}$, we define

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

and

$$J_C := \{i \pmod{2(q^2+q+1)} : \omega^i \in \mathcal{X}\}.$$

A partition of the conic C

Definition

For $d_0 \in I_C = \{d_i : i = 0, 1, \dots, q\}$, we define

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

and

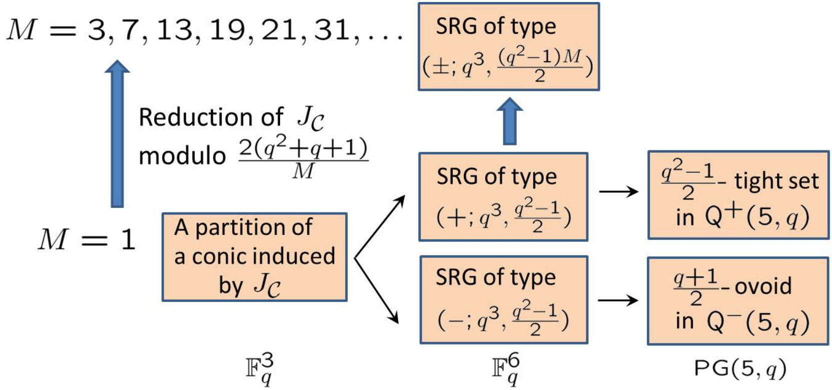
$$J_C := \{i \pmod{2(q^2+q+1)} : \omega^i \in \mathcal{X}\}.$$

We have $J_C \equiv I_C \pmod{q^2+q+1}$. The set $\mathcal{X}$ yields a four-class fission scheme of a three-class translation scheme on $(\mathbb{F}_{q^3}, +)$ related to the conic.

The partition of J_C into the even and odd parts induces the required partition T_1 and T_2 of I_C.

A new large family of SRGs from quotients of known SRGs

$\Phi_{M,\pm} := \{q \mid \exists$a SRG of type $(\pm; q^3, \frac{(q^2-1)M}{2})\} \Leftarrow$ infinite set??



K. Momihara, Construction of strongly regular Cayley graphs based on three-valued Gauss periods, **EJC**, (2018).

Main result

$\Phi_{M,\pm} := \{q \mid \exists$a SRG of type $(\pm; q^3, \frac{(q^2-1)M}{2})\}$

Main result

$$\Phi_{M,\pm} := \{q \mid \exists \text{a SRG of type } (\pm; q^3, \tfrac{(q^2-1)M}{2})\}$$

Main Thm 1 by M.& Xiang (2019)

Assume that there is $1 \le h \le M - 1$ s.t. $M \mid h^2 + h + 1$.

1. $\Phi_{M,+} \cup \Phi_{M,-}$ is an infinite set.
2. If $-1 \notin \langle 2 \rangle \pmod{M'}$ for $\forall M' \mid M$, both $\Phi_{M,+}$ and $\Phi_{M,-}$ are infinite sets.

Main result

$$\Phi_{M,\pm} := \{q \mid \exists \text{a SRG of type } (\pm; q^3, \tfrac{(q^2-1)M}{2})\}$$

Main Thm 1 by M.& Xiang (2019)

Assume that there is $1 \le h \le M-1$ s.t. $M \mid h^2+h+1$.

1. $\Phi_{M,+} \cup \Phi_{M,-}$ is an infinite set.
2. If $-1 \notin \langle 2\rangle \pmod{M'}$ for $\forall M' \mid M$, both $\Phi_{M,+}$ and $\Phi_{M,-}$ are infinite sets.

Main Thm 2 by M.& Xiang (2019)

Assume that

- M is an odd prime power,
- the class number of $\mathbb{Q}(\zeta_M + \zeta_M^{-1})$ is odd.

Then, if $-1 \in \langle 2\rangle \pmod{M}$, $\Phi_{M,+}$ is an infinite set. Furthermore, if $\mathrm{ord}_M(2) \equiv 2 \pmod{4}$, $\Phi_{M,-}$ is an infinite set.

Definition: Gauss period

- ω: a fixed primitive element of $\mathbb{F}_q$
- $\psi_{\mathbb{F}_q}$: a fixed nonprincipal additive character of $\mathbb{F}_q$
- N: a positive integer dividing $q-1$.

Definition: Gauss period

The *Nth Gauss periods* of $\mathbb{F}_q$ are the character values of $\omega^i\langle\omega^N\rangle$, $i = 0, 1, \ldots, N-1$:

$$\sum_{x\in\omega^i\langle\omega^N\rangle} \psi_{\mathbb{F}_q}(x), \quad 0 \le i \le N-1.$$

Problem

Problem

Let $N \mid q^2 + q + 1$. When do the Nth Gauss periods in $\mathbb{F}_{q^3}$ take exactly three values in an arithmetic progression?

T. Maruta, Cyclic and pseudo-cyclic MDS codes of dimension three, **ASMFUM**, (1995).

Problem

Let $N \mid q^2 + q + 1$. When do the Nth Gauss periods in $\mathbb{F}_{q^3}$ take exactly three values in an arithmetic progression?

Equivalent Problem

Take the reduction (as a multiset) of the conic
$I_C = \{i \pmod{q^2 + q + 1} \mid \mathrm{Tr}_{q^3/q}(\omega^{2i}) = 0\}$ modulo N, i.e.,

$$S_N := \{i \pmod{N} \mid i \in I_C\}.$$

Let c_x be the multiplicity of each $x \in \{0, 1, \ldots, N-1\}$ in S_N.
For which N and q does $c_x \in \{0, 1, 2\}$ for every x?

T. Maruta, Cyclic and pseudo-cyclic MDS codes of dimension three, **ASMFUM**, (1995).

Three-valued Gauss periods

Theorem by Maruta (1995)

- $M \in \mathbb{N}$: $1 \le \exists h \le M-1$ s.t. $M \mid h^2+h+1$
- q: a power of a prime p s.t. $q \equiv h \pmod{M}$
- $N = (q^2+q+1)/M$

If p is large enough, the Nth Gauss periods in $\mathbb{F}_{q^3}$ take exactly three values $-M+2q, -M+q, -M$.

T. D. Duc, K. H. Leung, B. Schmidt, Upper bounds for cyclotomic numbers, **arXiv: 1903.07314**, (2019).

Three-valued Gauss periods

Theorem by Maruta (1995)

- $M \in \mathbb{N}$: $1 \leq \exists h \leq M-1$ s.t. $M \mid h^2+h+1$
- q: a power of a prime p s.t. $q \equiv h \pmod{M}$
- $N = (q^2+q+1)/M$

If p is large enough, the Nth Gauss periods in $\mathbb{F}_{q^3}$ take exactly three values $-M+2q, -M+q, -M$.

Theorem by M.& Xiang (2019)

The claim above holds for any prime p satisfying

$$p > \left(\frac{12M}{\phi(M)}\right)^{\phi(M)/2\mathrm{ord}_M(p)}.$$

T. D. Duc, K. H. Leung, B. Schmidt, Upper bounds for cyclotomic numbers, **arXiv: 1903.07314**, (2019).

Example: $p = 7$ and $M = 3$

In this case, $N = (p^2 + p + 1)/M = 19$ and
the Gauss periods take $\alpha_1 = 11, \alpha_2 = 4, \alpha_3 = -3$.
Define $I_j := \{i \pmod N) : \psi_{\mathbb{F}_{q^3}}(\omega^i \langle \omega^N \rangle) = \alpha_j\}, \quad j = 1, 2, 3$.
Then,

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

Example: $p = 7$ and $M = 3$

In this case, $N = (p^2 + p + 1)/M = 19$ and
the Gauss periods take $\alpha_1 = 11, \alpha_2 = 4, \alpha_3 = -3$.
Define $I_j := \{i \pmod N) : \psi_{\mathbb{F}_{q^3}}(\omega^i \langle \omega^N \rangle) = \alpha_j\}, \quad j = 1, 2, 3$.
Then,

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

On the other hand,

$$I_C = \{4, 19, 24, 25, 28, 36, 38, 54\} \subseteq \mathbb{Z}_{p^2+p+1}$$

and

$$S_N = \{0, 0, 4, 5, 6, 9, 16, 17\} = 2^{-1}(I_1 \cup I_1 \cup I_2).$$

Construction based on three-valued Gauss periods

Assume that the Nth Gauss periods in $\mathbb{F}_{q^3}$ take three values $\alpha_1 = -M + 2q, \alpha_2 = -M + q, \alpha_3 = -M$.

- $I_j = \{i \pmod{N} : \psi_{\mathbb{F}_{q^3}}(\omega^i \langle \omega^N \rangle) = \alpha_j\}, j = 1, 2, 3$
- T_i, $i = 1, 2$: a *good* partition of I_2.
- $S_i := 4^{-1} T_i \pmod{N}$, $i = 1, 2$

Construction based on three-valued Gauss periods

Assume that the Nth Gauss periods in $\mathbb{F}_{q^3}$ take three values $\alpha_1 = -M + 2q, \alpha_2 = -M + q, \alpha_3 = -M$.

- $I_j = \{i \pmod{N} : \psi_{\mathbb{F}_{q^3}}(\omega^i\langle\omega^N\rangle) = \alpha_j\}, j = 1, 2, 3$
- T_i, $i = 1, 2$: a *good* partition of I_2.
- $S_i := 4^{-1}T_i \pmod{N}$, $i = 1, 2$

Construction by M. (2018)

Let $q \equiv 3 \pmod{4}$. Define

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

and

$$D = \bigcup_{i\in Y} \gamma^i\langle\gamma^{4N}\rangle \subseteq \mathbb{F}_{q^6}.$$

Then, $\mathrm{Cay}(\mathbb{F}_{q^6}, D)$ is a SRG of type $(-; q^3, \frac{(q-1)M}{2})$.

How to find a "good" partition of I_2

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
\begin{array}{c} I_{\mathcal{C}} \pmod{q^2+q+1} \\ \text{a conic} \end{array} \arrow[d, "\text{Reduction modulo N}"'] & J_{\mathcal{C}} \pmod{2(q^2+q+1)} \arrow[l, "\text{Partition}"'] \arrow[dl] \arrow[d, "\text{Reduction modulo 2N}"] \\
S_N \pmod{N} & \overline{S_N} \pmod{2N} \arrow[l, "\text{Reduction modulo N}"']
\end{tikzcd}
$$

The multiplicities are 0, 1, or 2.

This quotient induces a partition of I_2

How about the multiplicities?

$$S_N \equiv 2^{-1}(I_1 \cup I_1 \cup I_2) \pmod{N}$$

Proposition

If the multiplicity of each element in $\overline{S_N}$ is either $\mathbf{0}$ or $\mathbf{1}$, we have a suitable partition of I_2.

Equivalent condition

- $M = (q^2 + q + 1)/N$
- η: the quadratic character of $\mathbb{F}_{q^3}$
- ϵ_M: a primitive Mth root of unity in $\mathbb{F}_{q^3}$

Proposition

The multiplicity of each $x \in \{0, 1, \ldots, 2N - 1\}$ in the multiset $\overline{S_N}$ is either 0 or 1 iff $\eta(2) \neq \eta(1 + \epsilon_M^\ell)$ for $\forall \ell \in \{1, 2, \ldots, M - 1\}$.

Equivalent condition

- $M = (q^2 + q + 1)/N$
- η: the quadratic character of $\mathbb{F}_{q^3}$
- ϵ_M: a primitive Mth root of unity in $\mathbb{F}_{q^3}$

Proposition

The multiplicity of each $x \in \{0, 1, \ldots, 2N-1\}$ in the multiset $\overline{S_N}$ is either $\mathbf{0}$ or $\mathbf{1}$ iff $\eta(2) \neq \eta(1 + \epsilon_M^\ell)$ for $\forall \ell \in \{1, 2, \ldots, M-1\}$.

We can use Chebotarëv's density theorem to prove the following.

Theorem by M.& Xiang (2019)

For each odd integer M s.t. $1 \leq \exists h \leq M - 1$ with $M \mid h^2 + h + 1$, there are infinitely many primes p s.t. $\eta(2) \neq \eta(1 + \epsilon_M^\ell)$ for $\forall \ell \in \{1, 2, \ldots, M-1\}$ in $\mathbb{F}_{p^3}$.

$\Rightarrow \Phi_{M,+} \cup \Phi_{M,-}$ is an infinite set.

($\Phi_{M,\pm} := \{q \mid \exists$a SRG of type $(\pm; q^3, \frac{(q^2-1)M}{2})\}$)

Determination of a Galois group

In order to study whether each $\Phi_{M,+}$ and $\Phi_{M,-}$ is an infinite set, we need to determine

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_4, \sqrt{2}, \sqrt{1+\zeta_M}, \ldots, \sqrt{1+\zeta_M^{M-1}})/\mathbb{Q}).$$

Determination of a Galois group

In order to study whether each $\Phi_{M,+}$ and $\Phi_{M,-}$ is an infinite set, we need to determine

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_4, \sqrt{2}, \sqrt{1+\zeta_M}, \ldots, \sqrt{1+\zeta_M^{M-1}})/\mathbb{Q}).$$

Theorem by M.& Xiang (2019)

Let M be an odd prime power s.t. the class number of $\mathbb{Q}(\zeta_M + \zeta_M^{-1})$ is odd. If $\mathrm{ord}_M(2) \equiv 1 \pmod 2$ or $\mathrm{ord}_M(2) \equiv 2 \pmod 4$, both $\Phi_{M,+}$ and $\Phi_{M,-}$ are infinite sets.

Determination of a Galois group

In order to study whether each $\mathbf{\Phi}_{M,+}$ and $\mathbf{\Phi}_{M,-}$ is an infinite set, we need to determine

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_4, \sqrt{2}, \sqrt{1+\zeta_M}, \ldots, \sqrt{1+\zeta_M^{M-1}})/\mathbb{Q}).$$

Theorem by M.& Xiang (2019)

Let M be an odd prime power s.t. the class number of $\mathbb{Q}(\zeta_M + \zeta_M^{-1})$ is odd. If $\mathrm{ord}_M(2) \equiv 1 \pmod 2$ or $\mathrm{ord}_M(2) \equiv 2 \pmod 4$, both $\mathbf{\Phi}_{M,+}$ and $\mathbf{\Phi}_{M,-}$ are infinite sets.

Problem

Determine G in the case where M is not a prime power.

Problem

- J. Bamberg, S. Kelly, M. Law, T. Penttila, Tight sets and m-ovoids of finite polar spaces, **JCTA**, (2007).
- A. Cossidente, F. Pavese, Intriguing sets of quadrics in $\mathbf{PG(5,}\ \boldsymbol{q}\mathbf{)}$, **AG**, (2017).
- A. Cossidente, F. Pavese, On intriguing sets of finite symplectic spaces, **DCC**, (2018).
- G. Korchmáros, G. P. Nagy, P. Speziali, Hemisystems of the Hermitian surface, `arXiv:1710.06335`.
- M. Rodgers, On some new examples of Cameron-Liebler line classes, Ph.D Thesis (2012).

Problem

Can you obtain SRG with new parameters from known SRGs by using our “quotient” method?

Details

Consider a two-character set $\mathcal{D}$ in $\mathbf{PG}(d, q)$.
$\mathcal{D}$ can be viewed as a subset $I_{\mathcal{D}}$ of $\mathbb{Z}_{\frac{q^{d+1}-1}{q-1}}$.

Let $N \mid \frac{q^{d+1}-1}{q-1}$. Define

$$S_N = \{x \pmod{N} \mid x \in I_{\mathcal{D}}\}.$$

Assume that the multiplicity of each element $x \in \{0, 1, \ldots, N-1\}$ in S_N is a_1 or a_2.

Define

$$I_1 = \{x \pmod{N} \mid \text{the multiplicity of } x \text{ in } S_N \text{ is } a_1\}.$$

Problem

Let $E = \bigcup_{x \in I_1} \gamma^x \langle \gamma^N \rangle \subseteq \mathbb{F}_{q^{d+1}}$. Does $\mathbf{Cay}(\mathbb{F}_{q^{d+1}}, E)$ form a SRG?

Thank you very much for your attention!