Cyclotomic constructions of strongly regular Cayley graphs and difference sets

Qing Xiang

University of Delaware
Newark, DE 19716, USA
xiang@math.udel.edu

Joint work with Tao Feng, University of Delaware

Strongly Regular Graphs

A *strongly regular graph srg* (v, k, λ, μ) is a graph with v vertices that is regular of valency k and that has the following properties:

- For any two adjacent vertices x, y, there are exactly λ vertices adjacent to both x and y.
- For any two nonadjacent vertices x, y, there are exactly μ vertices adjacent to both x and y.

Classical examples of strongly regular graphs include the Paley graphs. Let $q = 4t + 1$ be a prime power. The *Paley graph* $\mathrm{P}(q)$ is the graph with the finite field $\mathbb{F}_q$ as vertex set, where two vertices are adjacent when they differ by a (nonzero) square. It is strongly regular with parameters $(4t + 1, 2t, t - 1, t)$.

Theorem. For a simple graph Γ of order v, not complete or edgeless, with adjacency matrix A, the following are equivalent:

- Γ is strongly regular with parameters (v, k, λ, μ) for certain integers k, λ, μ,
- $A^2 = kI + \lambda A + \mu(J - I - A)$ for certain real numbers k, λ, μ,
- A has precisely two distinct restricted eigenvalues.

Strongly regular graphs are closely related to two-weight codes, two-intersection sets in finite geometry, and partial difference sets. See the survey papers by Calderbank and Kantor (1986) and S. L. Ma (1994).

Cyclotomy

Let $q = p^f$ be a prime power, and let γ be a fixed primitive element of $\mathbb{F}_q$. Let $N > 1$ be a divisor of $q - 1$. We define the Nth *cyclotomic classes* $C_0, C_1, \ldots, C_{N-1}$ by

$$C_i = \{\gamma^{jN+i} \mid 0 \leq j \leq \frac{q-1}{N} - 1\},$$

where $0 \leq i \leq N - 1$.

Let ψ be the additive character of $\mathbb{F}_q$ defined by $\psi(x) = \xi_p^{\mathrm{Trace}_{q/p}(x)}$. The Nth *cyclotomic periods* (aka Gauss periods) are defined by

$$\eta_i = \sum_{x \in C_i} \psi(x),$$

where $0 \leq i \leq N - 1$.

Cyclotomic Strongly Regular Graphs

Let $D \subset \mathbb{F}_{p^f}$ be such that $-D = D$ and $0 \notin D$.

$\Gamma := \mathrm{Cay}(\mathbb{F}_{p^f}, D)$

The vertex set of Γ is $\mathbb{F}_{p^f}$, and two vertices are joined by an edge if their difference belongs to D. The subset D is usually called the "connection" set of Γ.

When $D = C_0$ is a subgroup of the multiplicative group $\mathbb{F}^*_{p^f}$ of $\mathbb{F}_{p^f}$, and if $\Gamma = \mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ is strongly regular, then we speak of a *cyclotomic strongly regular graph*.

Let $D \subset \mathbb{F}_{p^f}$ be such that $-D = D$ and $0 \notin D$. The restricted eigenvalues of $\mathrm{Cay}(\mathbb{F}_{p^f}, D)$ are exactly

$$\psi_a(D) := \sum_{d \in D} \psi_a(d),$$

where ψ_a run through all nontrivial additive characters of $\mathbb{F}_{p^f}$.

There is a nonabelian (but central) version of this result, usually attributed to Babai (1979), Diaconis and Shahshanhani (1981).

Theorem. Let G be a finite group and $D \subset G$ be such that $\{d^{-1} \mid d \in D\} = D$ and $1 \notin D$. Assume that D is stable under conjugation (that is, D is a union of conjugacy classes of G). Then the restricted eigenvalues of $\mathrm{Cay}(G, D)$ are given by

$$\lambda_\chi = \frac{1}{\chi(1)} \sum_{d \in D} \chi(d),$$

where χ range over all nontrivial irreducible characters of G. Moroever, the multiplicity of λ_χ is $\chi(1)^2$.

Problem. Assume that $-C_0 = C_0$. Determine for which p, f, N the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, C_0)$ is strongly regular. Equivalently, determine for which p, f, N the Nth cyclotomic periods η_i, $0 \leq i \leq N-1$, take only TWO distinct values.

An old theorem, due to Stickelberger (around 1890), gives us a sufficient condition that ensures $|\{\eta_a : 0 \leq a \leq N-1\}| = 2$.

Theorem. (uniform cyclotomy or pure Gauss sums)
Let p be a prime, $N \geq 2$, $q = p^{2ts}$, where $s \geq 1$, $N|(p^t+1)$ and t is the smallest such positive integer. Then the cyclotomic periods are given by
Case A. If s, p, $\frac{p^t+1}{N}$ are all odd, then

$$\eta_{N/2} = \sqrt{q} - \frac{\sqrt{q}+1}{N},\ \eta_i = -\frac{1+\sqrt{q}}{N},\ \textit{for all } i \neq \frac{N}{2}.$$

Case B. In all the other cases,

$$\eta_0 = -(-1)^s\sqrt{q} + \frac{(-1)^s\sqrt{q}-1}{N},\ \eta_i = \frac{(-1)^s\sqrt{q}-1}{N},\ \textit{for all } i \neq 0.$$

Conjecture. (Schmidt and White, 2002) Let $\mathbb{F}_{p^f}$ be the finite field of size p^f, $N|(p^f-1)$, and let C_0 be the subgroup of $\mathbb{F}_{p^f}$ of index N. Assume that $-C_0 = C_0$. If $\mathrm{Cay}(\mathbb{F}_{p^f}, C_0)$ is an SRG, then one of the following holds:

- (subfield case) $C_0 = \mathbb{F}_{p^e}^*$, where $e|f$,
- (semi-primitive case or self-conjugate case) There exists a positive integer t such that $p^t \equiv -1 \pmod{N}$,
- (exceptional case) Eleven "sporadic" examples.

A Example of De Lange

In some situations, while a **single** cyclotomic coset does not give rise to a strongly regular Cayley graph, a union of **several** cyclotomic cosets can give rise to an SRG.

Example 1 (De Lange, 1995) Let $p = 2$, $f = 12$, $N = 45$. Then

$$C_0 \cup C_5 \cup C_{10}$$

gives rise to an SRG, while C_0 does not. (See Munemasa's talk also.)

"Example c is interesting: it can be viewed as a graph with vertex set $\mathbb{F}_q^3$ for $q = 16$ such that each vertex has a unique neighbour in each of the $q^2 + q + 1 = 273$ directions. Probably some generalization is possible."

Examples of Ikuta and Munemasa

Example 2 (Ikuta and Munemasa, 2008) Let $p = 2$, $f = 20$, $N = 75$. Then

$$C_0 \cup C_3 \cup C_6 \cup C_9 \cup C_{12}$$

gives rise to an SRG, while C_0 does not.

Example 3 (Ikuta and Munemasa, 2008) Let $p = 2$, $f = 21$, $N = 49$. Then

$$C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6$$

gives rise to an SRG, while C_0 does not.

New infinite families of SRG

We will generalize each of the above three examples into an infinite family. Moreover we obtain nine more infinite families of new SRG by using union of cyclotomic classes.

- $p = 2$, $N = 3^m \cdot 5$, $f = \phi(N)/2 = 3^{m-1} \cdot 4$.
- $p = 2$, $N = 5^m \cdot 3$, $f = \phi(N)/2 = 5^{m-1} \cdot 4$.
- $p = 2$, $N = 7^m$, $f = \phi(N)/2 = 7^{m-1} \cdot 3$.

New infinite families of SRG, continued

- $p = 3,\ p_1 = 107,\ N = p_1^m,\ f = \phi(N)/2 = 53 \cdot 107^{m-1}$.
- $p = 5,\ p_1 = 19,\ N = p_1^m,\ f = \phi(N)/2 = 9 \cdot 19^{m-1}$.
- $p = 5,\ p_1 = 499,\ N = p_1^m,\ f = \phi(N)/2 = 249 \cdot 499^{m-1}$.
- $p = 17,\ p_1 = 67,\ N = p_1^m,\ f = \phi(N)/2 = 33 \cdot 67^{m-1}$.
- $p = 41,\ p_1 = 163,\ N = p_1^m,\ f = \phi(N)/2 = 81 \cdot 163^{m-1}$.
- $p = 3,\ p_1 = 5,\ p_2 = 7,\ N = 5^m \cdot 7,\ f = \phi(N)/2 = 12 \cdot 5^{m-1}$.
- $p = 3,\ p_1 = 7,\ p_2 = 5,\ N = 7^m \cdot 5,\ f = \phi(N)/2 = 12 \cdot 7^{m-1}$.
- $p = 3,\ p_1 = 17,\ p_2 = 19,\ N = 17^m \cdot 19,$
  $f = \phi(N)/2 = 144 \cdot 17^{m-1}$.
- $p = 3,\ p_1 = 19,\ p_2 = 17,\ N = 19^m \cdot 17,$
  $f = \phi(N)/2 = 144 \cdot 19^{m-1}$.

Gauss sums

Let p be a prime, f a positive integer, and $q = p^f$. Let ξ_p be a fixed complex primitive pth root of unity and let $\mathrm{Trace}_{q/p}$ be the trace from $\mathbb{F}_q$ to $\mathbb{Z}/p\mathbb{Z}$. Define

$$\psi : \mathbb{F}_q \to \mathbb{C}^*, \quad \psi(x) = \xi_p^{\mathrm{Trace}_{q/p}(x)},$$

which is a nontrivial character of the additive group of $\mathbb{F}_q$. Let

$$\chi : \mathbb{F}_q^* \to \mathbb{C}^*$$

be a character of $\mathbb{F}_q^*$. We define the *Gauss sum* by

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

Gauss sums can be viewed as the Fourier coefficients in the Fourier expansion of $\psi|_{\mathbb{F}_q^*}$ in terms of the multiplicative characters of $\mathbb{F}_q$. That is, for every $c \in \mathbb{F}_q^*$,

$$\psi(c) = \frac{1}{q-1} \sum_{\chi \in \hat{\mathbb{F}}_q^*} g(\bar{\chi})\chi(c),$$

where $\bar{\chi} = \chi^{-1}$ and $\hat{\mathbb{F}}_q^*$ denotes the character group of $\mathbb{F}_q^*$.

Relationship between Gauss sums and cyclotomic periods

$$
\begin{aligned}
\eta_a &= \sum_{c \in C_a} \psi(c) = \frac{1}{N} \sum_{x \in \mathbb{F}_q^*} \psi(\gamma^a x^N) \\
&= \frac{1}{N} \sum_{x \in \mathbb{F}_q^*} \frac{1}{q-1} \sum_{\chi \in \hat{\mathbb{F}}_q^*} g(\bar{\chi}) \chi(\gamma^a x^N) \\
&= \frac{1}{(q-1)N} \sum_{\chi \in \hat{\mathbb{F}}_q^*} g(\bar{\chi}) \chi(\gamma^a) \sum_{x \in \mathbb{F}_q^*} \chi(x^N) \\
&= \frac{1}{N} \sum_{\chi \in C_0^\perp} g(\bar{\chi}) \chi(\gamma^a)
\end{aligned}
$$

where $C_0^\perp$ is the subgroup of $\hat{\mathbb{F}}_q^*$ consisting of all χ which are trivial on C_0 (i.e., the unique subgroup of order N). This shows that cyclotomic periods are linear combinations of Gauss sums, with coefficients being (complex) Nth roots of unity.

Pure Gauss sums

Theorem (Stickelberger, 1890)
Let p be a prime, and $m > 2$ be an integer. Suppose that there is a positive integer t such that $p^t \equiv -1 \pmod{m}$, with t chosen minimal. Let χ be a character of order m of $\mathbb{F}_{p^f}^*$ for some positive integer f. Then $f = 2ts$ for some positive integer s, and

$$p^{-f/2} g(\chi) = \begin{cases} (-1)^{s-1}, & \text{if } p = 2, \\ (-1)^{s-1+\frac{(p^t+1)s}{m}}, & \text{if } p > 2. \end{cases}$$

Index 2 Gauss sums

The index 2 case ($[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = 2$) was studied by Baumert, McEliece, Mykkeltveit (1970's), Van der Vlugt (1995), Langevin (1997), Mbodj (1998), Meijer and Van der Vlugt (2003), and more recently by Yang and Xia (2010). We give a sample theorem below.

Theorem (Langevin, 1997)
Let $N = p_1^m$, where p_1 is a prime such that $p_1 > 3$ and $p_1 \equiv 3 \pmod 4$. Let p be a prime such that $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = 2$ (that is, $f := \mathrm{ord}_N(p) = \phi(N)/2$) and let $q = p^f$. Let χ be a multiplicative character of order N of $\mathbb{F}_q$, and h be the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then the Gauss sum $g(\chi)$ over $\mathbb{F}_q$ is determined up to complex conjugation by

$$g(\chi) = \frac{b + c\sqrt{-p_1}}{2} p^{h_0},$$

where

1. $h_0 = \frac{f-h}{2}$,
2. $b, c \not\equiv 0 \pmod p$,
3. $b^2 + p_1 c^2 = 4p^h$,
4. $bp^{h_0} \equiv -2 \pmod{p_1}$.

Constructions of SRG by using union of cyclotomic classes

Construction 1. $N = p_1^m$

Assume that $N = p_1^m$ (here $m \geq 1$, $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod 4$), p is a prime such that $\gcd(N, p) = 1$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, and as before let $C_0, C_1, \ldots, C_{N-1}$ be the N-th cyclotomic classes of $\mathbb{F}_q$.

Note that $-C_i = C_i$ for all $0 \leq i \leq N-1$ since either $2N|(q-1)$ or q is even. Define

$$D = \cup_{i=0}^{p_1^{m-1}-1} C_i$$

Using D as connection set, we construct the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$.

Theorem. The Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is a regular graph of valency $|D|$, and it has at most three distinct restricted eigenvalues.

Sketch of Proof. Let χ be a multiplicative character of $\mathbb{F}_q$ of order N. By the above theorem of Langevin, we have

$$g(\bar{\chi}) = \frac{b + c\sqrt{-p_1}}{2} p^{h_0}, \quad b, c \not\equiv 0 \pmod{p},$$

where $h_0 = \frac{f-h}{2}$ and h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, $b^2 + p_1 c^2 = 4p^h$, and $bp^{h_0} \equiv -2 \pmod{p_1}$.

The restricted eigenvalues of $\mathrm{Cay}(\mathbb{F}_q, D)$ can be computed:

$$\psi(\gamma^a D) = \begin{cases} \frac{p^{h_0} b}{2} - \frac{p^{h_0} b}{2p_1} - \frac{1}{p_1}, \\ \pm\frac{p^{h_0} c}{2} - \frac{p^{h_0} b}{2p_1} - \frac{1}{p_1}, \end{cases}$$

where $0 \leq a \leq N-1$. So $\mathrm{Cay}(\mathbb{F}_q, D)$ has at most three distinct restricted eigenvalues.

Corollary. Using the above notation, $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph if and only if $b, c \in \{1, -1\}$.

Therefore the problem of finding SRG using the above corollary becomes finding primes p, p_1 and integer $m \geq 1$ such that $N := p_1^m$, $\mathrm{ord}_N(p) = \phi(N)/2$, and

$$4p^h = 1 + p_1,$$

where h is the class number of $Q(\sqrt{-p_1})$.

As an example, choose $p = 2$, $p_1 = 7$, $N = p_1^m$. One can check easily that $\mathrm{ord}_{7^2}(2) = 21 = \phi(7^2)/2$. By induction we have that $\mathrm{ord}_N(2) = \phi(7^m)/2$ for all $m \geq 2$. The class number h of $\mathbb{Q}(\sqrt{-7})$ is equal to 1. Therefore we indeed have $\frac{1+p_1}{4} = p^h$ in this case. We obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 2^{3 \cdot 7^{m-1}}$, $k = \frac{v-1}{7}$, and with restricted eigenvalues $r = \frac{2^{h_0+2}-1}{7}$, $s = \frac{-3 \cdot 2^{h_0}-1}{7}$.

As another example, choose $p = 3$, $p_1 = 107$, $N = p_1^m$. One can check that $\mathrm{ord}_{107^2}(3) = 5671 = \phi(107^2)/2$. By induction we have that $\mathrm{ord}_N(3) = \phi(107^m)/2$ for all $m \geq 2$. The class number h of $\mathbb{Q}(\sqrt{-107})$ is equal to 3. Therefore we indeed have $\frac{1+p_1}{4} = p^h$ in this case. We obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with $v = q = 3^{53 \cdot 107^{m-1}}$, $k = \frac{v-1}{107}$, and with restrictedeigenvalues $r = \frac{53 \cdot 3^{h_0}-1}{107}$, $s = \frac{-54 \cdot 3^{h_0}-1}{107}$.

Construction 2. $N = p_1^m p_2$

We assume that $N = p_1^m p_2$ ($m \geq 1$), p_1, p_2 are primes such that $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, p is a prime such that $\gcd(p, N) = 1$ and $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$ and $\mathrm{ord}_{p_2}(p) = \phi(p_2)$. It follows that $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, and as before let $C_0, C_1, \ldots, C_{N-1}$ be the N-th cyclotomic classes of $\mathbb{F}_q$.

Note that we have $-C_i = C_i$ for all $0 \leq i \leq N-1$ since either $2N|(q-1)$ or q is even. Define

$$D = \cup_{i=0}^{p_1^{m-1}-1} C_{ip_2}.$$

Using D as connection set, we construct the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$.

Theorem. The Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is a regular graph of valency $|D|$, and it has at most five distinct restricted eigenvalues.

Let χ_1 be a character of order p_1^m and let χ_2 be a character of order p_2 of $\mathbb{F}_q^*$. Then using the evaluations of index 2 Gauss sums (a theorem by Mbodj from FFTA, 1998), we have

$$g(\bar{\chi}_1\bar{\chi}_2) = \frac{b + c\sqrt{-p_1p_2}}{2} p^{h_0},$$

where $h_0 = \frac{f-h}{2}$ (h is the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$), $b, c \not\equiv 0 \pmod{p}$, $b^2 + p_1p_2c^2 = 4p^h$, and $bp^{h_0} \equiv 2 \pmod{p_1p_2}$.

Corollary. Using the above notation, $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph if and only if $b, c \in \{1, -1\}$, h is even and $p_1 = 2p^{h/2} + (-1)^{\frac{p_1-1}{2}} b$, $p_2 = 2p^{h/2} - (-1)^{\frac{p_1-1}{2}} b$.

Example. Let $p = 2$, $p_1 = 3$, $p_2 = 5$, $N = 3^m \cdot 5$, with $m \geq 1$. One can easily prove by induction that $f := \mathrm{ord}_N(2) = \phi(N)/2 = 4 \cdot 3^{m-1}$ for all $m \geq 1$. The class number h of $\mathbb{Q}(\sqrt{-15})$ is equal to 2. Since $1 + p_1 p_2 = 4p^h$, we have $b, c \in \{1, -1\}$. From $bp^{(p_1-1)/2 \cdot (p_2-1)/2} \equiv 2p^{h/2} \pmod{p_1 p_2}$, we get $b = 1$. The conditions in the above Corollary are all satisfied. Therefore we obtain a strongly regular Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$, with

$$v = q = 2^{4 \cdot 3^{m-1}},\ k = \frac{v-1}{15} = 16^{3^{m-1}-1} + 16^{3^{m-1}-2} + \cdots + 16 + 1,$$

and with restricted eigenvalues $r = \frac{2^{h_0+3}-1}{15}$, $s = \frac{-7 \cdot 2^{h_0}-1}{15}$, where $h_0 = \frac{f-h}{2} = 2 \cdot 3^{m-1} - 1$.

Difference Sets

Let G be a multiplicatively written group of order v, and D a k-subset of G. We say that D is a (v, k, λ) *difference set* if the list of "differences" $xy^{-1}, x, y \in D, x \neq y$ contains each non-identity element of G precisely λ times.

A difference set D in G is said to be *Hadamard* if the parameters of D are $(4n-1, 2n-1, n-1)$ or $(4n-1, 2n, n)$.

A difference set D in a finite group G is called *skew Hadamard* (or antisymmetric) if G is the disjoint union of D, $D^{(-1)}$, and $\{1\}$, where $D^{(-1)} = \{d^{-1} \mid d \in D\}$.

A classical example: the Paley-Hadamard difference set (1933).

Let $q = 4n - 1$ be a prime power. Then the set D of nonzero squares of $\mathbb{F}_q$ is a skew Hadamard difference set in the additive group of $\mathbb{F}_q$.

A generalization using commutative semifields:

Theorem. (Weng, Qiu, Wang and X. 2007) Let $(S, +, *)$ be a commutative semifield of order q, where q is a prime power. Then $D := \{x * x \mid x \in S\} \setminus \{0\}$ is a skew Hadamard difference set in $(S, +)$ if $q \equiv 3 \pmod 4$, and D is a Paley type PDS if $q \equiv 1 \pmod 4$.

As before, let $q = p^f$, where p is a prime and f a positive integer. Let γ be a fixed primitive element of $\mathbb{F}_q$ and $N|(q-1)$ with $N > 1$. Let $C_0 = \langle \gamma^N \rangle$.

The case where $N = 4$. In this case C_0 is a difference set in $(\mathbb{F}_q, +)$ if $q = 4t^2 + 1$, where t is odd.

The case where $N = 8$. In this case C_0 is a difference set in $(\mathbb{F}_q, +)$ if $q = 8t^2 + 1 = 64u^2 + 9$, where t and u are both odd.

Conjecture. Let C_0 be defined as above. If C_0 is a difference set in $(\mathbb{F}_q, +)$, then N is necessarily $2, 4$, or 8.

Remarks. (1) This conjecture has been verified up to $N = 20$.

(2) The truth of the above conjecture implies that the only flag-transitive projective planes are the Desarguesian ones.

If one uses a union of cyclotomic classes, instead of just one single class, the only new family of difference sets found in this way is the Hall sextic difference sets.

The case where $N = 6$. Let C_0 be defined as above, and $C_i = \gamma^i C_0$, $1 \leq i \leq 5$. Then $C_0 \cup C_1 \cup C_3$ is a difference set in $(\mathbb{F}_q, +)$ if $q = 4x^2 + 27$ is congruent to 1 modulo 6.

One of the reasons that very few difference sets have been discovered by using unions of cyclotomic classes is that the investigations often relied on the so-called cyclotomic numbers and these numbers are in general very difficult to compute if N is large.

Skew Hadamard Difference Sets from Unions of Cyclotomic Classes

$N = 2p_1^m$, p_1 is prime, $m \geq 1$

Theorem. (Feng and X. 2011) Let p be a prime, $N > 1$ and $\gcd(p, N) = 1$. Assume that $f := \mathrm{ord}_N(p) = \phi(N)/2$ (that is, we are in the index 2 case), and $N = 2p_1^m$, with $p_1 \equiv 7 \pmod 8$. Let $q = p^f$ and C_i be the same as defined before. Let I be any subset of $\mathbb{Z}/N\mathbb{Z}$ such that

$$\{i \pmod{p_1^m} \mid i \in I\} = \mathbb{Z}/p_1^m\mathbb{Z}, \text{ and } D = \cup_{i \in I} C_i.$$

Then D is a skew Hadamard difference set in $(\mathbb{F}_q, +)$ if $p \equiv 3 \pmod 4$ and D is a Paley type PDS if $p \equiv 1 \pmod 4$.

Examples

Let $p_1 = 7$, $N = 14$, $p = 11$. Then it is routine to check that $\mathrm{ord}_N(p) = 3 = \phi(N)/2$. Let C_i, $0 \leq i \leq 13$, be the cyclotomic classes of order 14 of $\mathbb{F}_{11^3}$.

(1) Take $I = \{0, 1, 2, 3, 4, 5, 6\}$. Then by the above theorem, $D = C_0 \cup C_1 \cup \cdots \cup C_6$ is a skew Hadamard difference set in $(\mathbb{F}_{11^3}, +)$. Let $\mathrm{Dev}(D)$ denote the symmetric design developed from the difference set D. One can use a computer to find that $Aut(\mathrm{Dev}(D))$ has size $5 \cdot 11^3 \cdot 19$.

(2) Take $I = \{0, 1, 3, 4, 5, 6, 9\}$. Then $D' = C_0 \cup C_1 \cup C_3 \cup C_4 \cup C_5 \cup C_6 \cup C_9$ is also a skew Hadamard difference set in $(\mathbb{F}_{11^3}, +)$. One finds by using a computer that $Aut(\mathrm{Dev}(D'))$ has size $3 \cdot 5 \cdot 11^3 \cdot 19$.

The automorphism group of the Paley design has size $3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 19$. So the three difference sets D, D' and the Paley difference set in $(\mathbb{F}_{11^3}, +)$ are pairwise inequivalent.

Based on some computational evidence, we conjecture that $Aut(\mathrm{Dev}(D))$, with $D = \cup_{i \in I} C_i$ as given in the statement of the theorem, is generated by the following three types of elements: (i) translations by elements of $\mathbb{F}_q$, (ii) multiplications by elements in C_0, and (iii) σ_p^i, $p^i I = I$, where σ_p is the Frobenius automorphism of the finite field $\mathbb{F}_{p^f}$.

The case where $N = 2p_1^m$, p_1 is a prime congruent to 3 modulo 8:

This case is more complicated. We have a similar construction when $m = 1$. For details, please see the preprint "Cyclotomic constructions of skew Hadamard difference sets" `arXiv: 1101.2994v1`.

Thank you for your attention!