# Cyclotomy, difference sets, sequences with low correlation, strongly regular graphs, and related geometric substructures

Koji Momihara, Qi Wang and Qing Xiang

**Abstract.** In this paper, we survey constructions of and nonexistence results on combinatorial/geometric structures which arise from unions of cyclotomic classes of finite fields. In particular, we survey both classical and recent results on difference sets related to cyclotomy, and cyclotomic constructions of sequences with low correlation. We also give an extensive survey of recent results on constructions of strongly regular Cayley graphs and related geometric substructures such as $m$-ovoids and $i$-tight sets in classical polar spaces.

**Keywords.** Cyclotomy, difference set, finite geometry, projective two-intersection set, strongly regular graph, sequence.

**AMS classification.** 05B10, 05B25, 11T22.

## 1 Introduction

Let $q = p^\ell$ be a prime power, and $\mathbb{F}_q$ be the finite field of order $q$. We use $\mathbb{F}_q^*$ to denote the set of nonzero elements of $\mathbb{F}_q$. It is well known that $\mathbb{F}_q^*$ is a cyclic group of order $q-1$. When $q$ is odd, let $C_0$ denote the unique subgroup of index 2 of $\mathbb{F}_q^*$; that is, $C_0$ is the subgroup of $\mathbb{F}_q^*$ consisting of the nonzero squares of $\mathbb{F}_q$. The set $C_0$ has played very important roles in the construction of various combinatorial structures such as Hadamard matrices, difference sets, and strongly regular graphs. The earliest use of $C_0$ for constructing Hadamard matrices goes back to Paley [83]. Subsequently, many researchers considered using subgroups of $\mathbb{F}_q^*$ of higher indices and their cosets for constructing difference sets, binary sequences with low correlation, and strongly regular Cayley graphs, etc. The additive properties of the subgroups of $\mathbb{F}_q^*$ form a large part of what we call the theory of cyclotomy today. To a large extent, the theory of cyclotomy is a study of generalizations of Paley's work in [83].

We now give the definition of difference sets in a (not necessarily cyclic) group of order $v$. Let $G$ be a finite multiplicative group of order $v$. A $k$-element subset $D$ of $G$ is called a $(v, k, \lambda)$ *difference set* in $G$ if the list of "differences" $d_1 d_2^{-1}$, $d_1, d_2 \in D$,

Koji Momihara was supported by JSPS under Grant-in-Aid for Young Scientists (B) 17K14236 and Scientific Research (B) 15H03636. Qi Wang was supported by the National Natural Science Foundation of China under Grant no. 11601220. Qing Xiang was supported by an NSF grant DMS-1600850, and a JSPS invitational fellowship for research in Japan S17114.

$d_1 \neq d_2$, represents each nonidentity element in $G$ exactly $\lambda$ times. A moment's reflection shows that the translates of $D$ by all group elements form the blocks of a $(v, k, \lambda)$ symmetric design, and $G$ is a regular automorphism group of the design. For this reason difference sets play an important role in combinatorial design theory.

Given a subset $D$ in the cyclic group $(\mathbb{Z}/v\mathbb{Z}, +)$, we define its *characteristic sequence* $\mathbf{s} = (s_i)_{0\le i\le v-1}$ with the *support* $D$ by setting $s_i = 1$ if $i \in D$, and $s_i = -1$ otherwise. The *periodic autocorrelation* of a binary sequence $\mathbf{s}$ at the shift $\tau$, $0 \le \tau < v$, is defined as $\mathcal{A}_{\mathbf{s}}(\tau) = \sum_{i=0}^{v-1} s_i s_{i+\tau}$, where $i + \tau$ is read modulo the period $v$. From the definition of difference set, we see that $D$ is a $(v, k, \lambda)$ difference set in $\mathbb{Z}/v\mathbb{Z}$ if and only if

$$\mathcal{A}_{\mathbf{s}}(\tau) = \begin{cases} v, & \text{if } \tau \equiv 0 \pmod v, \\ v - 4(k-\lambda), & \text{otherwise.} \end{cases} \tag{1.1}$$

This shows the equivalence of binary sequences with two-level autocorrelation and cyclic $(v, k, \lambda)$ difference sets. More generally, $(v, k, \lambda)$ abelian difference sets are equivalent to binary arrays with two-level autocorrelation. For background material on difference sets, we refer the reader to the books [10, 65] and Chapter 6 of [12].

Let $q = p^\ell$ be a prime power, and let $\gamma$ be a fixed primitive element of $\mathbb{F}_q$. Let $N > 1$ be a divisor of $q - 1$. We define the $N^{\text{th}}$ *cyclotomic classes* $C_i^{(N,q)}$ of $\mathbb{F}_q$ by

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

where $0 \le i \le N - 1$. That is, $C_0^{(N,q)}$ is the subgroup of $\mathbb{F}_q^*$ consisting of all nonzero $N^{\text{th}}$ powers in $\mathbb{F}_q$, and $C_i^{(N,q)} = \gamma^i C_0^{(N,q)}$, for $1 \le i \le N - 1$. The case where $N = 2$ was first used by Paley [83] to construct the Paley difference set when $q \equiv 3 \pmod 4$, and the Paley graph when $q \equiv 1 \pmod 4$. Even though the construction is deterministic, the resulting combinatorial structures (i.e., the Paley difference sets/graphs) are pseudorandom or quasirandom. The $N^{\text{th}}$ cyclotomic classes (with $N > 2$) also exhibit pseudorandom behaviors.

(1) Roughly speaking, a pseudorandom graph is a graph that behaves like a random graph of the same edge density. The notion of quasirandom (also called pseudorandom) graphs was made precise by Thomason [98] and Chung, Graham and Wilson [21]. The Paley graphs are now standard examples of explicitly constructed quasirandom graphs.

(2) Elements of $C_0^{(N,q)}$ are distributed in $\mathbb{F}_q$ in a way that is random-like and also very regular at the same time. Here by random-like behavior, we mean that "being an $N^{\text{th}}$ power" is like a random event of probability $\frac{1}{N}$. For the precise statement we refer the reader to Sziklai [95] (see also [103]). The $N = 2$ case was treated by Szönyi [96] and Babai, Gal and Widgerson [3].

(3) The characteristic sequences of many difference sets from cyclotomic classes are pseudorandom with respect to certain randomness postulates, including balancedness, run property, low autocorrelation [52], pattern distribution [38], etc.

In this survey paper, we will mainly focus on constructions of various combinatorial/geometric structures by using cyclotomic classes. The paper is organized as follows. In Section 2, we survey both classical and recent results on difference sets related to cyclotomy. The highlights are some recent results of Xia [104] on the long-standing conjecture that if $C_0^{(N,q)}$ is a difference set in $(\mathbb{F}_q, +)$, then $N$ is a power of 2; and the constructions of skew Hadamard difference sets by Feng and the third author [48] by using unions of cyclotomic classes. In Section 3, we give a brief survey of results on sequences with low correlation which are related to cyclotomy. Section 4 is devoted to strongly regular Cayley graphs arising from cyclotomy and related geometric substructures such as $m$-ovoids and $i$-tight sets in polar spaces; many families of strongly regular Cayley graphs with new parameters have been constructed by using cyclotomic classes during the past few years; we survey these constructions and the more recent constructions of $m$-ovoids and $i$-tight sets in classical polar spaces.

## 2 Cyclotomy and difference sets

The idea of using cyclotomic classes to construct difference sets goes back to Paley [83]. In the mid-20th century, Baumert, Chowla, Hall, Lehmer, Storer, Whiteman, Yamamoto, etc. pursued this line of research vigorously. Storer's book [94] contains a summary of results in this direction up to 1967. Important in the study of cyclotomic (or power residue) difference sets are the cyclotomic numbers. Let $q = p^\ell$ be a prime power, and let $N > 1$ be a divisor of $q - 1$. As we did in Section 1, we use $C_i^{(N,q)}, 0 \le i \le N-1$, to denote the cyclotomic classes of index $N$ of $\mathbb{F}_q$. For integers $a, b$ with $0 \le a, b < N$, the cyclotomic number $(a, b)_N$ is defined by

$$(a, b)_N = |(C_a^{(N,q)} + 1) \cap C_b^{(N,q)}|.$$

Cyclotomic numbers are useful in many combinatorial investigations, including the study of difference sets in $(\mathbb{F}_q, +)$. These numbers $(a, b)_N$ for $q$ prime have been computed when $N \le 24$ and $N \notin \{13, 17, 19, 21, 22, 23\}$ (cf. [11, p.152]). But it should be noted that when $N$ is large, the formulae given for $(a, b)_N$ are often not explicit. In the following two subsections, we survey recent results on existence/nonexistence results on difference sets in $(\mathbb{F}_q, +)$ arising from unions of cyclotomic classes.

### 2.1 A Single Class

We first consider the question when a cyclotomic class $C_i^{(N,q)}$, where $i$ is some integer such that $0 \le i \le N - 1$, is a difference set in $(\mathbb{F}_q, +)$. Since $C_i^{(N,q)} = \gamma^i C_0^{(N,q)}$,

the question is equivalent to: When is the cyclotomic class $C_0^{(N,q)}$ a difference set in $(\mathbb{F}_q, +)$? Paley [83] is the first to answer this question completely in the case when $N = 2$. Later, Chowla [20] settled the problem in the case when $q$ is prime and $N = 4$; Lehmer [67] gave necessary and sufficient conditions for $C_0^{(N,q)}$ to be a difference set in $(\mathbb{F}_q, +)$ in terms of cyclotomic numbers.

**Theorem 2.1.** *Let $C_0^{(N,q)}$ be defined as above. Then $C_0^{(N,q)}$ is a difference set in $(\mathbb{F}_q, +)$ if and only if $N$ is even, $(q-1)/N$ is odd, and*

$$(a,0)_N = \frac{(q-1-N)}{N^2}$$

*for $a = 0, 1, 2, \ldots, \frac{N}{2} - 1$.*

Theorem 2.1 is useful when $N$ is small. Using this theorem, not only one can recover the results of Paley and Chowla, but also obtain complete results in the cases where $N = 6$ or 8.

**Theorem 2.2.** ([67]) *Let $\mathbb{F}_q$ be the finite field of order $q$, where $q = p^\ell$ is a power of an odd prime $p$. Let $N \geq 2$ be an even divisor of $q-1$, and $C_0^{(N,q)}$ be the subgroup of $\mathbb{F}_q^*$ of index $N$.*

*(1) When $N = 2$, $C_0^{(2,q)}$ is a difference set in $(\mathbb{F}_q, +)$ if and only if $q \equiv 3 \pmod 4$.*

*(2) When $N = 4$, $C_0^{(4,q)}$ is a difference set in $(\mathbb{F}_q, +)$ if and only if $q = p = 1 + 4t^2$ for some odd integer $t$.*

*(3) When $N = 6$, $C_0^{(6,q)}$ is never a difference set in $(\mathbb{F}_q, +)$.*

*(4) When $N = 8$, $C_0^{(8,q)}$ is a difference set in $(\mathbb{F}_q, +)$ if and only if $q = p = 1+8u^2 = 9 + 64v^2$ for some odd integers $u$ and $v$.*

There are a couple of folklore conjectures in this area. It seems difficult to find the exact origin of these conjectures. The third author of the survey was certainly aware of these conjectures many years ago; for example, the stronger conjecture below was mentioned explicitly in [48, p. 246] and [106]. It is quite certain that the history of these conjectures is much longer. The first conjecture is the weaker conjecture.

**Conjecture 2.3.** *Let $\mathbb{F}_q$ be the finite field of order $q$, where $q = p^\ell$ is an odd prime power. Let $N \geq 2$ be an even divisor of $q-1$, and $C_0^{(N,q)}$ be the subgroup of $\mathbb{F}_q^*$ of index $N$. If $C_0^{(N,q)}$ is a difference set in $(\mathbb{F}_q, +)$, then $N$ must be a power of 2.*

The next conjecture is stronger.

**Conjecture 2.4.** *Let $\mathbb{F}_q$ be the finite field of order $q$, where $q = p^\ell$ is an odd prime power. Let $N \geq 2$ be an even divisor of $q-1$, and $C_0^{(N,q)}$ be the subgroup of $\mathbb{F}_q^*$ of index $N$. If $C_0^{(N,q)}$ is a difference set in $(\mathbb{F}_q, +)$, then $N = 2, 4,$ or 8.*

We mention that in a recent paper [104], Xia posed essentially the same conjectures as the above folklore conjectures. (It seems that Xia was unaware of the existence of the folklore conjectures above.) Many researchers worked towards settling these conjectures. In the period 1953-1967, the combined work of seven authors showed the nonexistence of difference sets of the form $C_0^{(N,p)}$ in $(\mathbb{F}_p, +)$ for all $8 < N < 20$, where $p$ is an odd prime; see the book [10] and [11, Chapter 5] for references. In 1970, Muskat and Whiteman [77] obtained partial results for the $N = 20$ case. Evans [42] finally finished the $N = 20$ case by proving that $C_0^{(20,p)}$ is never a difference set in $(\mathbb{F}_p, +)$, where $p$ is an odd prime. All these nonexistence results were obtained by using Theorem 2.1 and cyclotomic numbers. When $N$ is large, Lehmer's theorem is not very useful since the cyclotomic numbers involved are difficult to compute; instead Gauss sums and Jacobi sums have proved to be more effective. In a recent paper [104], by using Jacobi sums and extensive Gröbner basis computations of certain overdetemined polynomial systems, Xia proved the following theorem.

**Theorem 2.5.** ([104]) *Let $\mathbb{F}_q$ be the finite field of order $q$, where $q = p^f$ is an odd prime power. Let $N \geq 2$ be an even divisor of $q - 1$, and $C_0^{(N,q)}$ be the subgroup of $\mathbb{F}_q^*$ of index $N$. If $N \leq 22$ and $N \neq 2, 4$ or $8$, then $C_0^{(N,q)}$ is never a difference set in $(\mathbb{F}_q, +)$.*

Very recently, Evans and Van Veen [41] proved nonexistence of power residue difference sets in $(\mathbb{F}_p, +)$ for the case where $N = 24$ and $p$ is a prime by computing cyclotomic numbers with the help of a Mathematica program.

The investigations of the problem when $C_0^{(N,q)}$ is a difference set in $(\mathbb{F}_q, +)$ have also been motivated by questions in finite geometry. A finite projective plane is said to be *flag-transitive* if its group of automorphisms acts transitively on the point-line flags. Clearly Desarguesian planes are flag-transitive. Conversely, it is an old and fundamental conjecture in the theory of projective planes, first mentioned in Higman and McLaughlin [58], that every flag-transitive finite projective plane is Desarguesian. The following theorem, mainly proved by Kantor [62], relates flag-transitive projective planes to cyclotomic difference sets.

**Theorem 2.6.** *If there exists a non-Desarguesian flag-transitive projective plane of order $n$, then $n^2 + n + 1 := p$ is prime, $n > 8$ is even, and $C_0^{(n,p)}$ is a $(p, n + 1, 1)$-difference set in $(\mathbb{F}_p, +)$.*

By the above theorem, the validity of Conjecture 2.4 implies that finite flag-transitive projective planes must be Desarguesian. This provided strong motivations to investigate Conjectures 2.3 and 2.4. Even though many researchers have worked on Conjectures 2.3 and 2.4 for more than sixty years, it seems that we are still far from solving these conjectures. Thas and Zagier [97] investigated the special case of Conjectures 2.3 and 2.4 related to flag-transitive projective planes. They [97] called a pair

$(p, n)$ *special*, where $p$ is an odd prime and $1 < n < p-1$ an integer dividing $p-1$, if $C_0^{(n,p)}$ is a $(p, n+1, 1)$-difference set in $(\mathbb{F}_p, +)$. Using nontrivial computations, Thas and Zagier [97] classified all special pairs $(p, n)$, when $p < 4 \times 10^{22}$; no surprises arise from the classification.

To end this subsection, we caution the readers that two papers with serious mistakes got published during the past 30 years. Feit [43] claimed that if there is a non-Desarguesian projective plane of order $n$, then $n$ is not a power of 2. In [82], Ott claimed that any flag-transitive finite projective plane has prime power order. Together with Theorem 2.6, these two results would imply the nonexistence of non-Desarguesian flag-transitive finite projective planes. Unfortunately both papers, [43] and [82], contain serious mistakes. We refer the readers to [108] and [97] for the exact places in [43, 82] where the mistakes were made.

## 2.2 Two or More Classes

If Conjecture 2.4 is true, then $C_0^{(N,q)}$ is rarely a difference set in $(\mathbb{F}_q, +)$. So a natural question is: When is a union of two or more cyclotomic classes a difference set in $(\mathbb{F}_q, +)$ while a single cyclotomic class is not? So far there have been very few results on this question. The first result is a constructive one due to Marshal Hall Jr. [54]. See also [55, Section 11.6].

**Theorem 2.7.** *Let $q$ be an odd prime power of the form $q = 4x^2 + 27$ for some integer $x$. Then $C_0^{(6,q)} \cup C_1^{(6,q)} \cup C_3^{(6,q)}$ is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$ difference set in $(\mathbb{F}_q, +)$.*

The difference sets arising from the above theorem are usually called *the Hall sextic residue difference sets*. They were first constructed in the case where $q$ is a prime of the form $4x^2 + 27$. Later in [55], the construction was done in the more general setting where $q$ is a prime power of the form $4x^2 + 27$. However, we note that, as pointed out in [81], there are only finitely many proper prime powers of the form $4x^2 + 27$. A second remark is that the above theorem was proved in [54, 55] by rather detailed computations of the cyclotomic numbers $(a, b)_6$. It would be interesting to have a proof without using cyclotomic numbers. The reason is that having such a proof will probably pave the way for discovering new difference sets. The investigations of cyclotomic difference sets in the 20th century relied heavily on cyclotomic numbers which are in general very difficult to compute if $N$ is large. It appears that methods using Gauss sums and Jacobi sums directly are more effective for large $N$.

After Marshall Hall Jr.'s work in 1956, several researchers investigated the question when a union of two or more cyclotomic classes is a difference set in the cases where $N = 8, 10$, or 12; only one sporadic difference set, a $(31, 6, 1)$-difference set which is a union of two cyclotomic classes, was found [56] in the case where $N = 10$. Most researchers thought that no new difference sets can be found by taking unions of cyclotomic classes. Therefore it came as a great surprise that in 2012 Feng and the third author [48] found new infinite families of difference sets by taking unions

of cyclotomic classes with $N = 2p_1^m$, where $p_1$ is a prime. We give the detailed statement below. (A difference set $D$ in an additively written finite group $G$ is called *skew Hadamard* if $G$ is the disjoint union of $D$, $-D$, and $\{0\}$. A skew Hadamard difference set in a group of order $v$ necessarily has parameter $(v, \frac{v-1}{2}, \frac{v-3}{4})$.)

**Theorem 2.8.** ([48]) *Let $p_1 \equiv 7 \pmod 8$ be a prime, $N = 2p_1^m$, and let $p$ be a prime such that $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $s$ be an odd integer, $q = p^{fs}$, $I$ any subset of $\mathbb{Z}/N\mathbb{Z}$ such that $\{i \pmod{p_1^m} \mid i \in I\} = \mathbb{Z}/p_1^m\mathbb{Z}$, and let*

$$D = \bigcup_{i \in I} C_i^{(N,q)} \subseteq \mathbb{F}_q^*.$$

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

Several remarks are in order. First, the proof of the above theorem uses index 2 Gauss sums instead of cyclotomic numbers. Second, the difference sets from Theorem 2.8 are not cyclic since the $f$ satisfying the conditions of the theorem is always greater than 1. Third, there is a lot of flexibility in choosing the index set $I$ in Theorem 2.8; namely, there are $2^{p_1^m}$ choices for the index set $I$ since each pair $\{i, i + p_1^m\}$, $0 \le i \le p_1^m - 1$, contributes exactly one element to $I$. Fourth, the inequivalence between the difference sets from Theorem 2.8 and the Paley difference sets was proved by the first author in [73] by using triple intersection numbers.

The case where $p_1$ is a prime congruent to 3 modulo 8 and $N = 2p_1^m$ is more complicated. Feng and the third author [48] first gave a construction of skew Hadamrd difference sets in the case where $N = 2p_1$, $p_1 \equiv 3 \pmod 8$ is a prime. Later on, this construction was generalized by Feng, Momihara and Xiang [46] to work in the case where $N = 2p_1^m$, $p_1 \equiv 3 \pmod 8$ is a prime. Below we state the construction from [46].

**Theorem 2.9.** ([46]) *Let $p_1 \equiv 3 \pmod 8$ be a prime, $p_1 \neq 3$, $N = 2p_1^m$, and let $p \equiv 3 \pmod 4$ be a prime such that $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, $J = \langle p \rangle \cup 2\langle p \rangle \cup \{0\} \pmod{2p_1}$, and define*

$$D = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j \in J} C_{2i+p_1^{m-1}j}$$

*Assume that $1 + p_1 = 4p^h$, where $h$ is the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then $D$ is a skew Hadamard difference set in the additive group of $\mathbb{F}_q$.*

Note that in Theorem 2.9, we need to choose a suitable primitive element $\gamma$ of $\mathbb{F}_q$ in order for the construction to work. We refer the reader to [46] for details on how to choose such a primitive element of $\mathbb{F}_q$.

# 3 Sequences with low correlation from cyclotomy

In this section, we survey results on binary and quaternary sequences with low correlation. Since there exist several excellent surveys on this subject, e.g. [1, 31, 53, 57, 90], we will concentrate on sequences constructed by using cyclotomy. As indicated in (1.1), binary sequences with two-level periodic autocorrelation $\{-1, v\}$ are equivalent to cyclic difference sets with parameters $(v, (v-1)/2, (v-3)/4)$. Cyclotomy is a powerful tool for constructing such cyclic difference sets, as we saw in Section 2. Note that the Paley difference set is the classical example of such cyclic difference sets (with $v = p$ a prime) from cyclotomy, and the corresponding characteristic sequence is usually called *the Legendre sequence* since the sequence can be defined by the Legendre symbol. In addition, binary sequences of composite length, and quaternary sequences, can also be explicitly constructed using cyclotomy. Below we give a summary of results on such sequences constructed from cyclotomy.

## 3.1 Binary sequences from cyclotomy

By (1.1), clearly we have $\mathcal{A}_{\mathbf{s}}(\tau) \equiv v \pmod 4$. Thus, it is natural to classify binary sequences into four categories according to $v \equiv 3 \pmod 4$, $v \equiv 2 \pmod 4$, $v \equiv 1 \pmod 4$, and $v \equiv 0 \pmod 4$. For each of these four categories, cyclotomy has played an important role in constructing such binary sequences. For $v \equiv 3 \pmod 4$, binary sequences with two-level autocorrelation $\{-1, v\}$ are said to have *ideal* autocorrelation (for good surveys, see [17, 53, 105]). It seems very difficult to completely classify binary sequences with ideal autocorrelation, either in terms of sequences or in terms of their supports which are cyclic difference sets. Among the known constructions, there are three arising from cyclotomy:

(1) the characteristic sequences of Paley difference sets [83];

(2) the characteristic sequences of Hall sextic difference sets [54];

(3) the twin-prime sequences involving cyclotomic classes of index 2 in both $\mathbb{F}_p$ and $\mathbb{F}_{p+2}$ [93], where $p$ and $p+2$ are twin primes.

We remark that $p$-ary sequences with ideal two-level autocorrelation $\{-1, v\}$ are equivalent to relative difference sets with Singer parameters, and are characterized by the $d$-homogeneous property [86, 87].

A natural question to ask is whether there exist binary sequences with two-level autocorrelation in the other three categories for which $v \not\equiv 3 \pmod 4$. This question remains open. However, it is evident that the optimal cases for $v \not\equiv 3 \pmod 4$ are binary sequences with three-level autocorrelation [61] (called *optimal* autocorrelation). The supports of such binary sequences with optimal autocorrelation are almost difference sets. (A subset $D$ of a finite group $G$ is called an *almost difference sets* if the list of "differences" $d_1 d_2^{-1}$, with $d_1, d_2 \in D$ and $d_1 \neq d_2$ represents each nonidentity element in $G$ either $\lambda$ times or $\lambda + 1$ times [2, 40].) For $v \equiv 2 \pmod 4$, there are

two constructions of binary sequences with three-level autocorrelation $\{2, -2, v\}$ related to cyclotomy: One was given by Sidelnikov [92] (see also [99, 68]), where the support $D \subseteq (\mathbb{Z}/(q-1)\mathbb{Z}, +)$ is defined as $\log_\gamma(C_1^{(2,q)} - 1)$ with $q \equiv 3 \pmod 4$ a prime power and $\gamma$ a primitive element of $\mathbb{F}_q$; the other construction was given by Ding, Helleseth and Martinsen [40], which in fact uses a union of cyclotomic classes of index 4 and relies on the explicit computations of cyclotomic numbers.

For the case $v \equiv 1 \pmod 4$, all three currently known constructions of binary sequences with autocorrelation values $\{1, -3, v\}$ involve cyclotomy: the first is the Legendre sequence, whose support is the Paley partial difference set; the second was given by Ding, Helleseth and Lam [39], and the support is a union of two consecutive cyclotomic classes of index 4, i.e., $D = C_0^{(4,p)} \cup C_1^{(4,p)}$, where $p = x^2 + 4$ is a prime with $x \equiv 1 \pmod 4$; the third construction utilized the so-called generalized cyclotomy, which generalized the twin-prime construction of difference sets to that of almost difference sets by cyclotomic classes of index 2 in both $\mathbb{F}_p$ and $\mathbb{F}_{p+4}$, where both $p$ and $p + 4$ are primes. We note that the second construction $D = C_0^{(4,p)} \cup C_1^{(4,p)}$ was discussed in [102], where the corresponding pseudo-Paley graphs were distinguished from the classical Paley graphs by using $p$-ranks.

Most of the constructions in the case where $v \equiv 0 \pmod 4$ interleave four appropriately shifted copies of binary sequences with ideal two-level autocorrelation, while the construction by Sidelnikov [92] is an exception: $D := \log_\gamma(C_1^{(2,q)} - 1)$ with $q \equiv 1 \pmod 4$ a prime power and $\gamma$ a primitive element in $\mathbb{F}_q$.

### 3.2 Quaternary sequences from cyclotomy

Given a quaternary sequence $\mathbf{s}$ of period $v$ over $\{1, i, -1, i^3\}$ where $i = \sqrt{-1}$, the *periodic autocorrelation* at shift $\tau$ with $0 \le \tau < v$ is defined as $\mathcal{A}_{\mathbf{s}}(\tau) = \sum_{i=0}^{v-1} s_i \overline{s_{i+\tau}}$, where $i + \tau$ is read modulo $v$. Each quaternary sequence can be interpreted as two binary sequences via the inverse Gray mapping $\phi^{-1} : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, where $\phi^{-1}(0,0) = 0$, $\phi^{-1}(0,1) = 1$, $\phi^{-1}(1,1) = 2$, and $\phi^{-1}(1,0) = 3$. There are many results on quaternary sequences with binary sequences with low autocorrelation as building blocks due to [64, Eqn. (6)]. Instead of giving a complete survey of these results in this section (for recent progress, see for example [72]), we present two constructions of quaternary sequences directly from cyclotomic classes.

The first construction again is due to Sidelnikov [92], which generates quaternary sequences by $\log_\gamma(C_j^{(4,q)} - 1)$ for $j = 0, 1, 2, 3$ with $q - 1$ divisible by 4 and $\gamma$ a primitive element in $\mathbb{F}_q$. More generally, for an arbitrary divisor $M$ of $q - 1$, $M$-ary sequences of period $q - 1$ are obtained in this way with autocorrelation upper bounded by 4.

Very recently, a construction of quaternary sequences with autocorrelation bounded by 3 was proposed in [72] from cyclotomic classes of index 8. Let $p = x^2 + 16 = a^2 + 2b^2 \equiv 1 \pmod{16}$ ($x \equiv a \equiv 1 \pmod 4$) be a prime such that $x - a = 4$.

Define $D_0 = C_2^{(8,p)} \cup C_6^{(8,p)}$, $D_1 = C_1^{(8,p)} \cup C_3^{(8,p)}$, $D_2 = C_0^{(8,p)} \cup C_4^{(8,p)}$, and $D_3 = C_5^{(8,p)} \cup C_7^{(8,p)}$, and the quaternary sequence $\mathbf{s}$ of period $p$ is defined by

$$s_t = (\sqrt{-1})^j, \qquad \text{if } t \in D_j,$$

for $j \in \{0,1,2,3\}$ and $s_0 = 1$. Then the quaternary sequence $\mathbf{s}$ has autocorrelation values $\{-1,-3,3,p\}$. The proof was completed by an explicit computation of cyclotomic numbers of order 8. Note that the first several primes satisfying the conditions of this construction are $17, 97, 641, 2417, 6577, 14657$.

## 4 Strongly regular Cayley graphs from cyclotomy

A *strongly regular graph* $\mathrm{srg}(v,k,\lambda,\mu)$ is a simple and undirected graph, neither complete nor edgeless, that has the following properties:

(1) It is a regular graph of order $v$ and valency $k$.

(2) For each pair of adjacent vertices $x, y$, there are $\lambda$ vertices adjacent to both $x$ and $y$.

(3) For each pair of nonadjacent vertices $x, y$, there are $\mu$ vertices adjacent to both $x$ and $y$.

Let $\Gamma$ be a (simple, undirected) graph. The adjacency matrix of $\Gamma$ is the $(0,1)$-matrix $A$ with both rows and columns indexed by the vertex set of $\Gamma$, where $A_{xy} = 1$ when there is an edge between $x$ and $y$ in $\Gamma$ and $A_{xy} = 0$ otherwise. A useful way to check whether a graph is strongly regular is by using the eigenvalues of its adjacency matrix. For convenience we call an eigenvalue *restricted* if it has an eigenvector which is not a multiple of the all-ones vector $\mathbf{1}$. (For a $k$-regular connected graph, the restricted eigenvalues are the eigenvalues different from $k$.)

**Theorem 4.1.** *For a simple graph $\Gamma$ of order $v$, neither complete nor edgeless, with adjacency matrix $A$, the following are equivalent:*

(i) *$\Gamma$ is strongly regular with parameters $(v,k,\lambda,\mu)$ for certain integers $k,\lambda,\mu$,*

(ii) *$A^2 = (\lambda-\mu)A + (k-\mu)I + \mu J$ for certain real numbers $k,\lambda,\mu$, where $I, J$ are the identity matrix and the all-ones matrix, respectively,*

(iii) *$A$ has precisely two distinct restricted eigenvalues.*

For a proof of Theorem 4.1, we refer the reader to [15]. An effective method to construct strongly regular graphs is by using Cayley graphs. Let $G$ be an additively written group of order $v$, and let $D$ be a subset of $G$ such that $0 \notin D$ and $-D = D$, where $-D = \{-d \mid d \in D\}$. The *Cayley graph on $G$ with connection set $D$*, denoted by $\mathrm{Cay}(G,D)$, is the graph with the elements of $G$ as vertices; two vertices are adjacent if and only if their difference belongs to $D$. In the case when $\mathrm{Cay}(G,D)$ is a strongly regular graph, the connection set $D$ is called a (regular) *partial difference*

*set*. Examples of strongly regular Cayley graphs are the Paley graphs $\mathrm{P}(q)$, where $q$ is a prime power congruent to 1 modulo 4, the Clebsch graph, and the affine orthogonal graphs ([15]). For $\Gamma = \mathrm{Cay}(G, D)$ with $G$ abelian, the eigenvalues of $\Gamma$ are exactly $\chi(D) := \sum_{d\in D} \chi(d)$, where $\chi$ runs through the character group of $G$. This fact reduces the problem of computing eigenvalues of abelian Cayley graphs to that of computing some character sums, and is the underlying reason why the Cayley graph construction has been very effective for the purpose of constructing srgs. The survey of Ma [69] contains much of what is known about partial difference sets and about connections with strongly regular graphs.

In this section, we always take the additive group of a finite field as the underlying group $G$ and take a union of cyclotomic classes as connection sets. Many reseachers have studied the problem of determining when a union $D$ of cyclotomic classes forms a partial difference set. In some of the papers, the authors used the language of codes or finite geometry in their studies instead of strongly regular Cayley graphs or partial difference sets. We choose to use the language of srgs here.

**Example 4.2.** *Here are three known "sporadic" examples of strongly regular Cayley graphs on finite fields:*

*(1) ([101])* $\mathrm{Cay}(\mathbb{F}_{3^4}, D)$ *with* $D = \bigcup_{i\in\{0,1,3\}} C_i^{(8,3^4)}$ *is an srg*$(3^4, 30, 9, 12)$*;*

*(2) ([59])* $\mathrm{Cay}(\mathbb{F}_{2^{12}}, D)$ *with* $D = \bigcup_{i\in\{0,7\}} C_i^{(35,2^{12})}$ *is an srg*$(2^{12}, 234, 2, 14)$*;*

*(3) ([35])* $\mathrm{Cay}(\mathbb{F}_{3^8}, D)$ *with* $D = \bigcup_{i\in\{0,1,2,8,10,11,13\}} C_i^{(16,3^8)}$ *is an srg*$(3^8, 2870, 1249, 1260)$.

## 4.1 Cyclotomic strongly regular graphs

Let $p$ be a prime, $\ell$ and $m$ be positive integers, and let $q = p^\ell$. Let $N > 1$ be an integer such that $N|(q^m - 1)$, and $\gamma$ be a primitive element of $\mathbb{F}_{q^m}$. For a subset $D$ of $\mathbb{F}_{q^m}^*$, we call $\mathrm{Cay}(\mathbb{F}_{q^m}, D)$ a *cyclotomic strongly regular graph* if $D$ is a single cyclotomic class of $\mathbb{F}_{q^m}$ and $\mathrm{Cay}(\mathbb{F}_{q^m}, D)$ is strongly regular. The Paley graphs are primary examples of cyclotomic srgs. Also, if $D$ is the multiplicative group of a subfield of $\mathbb{F}_{q^m}$, then it is clear that $\mathrm{Cay}(\mathbb{F}_{q^m}, D)$ is strongly regular. These cyclotomic srgs are usually called *subfield examples*. Next, if there exists a positive integer $j$ such that $p^j \equiv -1 \pmod N$, then $\mathrm{Cay}(\mathbb{F}_{q^m}, D)$ is strongly regular. See [9] for a proof of this result. These examples are usually called *semi-primitive*. A generalization of semi-primitive srgs so that its connection set is a union of at least two cyclotomic classes was given in [14]; that generalization will be explained in Subsection 4.2.

In [89], Schmidt and White gave the following necessary and sufficient condition for $\mathrm{Cay}(\mathbb{F}_{q^m}, D)$ to be a cyclotomic srg.

**Theorem 4.3.** ([89]) *With notation as above, assume that* $N$ *divides* $(q^m - 1)/(q - 1)$. *Let* $f$ *be the order of* $p$ *modulo* $N$, *and put* $s = m\ell/f$. *Then,* $\mathrm{Cay}(\mathbb{F}_{q^m}, C_0^{(N,q^m)})$ *is*

*strongly regular if and only if there exists a positive integer $u$ satisfying the following three conditions:*

*(i)* $u \mid (N-1)$;

*(ii)* $up^{st} \equiv \pm 1 \pmod{N}$;

*(iii)* $u(N-u) = (N-1)p^{s(f-2t)}$.

*Here, $t$ is the largest power of $p$ dividing the Gauss sums $G_{q^m}(\chi)$ for all nontrivial multiplicative character $\chi$ of $\mathbb{F}_{q^m}$ of order dividing $N$.*

The necessary and sufficient conditions in the above theorem can be used to search for cyclotomic srgs $\mathrm{Cay}(\mathbb{F}_{q^m}, C_0^{(N,q^m)})$ with large $N$. The eleven sporadic examples in Table 1 which are neither subfield examples nor semi-primitive examples were found in this way in [89] (some of the eleven examples in Table 1 were already known before the search conducted in [89]; see [8, 66]). A generalization of these sporadic examples so that their connection sets are union of at least two cyclotomic classes was given in [46, 49, 51, 74]. We will explain that generalization in Subsection 4.3.

Table 1. Eleven sporadic examples

| No. | $N$ | $q$ | $m$ | $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle]$ |
|---|---|---|---|---|
| 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 |

On the other hand, Schmidt and White [89] made the following conjecture on cyclotomic srgs, which can be thought as a counterpart of Conjecture 2.4 for cyclotomic srgs.

**Conjecture 4.4.** ([89]) *Assume that $N \mid (q^m-1)/(q-1)$. Then,* $\mathrm{Cay}(\mathbb{F}_{q^m}, C_0^{(N,q^m)})$ *is strongly regular if and only if it is either a subfield example, or a semi-primitive example or one of the eleven sporadic examples of Table 1.*

The Schmidt-White conjecture remains open. There are some results on this conjecture in [89] under the condition $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle] = 2$ and the assumption of the generalized Riemann hypothesis.

**Remark 4.5.** Theorem 4.3 and Conjecture 4.4 were stated in terms of two-weight irreducible cyclic codes in [89]. We briefly explain the connection between two-weight irreducible cyclic codes and cyclotomic srgs below.

For a positive divisor $n$ of $q^m - 1$, let $\xi$ be a primitive $n$th root of unity in $\mathbb{F}_{q^m}$. Then,

$$C = \left\{ c(y) := \left(\mathrm{Tr}_{q^m/q}(y\xi^i)\right)_{i=0}^{n-1} \mid y \in \mathbb{F}_{q^m} \right\}$$

is called an *irreducible cyclic code* of length $n$ over $\mathbb{F}_q$. McEliece [70] showed that if $N := (q^m-1)/n$ divides $(q^m-1)/(q-1)$, the Hamming weight of $c(y)$ for $y \in \mathbb{F}_{q^m}^*$ is given by

$$\frac{(q-1)}{qN}(q^m - 1 - N \cdot \psi_{\mathbb{F}_{q^m}}(yC_0^{(N,q^m)})),$$

where $\psi_{\mathbb{F}_{q^m}}$ is the canonical additive character of $\mathbb{F}_{q^m}$. Hence, $C$ is a two-weight code if and only if $\psi_{\mathbb{F}_{q^m}}(yC_0^{(N,q^m)})$, $y \in \mathbb{F}_{q^m}^*$, take exactly two values, i.e., $\mathrm{Cay}(\mathbb{F}_{q^m}, C_0^{(N,q^m)})$ is strongly regular. For more details on the correspondence between projective two-weight codes and strongly regular Cayley graphs on finite fields, see, e.g., [15, p. 140].

## 4.2 A generalization of semi-primitive examples

Let $q = p^m$ be a prime power with $p$ a prime and $N$ be a positive integer dividing $q-1$. Let $\gamma$ be a primitive element of $\mathbb{F}_q$. Assume that there is a $j > 0$ such that $p^j \equiv -1 \pmod N$. Choose $j$ minimal with this property and write $m = 2js$.

The following theorem is a generalization of semi-primitive examples of cyclotomic srgs so that their connection sets are unions of at least two cyclotomic classes.

**Theorem 4.6.** ([14, 18]) *With notation as above, let $J$ be a subset of $\{0,1,\ldots,N-1\}$ of size $\ell$ and $D = \bigcup_{i\in J} C_i^{(N,q)}$. If $D = -D$, then $\mathrm{Cay}(\mathbb{F}_q, D)$ is an srg with parameters $(u^2, r(u-\epsilon)\epsilon u + r^2 - 3\epsilon r, r^2 - \epsilon r)$ with $u = p^{js}$ and $r = \ell(p^{js}+\epsilon)/N$, where $\epsilon = -1$ or $1$ depending on whether $s$ is even or odd. In particular, for $a = 0,1,\ldots,N-1$,*

$$\psi_{\mathbb{F}_q}(\gamma^a D) = \frac{u((-1)^s\sqrt{q}-1)}{N} + \begin{cases} (-1)^{s+1}\sqrt{q}, & \text{if } \delta^s = 1 \text{ and } a \in -J \pmod N \\ & \quad \text{or } \delta^s = -1 \text{ and } a \in -J + N/2 \pmod N, \\ 0, & \text{otherwise,} \end{cases}$$

*where*

$$\delta = \begin{cases} 1, & \text{if } N \text{ is even and } (p^j+1)/N \text{ is odd,} \\ -1, & \text{otherwise.} \end{cases}$$

We mention that an srg is said to be of *Latin square type* (respectively, *negative Latin square type*) if $(v,k,\lambda,\mu)=(u^2,r(u-\epsilon),\epsilon u+r^2-3\epsilon r,r^2-\epsilon r)$ and $\epsilon=1$ (respectively, $\epsilon=-1$). Most known strongly regular Cayley graphs are of Latin square or negative Latin square type.

In [14], the following two further generalizations were given. Pick several positive integers $N_i$, $i\in I$, with $N_i\mid(q-1)$. For each $i\in I$, let $J_i$ be a subset of $\{0,1,\ldots,N_i-1\}$. We define $D_i=\bigcup_{j\in J_i}C_j^{(N_i,q)}$, and assume that $D_i$ are mutually disjoint. Then, it is possible for $D$ to give rise to a strongly regular Cayley graph. The precise statements are given below.

**Proposition 4.7.** *Let $p$ be an odd prime and $N_i=p^{j_i}+1$ for $i=1,2$. Let $q=p^m$ with $m=4j_1s_1=4j_2s_2$. Take $J_1$ as a subset of $\{2h\mid h=0,1,\ldots,N_1/2-1\}$ and $J_2$ as a subset of $\{2h+1\mid h=0,1,\ldots,N_2/2-1\}$. Define $D_i=\bigcup_{j\in J_i}C_j^{(N_i,q)}$, $i=1,2$, and $D=D_1\cup D_2$. Then, $\mathrm{Cay}(\mathbb{F}_q,D)$ is an srg of negative Latin square type.*

The proof of Proposition 4.7 is obvious since $D_1\cap D_2=\emptyset$ and $a\in -J_i\pmod{N_i}$ cannot hold for $i=1$ and 2 simultaneously.

**Example 4.8.** *Let $(p,j_1,j_2,N_1,N_2,f)=(3,1,2,4,10,8)$, $J_1=\{0\}$, $J_2=\{1\}$, and $J=\{0,1,4,8,11,12,16\}$. Then,*

$$D=\bigcup_{i=1,2}\bigcup_{h\in J_1}C_h^{(N_i,q)}=\bigcup_{h\in J}C_h^{(20,q)},$$

*and $\mathrm{Cay}(\mathbb{F}_q,D)$ is an srg with parameters $(v,k,\lambda,\mu)=(3^8,2296,787,812)$.*

Similar to Proposition 4.7, we have the following.

**Proposition 4.9.** *Let $p$ be an odd prime and $N_i=p^{j_i}+1$ for $i=1,2$. Let $q=p^m$ with $m=2j_1s_1=2j_2s_2$, where $s_1$ and $s_2$ are odd. Take $J_1$ as a subset of $\{2h\mid h=0,1,\ldots,N_1/2-1\}$ and $J_2$ as a subset of $\{2h+1\mid h=0,1,\ldots,N_2/2-1\}$. Assume that $\bigcup_{i\in J_1}C_{-i+N_1/2}^{(N_1,q)}$ and $\bigcup_{i\in J_2}C_{-i+N_2/2}^{(N_2,q)}$ are disjoint. Define $D_i=\bigcup_{j\in J_i}C_j^{(N_i,q)}$, $i=1,2$, and $D=D_1\cup D_2$. Then, $\mathrm{Cay}(\mathbb{F}_q,D)$ is an srg of negative Latin square type.*

There are many choices of $p$ and $j_i$, $i=1,2$, satisfying the condition of Proposition 4.9. For example, if $p\equiv 3\pmod 4$ and $j_1$ and $j_2$ are both odd, then $\bigcup_{i\in J_1}C_{-i+N_1/2}^{(N_1,q)}$ and $\bigcup_{i\in J_2}C_{-i+N_2/2}^{(N_2,q)}$ are disjoint.

### 4.3 A generalization of sporadic or subfield examples

In [46, 49, 51], the authors found infinite families of strongly regular Cayley graphs on finite fields generalizing seven of the eleven sporadic examples of cyclotomic srgs in Table 1. Their constructions used unions of "consecutive" cyclotomic classes of finite

fields as connection sets for the Cayley graph construction. In particular, the following theorem was proved.

**Theorem 4.10.** *(i)* ([49]) *Let* $q = p^{p_1^{m-1}(p_1-1)/2}$, $N = p_1^m$, *and* $D = \bigcup_{i=0}^{p_1^{m-1}-1} C_i^{(N,q)}$. *Then,* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is strongly for any* $m \geqslant 1$ *in the following cases:*

$$(p, p_1) = (2, 7), (3, 107), (5, 19), (5, 499), (17, 67), (41, 163).$$

*(ii)* ([51]) *Let* $q = p^{p_1^{m-1}(p_1-1)/4}$, $N = p_1^m$, *and* $D = \bigcup_{i=0}^{p_1^{m-1}-1} C_i^{(N,q)}$. *Then,* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is strongly regular for any* $m \geqslant 1$ *in the following cases:*

$$(p, p_1) = (3, 13), (7, 37).$$

*(iii)* ([46]) *Let* $q = p^{p_1^{m-1}(p_1-1)p_2^{n-1}(p_2-1)/2}$, $N = p_1^m p_2^n$, *and* $D = \bigcup_{i=0}^{p_1^{m-1}-1} \bigcup_{j=0}^{p_2^{n-1}-1} C^{(N,q)}_{p_2^n i + p_1^m j}$. *Then,* $\mathrm{Cay}(\mathbb{F}_q, D)$ *is strongly regular for any* $m, n \geqslant 1$ *in the following cases:*

$$(p, p_1, p_2) = (2, 3, 5), (3, 5, 7), (3, 17, 19).$$

The srgs in the cases when $(p, p_1) = (2, 7), (3, 13)$ and $(p, p_1, p_2) = (2, 3, 5)$ in Theorem 4.10 are generalizations of subfield examples. The others are generalizations of sporadic examples of Table 1. In all cases, it holds that $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = [(\mathbb{Z}/p_1\mathbb{Z})^* : \langle p \rangle]$ or $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = [(\mathbb{Z}/p_1p_2\mathbb{Z})^* : \langle p \rangle]$. The proofs are based on known evaluations of index 2 or 4 Gauss sums (see [44, 107]).

Note that it is unlikely that one can generalize the 1st example in Table 1 by a similar method since $[(\mathbb{Z}/11^m\mathbb{Z})^* : \langle 3 \rangle] \neq [(\mathbb{Z}/11\mathbb{Z})^* : \langle 3 \rangle]$ for $m \geqslant 2$. In order to generalize the 5th and 8th srgs in Table 1 into infinite families, we may need to evaluate Gauss sums of index 6. However, it seems very difficult to compute Gauss sums of index $e$ when $e > 4$. As a result, it is hard to find new srgs on $\mathbb{F}_q$ in the index $e > 4$ cases. On the other hand, in [74], the first author of this survey succeeded in giving a recursive construction of srgs, which enables him to generalize the remaining examples into infinite families not using explicit evaluations of Gauss sums. Instead, he studied the rationality of "relative" Gauss sums.

**Theorem 4.11.** ([74]) *Let* $N_1 = p_1 \cdots p_m p_{m+1} \cdots p_\ell$, *where* $p_i$*'s are distinct odd primes, and assume that* $[(\mathbb{Z}/h\mathbb{Z})^* : \langle p \rangle] = e$. *Furthermore, Let* $N = p_1^{e_1} \cdots p_m^{e_m} p_{m+1}^{e_{m+1}} \cdots p_\ell^{e_\ell}$, *where* $e_i \geqslant 1$ *for* $1 \leqslant i \leqslant m$ *and* $e_i = 1$ *for* $m+1 \leqslant i \leqslant \ell$, *and assume that* $\langle p \rangle$ *is of index* $e$ *modulo* $N$. *Let* $q_1 = p^d$ *and* $q = p^f$, *where* $d = \phi(N_1)/e$ *and* $f = \phi(N)/e$. *Here,* $\phi$ *is the Euler totient function. Put* $h_j = \prod_{i \neq j} p_i$ *for* $1 \leqslant j \leqslant m$. *Assume that there exists an integer* $s_j$ *such that* $p^{s_j} \equiv -1 \pmod{h_j}$ *for* $1 \leqslant j \leqslant m$. *Let*

$$D := \bigcup_{i_1=0}^{p_1^{e_1-1}-1} \cdots \bigcup_{i_m=0}^{p_m^{e_m-1}-1} C^{(N,q)}_{i_1 n_1 + \cdots + i_m n_m},$$

*where* $n_j = \prod_{i \neq j} p_i^{e_i}$. *If* $\mathrm{Cay}(\mathbb{F}_{q_1}, C_0^{(N_1,q_1)})$ *is an srg, then so is* $\mathrm{Cay}(\mathbb{F}_q, D)$.

**Example 4.12.** *(i) We can apply Theorem 4.11 to the 5th srg in Table 1 as* $(\ell, p_1, p, e) = (1, 43, 11, 6)$. *In this case, we do not need the condition that there exists an integer* $s_j$ *such that* $p^{s_j} \equiv -1 \pmod{h_j}$. *It is clear that* $[(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* : \langle p \rangle] = 6$ *for any* $e_1 \geqslant 1$. *Hence,* $\mathrm{Cay}(\mathbb{F}_{p^{p_1^{e_1-1}(p_1-1)/6}}, D)$ *is strongly regular, where*

$$D = \bigcup_{i=0}^{p_1^{e_1-1}-1} C_i^{(p_1^{e_1}, p^{p_1^{e_1-1}(p_1-1)/6})}.$$

*There are many examples in the subfield case satisfying the condition of Theorem 4.11 with* $\ell = 1$, *for example,*

$$(p, f, p_1, e) = (3, 3, 13, 4), (2, 5, 31, 6), (5, 3, 31, 10), (2, 9, 73, 8).$$

*In these cases, we have* $[(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^* : \langle p \rangle] = e$ *for any* $e_1 \geqslant 1$. *Hence, these examples can be similarly generalized into infinite families.*

*(ii) We can apply Theorem 4.11 to the 8th srg in Table 1 as* $(\ell, m, p_1, p_2, p, e) = (2, 1, 19, 7, 5, 6)$. *In this case, there exists an integer* $s_2$ *such that* $p^{s_2} \equiv -1 \pmod{p_2}$. *It is clear that* $[(\mathbb{Z}/p_1^{e_1}p_2\mathbb{Z})^* : \langle p \rangle] = 6$ *for any* $e_1 \geqslant 1$. *Hence,* $\mathrm{Cay}(\mathbb{F}_{p^{p_1^{e_1-1}(p_1-1)(p_2-1)/6}}, D)$ *is strongly regular, where*

$$D = \bigcup_{i=0}^{p_1^{e_1-1}-1} C_i^{(p_1^{e_1}p_2, p^{p_1^{e_1-1}(p_1-1)(p_2-1)/6})}.$$

*There are many examples in the subfield case satisfying the condition of Theorem 4.11 with* $\ell = 2$, *for example,*

$$(p, f, p_1, p_2, e) = (2, 4, 3, 5, 2), (2, 8, 5, 17, 8), (2, 10, 31, 11, 30), (2, 14, 127, 43, 378).$$

*In the former two cases, we have* $[(\mathbb{Z}/p_1^{e_1}p_2^{e_2}\mathbb{Z})^* : \langle p \rangle] = e$ *for any* $e_1, e_2 \geqslant 1$ *and* $p$ *is semi-primitive modulo both* $p_1$ *and* $p_2$. *In the latter two cases, we have* $[(\mathbb{Z}/p_1^{e_1}p_2\mathbb{Z})^* : \langle p \rangle] = e$ *for any* $e_1 \geqslant 1$, *and* $p$ *is semi-primitive modulo* $p_2$ *only. Hence, these examples can be generalized into infinite families by using Theorem 4.11.*

## 4.4 On de Lange's sporadic examples of srgs

In [35], de Lange found four "sporadic" examples of strongly regular Cayley graphs on the additive groups of finite fields by using a computer. The srgs he found have the following parameters:

(1) $(v, k, \lambda, \mu) = (3^8, 2296, 787, 812)$;

(2) $(v, k, \lambda, \mu) = (3^8, 2870, 1249, 1260)$;

(3) $(v,k,\lambda,\mu)=(2^{12},273,20,18)$;

(4) $(v,k,\lambda,\mu)=(2^{12},1911,950,840)$.

The 3rd and 4th examples of srgs are dual to each other; hence de Lange found essentially three examples. In particular, the 2nd example is the one given in Example 4.2 (3). As explained in Example 4.8 and Theorem 4.10 (iii), the 1st and 3rd examples above have already been generalized in [14] and [49], respectively. However, it seems difficult to generalize the 2nd example above into an infinite family of srgs. In [106], the third author asked the question of generalizing the last example of de Lange (see Problem 5.2 in [106]). In this subsection, we show that there is an infinite family of srgs including an srg with the same parameters as those of the 2nd example above.

We will need the following families of srgs.

**Theorem 4.13.** ([18]) *Let $Q:\mathbb{F}_q^n\to\mathbb{F}_q$ be a nonsingular quadratic form, where $n=2m$ is even and $q$ is an odd prime power. Define $\mathsf{Q}=\{x\in\mathbb{F}_q^n\setminus\{\mathbf{0}\}\,|\,Q(x)=0\}$ and $D_i=\{x\in\mathbb{F}_q^n\,|\,Q(x)\in C_i^{(2,q)}\}$, $i=0,1$. Then, each $\mathrm{Cay}(\mathbb{F}_q^n,D_i)$, $i=0,1$, is an srg with parameters $(u^2,r(u-\epsilon),\epsilon u+r^2-3\epsilon r,r^2-\epsilon r)$ with $u=q^m$ and $r=\epsilon q^{m-1}(q-1)/2$, where $\epsilon=1$ or $-1$ depending on whether $Q$ is hyperbolic or elliptic.*

The srg $\mathrm{Cay}(\mathbb{F}_q,D_0)$ in the above theorem is called an *affine polar graph*. In [75], the following recursive construction of srgs was given as a generalization of the construction above. Let $q$ be a prime power and $N>1$ be an integer dividing $q-1$. Furthermore, let $\gamma$ be a fixed primitive element of $\mathbb{F}_{q^2}$, and let $\omega=\mathrm{Norm}_{q^2/q}(\gamma)$, which is a primitive element of $\mathbb{F}_q$. Put $C_i^{(e,q^2)}=\gamma^i\langle\gamma^N\rangle$, $i=0,1,\ldots,N-1$. Let $Q:\mathbb{F}_q^n\to\mathbb{F}_q$ be a quadratic form. For $y\in\mathbb{F}_q$, define $D_y=\{x\in\mathbb{F}_q^n\,|\,Q(x)=y\}$, and for a subset $E$ of $\mathbb{F}_q$, write $D_E=\sum_{y\in E}D_y$.

**Theorem 4.14.** *Let $J$ be a subset of $\{0,1,\ldots,N-1\}$, and let $E=\bigcup_{i\in J}C_i^{(N,q)}$. Assume that $\mathrm{Cay}(\mathbb{F}_{q^2},\bigcup_{i\in J}C_i^{(N,q^2)})$ is an srg of negative Latin square type. Let $Q:\mathbb{F}_q^n\to\mathbb{F}_q$ be a nonsingular quadratic form, where $n=2m$ is even. Then, $\mathrm{Cay}(\mathbb{F}_q^n,D_E)$ is an srg$(u^2,r(u-\epsilon),\epsilon u+r^2-3\epsilon r,r^2-\epsilon r)$ with $u=q^m$ and $r=\epsilon|J|q^{m-1}(q-1)/N$, where $\epsilon=1$ or $-1$ depending on whether $Q$ is hyperbolic or elliptic.*

In [75, 76], the authors gave constructions of strongly regular graph $\mathrm{Cay}(\mathbb{F}_{q^2},D)$ of negative Latin square type such that $D$ is a union cosets of $C_0^{(q-1,q^2)}$ based on cyclotomic srgs, which can be used as starters in order to apply Theorem 4.14. Furthermore, in [47], the authors studied a construction of srgs based on weakly regular bent functions instead of quadratic forms in Theorem 4.14.

We will also need the following family of srgs.

**Example 4.15.** *Let $q$ be an odd prime power and $Q : \mathbb{F}_q^8 \to \mathbb{F}_q$ be an elliptic quadratic form defined by*

$$Q(x) = \mathrm{Tr}_{q^8/q}(x^{q^4+1}). \tag{4.1}$$

*We define $\mathsf{Q} = \{x \in \mathbb{F}_q^n \setminus \{\mathbf{0}\} \,|\, Q(x) = 0\}$. Let $D = C^{(q^2+1,q^8)}_{(q^2+1)/2}$. Then, $D \subseteq \mathsf{Q}$, and $\mathrm{Cay}(\mathbb{F}_{q^8}, D)$ is strongly regular with negative Latin square type parameters $(q^8, r(q^4+1), -q^4+r^2+3r, r^2+r)$, where $r = q^2-1$, since $q^2 \equiv -1 \pmod N$ with $N = q^2+1$ (i.e., the semi-primitive condition holds here). In this case, $\mathrm{Cay}(\mathbb{F}_{q^8}, \mathsf{Q}\setminus D)$ is also an srg of the same type.*

Finally, we use the following theorem of van Dam [100].

**Theorem 4.16.** *Let $\{G_1, G_2, \ldots, G_d\}$ be a decomposition of the complete graph on a vertex set $X$, where each $G_i$ is strongly regular. If the $G_i$'s are all of Latin square type or all of negative Latin square type, then a union of any subset of $\{G_1, G_2, \ldots, G_d\}$ is also an srg of the same type on $X$.*

**Remark 4.17.** In [100], van Dam actually proved that the decomposition $\{G_1, G_2, \ldots, G_d\}$ forms a $d$-class amorphic association scheme under the same assumption of Theorem 4.16. We will not need the full strength of this result. The theorem above suffices for our purpose.

**Example 4.18.** *Let $q$ be an odd prime power and $n = 8$. Let $Q : \mathbb{F}_q^n \to \mathbb{F}_q$ be a nonsingular elliptic quadratic form. Let $G_1 = \mathrm{Cay}(\mathbb{F}_q^n, D_1)$ be an affine polar graph of negative Latin square type associated with $Q$, and $G_2 = \mathrm{Cay}(\mathbb{F}_q^n, D_2)$ be the srg defined in (4.1). Then, the four graphs $G_1$, $G_2$, $G_3 = \mathrm{Cay}(\mathbb{F}_q^n, \mathbb{F}_q^n \setminus (\{\mathbf{0}\} \cup \mathsf{Q} \cup D_1))$, $G_4 = \mathrm{Cay}(\mathbb{F}_q^n, \mathsf{Q} \setminus D_2)$ give a decomposition of the complete graph on $\mathbb{F}_q^n$, where each $G_i$ is an srg of negative Latin square type. By Theorem 4.16, the graph $\Gamma = G_1 + G_3$ is also an srg of negative Latin square type. Take $q = 3$, and then the graph $\Gamma$ is an srg with parameters $(v, k, \lambda, \mu) = (3^8, 2870, 1249, 1260)$. This srg has the same parameters as those of de Lange's 2nd example $\Gamma'$ of srgs. We checked that $\Gamma$ and $\Gamma'$ are nonisomorphic by a computer. In particular, we have $\#\mathsf{Aut}(\Gamma) = 2^7 \cdot 3^{12} \cdot 5 \cdot 41$ and $\#\mathsf{Aut}(\Gamma') = 2^4 \cdot 3^8 \cdot 5 \cdot 41$.*

## 4.5 Projective two-intersection sets, $m$-ovoids, and $i$-tight sets

During the past few years, strongly regular Cayley graphs defined on the additive groups of finite fields have been extensively studied due to their close connections with certain substructures in finite geometry. In most published works by geometers, the authors used the language of projective two-intersection sets, or two-character sets. Because of the large amount of papers published in this direction, it is difficult to summarize all known constructions and existence results in this short subsection. Instead we will focus on explaining the connections between projective two-intersection sets

and strongly regular Cayley graphs on finite fields, and a linkage with geometric objects, called $m$-ovoids and $i$-tight sets in polar spaces.

A set $\mathcal{M}$ of points of a projective space $\mathsf{PG}(n-1,q)$ is called a *projective two-intersection set of type* $(a,b)$ (or simply, a *set of type* $(a,b)$) if every hyperplane of $\mathsf{PG}(n-1,q)$ meets $\mathcal{M}$ in $a$ or $b$ points. In some papers, a projective two-intersection set is also called a *two-character set*.

**Example 4.19.**

*(1) A hyperoval in* $\mathsf{PG}(2,2^f)$ *is a set of type* $(0,2)$.

*(2) A unital in* $\mathsf{PG}(2,q^2)$ *is a set of type* $(1,q+1)$.

*(3) A nodegenerate quadric* $\mathsf{Q}$ *in* $\mathsf{PG}(2m-1,q)$ *is a set of type* $(\theta_m - q^{2m-2}, \theta_m - q^{2m-2} - \epsilon q^{m-1})$, *where* $\theta_m = \frac{(q^m-\epsilon)(q^{m-1}+\epsilon)}{q-1}$ *and* $\epsilon = 1$ *or* $-1$ *depending on whether* $\mathsf{Q}$ *is hyperbolic or elliptic.*

See [37] for a generalization of (1) in Example 4.19 and [13] for a difference of two quadrics construction.

Let $N = (q^n-1)/(q-1)$, and let $\gamma$ be a primitive element of $\mathbb{F}_{q^n}$. We identify the points of $\mathsf{PG}(n-1,q)$ with $\mathbb{Z}_N$ as follows: View $\mathbb{F}_{q^n}$ as an $n$-dimensional space over $\mathbb{F}_q$, and use $\mathbb{F}_{q^n}$ as the underlying vector space of $\mathsf{PG}(n-1,q)$. We identify the projective point $\langle \gamma^i \rangle$ with $i \in \mathbb{Z}_N$. Then, all hyperplanes in $\mathsf{PG}(n-1,q)$ are given by

$$H_i := \{\langle \gamma^j \rangle \mid \mathrm{Tr}_{q^n/q}(\gamma^{i+j}) = 0, j \in \mathbb{Z}_N\}, \ i \in \mathbb{Z}_N.$$

Now let $\mathcal{M}$ be a set of points of $\mathsf{PG}(n-1,q)$, and define

$$D := \{xy : y \in \mathbb{F}_q^*, \langle x \rangle \in \mathcal{M}\} \subseteq \mathbb{F}_{q^n}.$$

Then, we have

$$\psi_{\mathbb{F}_{q^n}}(\gamma^i D) = \sum_{y \in \mathbb{F}_q} \sum_{x \in \mathcal{M}} \zeta_p^{\mathrm{Tr}_{q^n/q}(\gamma^i xy)} - |\mathcal{M}| = q|H_i \cap \mathcal{M}| - |\mathcal{M}|.$$

Hence, $\mathcal{M}$ is a set of type $(a,b)$ in $\mathsf{PG}(n-1,q)$ if and only if the character values of $D$ take exactly two values $qa - |\mathcal{M}|$ and $qb - |\mathcal{M}|$, i.e., $\mathrm{Cay}(\mathbb{F}_{q^n}, D)$ is strongly regular with parameters $(q^n, (q-1)|\mathcal{M}|, \lambda, \mu)$, where $\lambda$ and $\mu$ can be computed from $a$, $b$, $|\mathcal{M}|$, $q$, and $n$.

There are many known constructions of projective two-intersection sets. See, e.g., [23, 24, 25, 27, 30, 36, 33, 60, 80, 79, 84, 85], for recent constructions of projective two-intersection sets.

Many projective two-intersection sets arise from $m$-ovoids and $i$-tight sets in classical polar spaces. Conversely, projective two-intersection sets with certain special properties can give rise to $m$-ovoids and $i$-tight sets. Many recent constructions of $m$-ovoids and $i$-tight sets came about via constructions of projective 2-intersection sets satisfying special properties, see, e.g. [45, 7].

Let $V = \mathbb{F}_q^n$ be an $n$-dimensional vector space over $\mathbb{F}_q$ and $f$ be a non-degenerate sesquilinear or non-singular quadratic form defined on $V$. A finite classical polar space associated with the form $f$ is the geometry consisting of subspaces of $\mathsf{PG}(n-1,q)$ induced by the totally isotropic subspaces with relation to $f$. A polar space $S$ contains totally isotropic points, lines, planes, etc. The (totally isotropic) subspaces of maximum dimension are called *maximals* of $S$. The *rank* of $S$ is the vector dimension of its maximals.

There are three types of finite classical polar spaces; Orthogonal polar spaces (parabolic quadric $\mathsf{Q}(2r,q)$, hyperbolic quadric $\mathsf{Q}^+(2r-1,q)$, elliptic quadric $\mathsf{Q}^-(2r-1,q)$); symplectic polar spaces ($\mathsf{W}(2r-1,q)$); and Hermitian polar spaces ($\mathsf{H}(2r,q^2)$, $\mathsf{H}(2r-1,q^2)$). See Table 2 for polar spaces and their ranks and forms $f$. (In Table 2, $f(x_0,x_1) = ax_0^2 + bx_0x_1 + cx_1^2$ is an irreducible quadratic form in two indeterminates.)

Table 2. Classical polar spaces

| Polar space | dimension | rank | form |
|---|---|---|---|
| $\mathsf{Q}(2r,q)$ | $n=2r+1$ | $r$ | $x_0^2 + x_1x_2 + \cdots + x_{2r-1}x_{2r}$ |
| $\mathsf{Q}^+(2r-1,q)$ | $n=2r$ | $r$ | $x_0x_1 + \cdots + x_{2r-2}x_{2r-1}$ |
| $\mathsf{Q}^-(2r-1,q)$ | $n=2r$ | $r-1$ | $f(x_0,x_1) + x_2x_3 + \cdots + x_{2r-2}x_{2r-1}$ |
| $\mathsf{W}(2r-1,q)$ | $n=2r$ | $r$ | $x_0y_1 + y_0x_1 + \cdots + x_{2r-2}y_{2r-1} + x_{2r-1}y_{2r-2}$ |
| $\mathsf{H}(2r,q^2)$ | $n=2r+1$ | $r$ | $x_0^{q+1} + \cdots + x_{2r}^{q+1}$ |
| $\mathsf{H}(2r-1,q^2)$ | $n=2r$ | $r$ | $x_0^{q+1} + \cdots + x_{2r-1}^{q+1}$ |

Let $S$ be a polar space of rank $r$ over $\mathbb{F}_q$. An *$m$-ovoid* is a set $\mathcal{M}$ of points of $S$ such that every maximal of $S$ meets $\mathcal{M}$ in exactly $m$ points. For example, the whole point set of $S$ itself is a $\frac{q^r-1}{q-1}$-ovoid. For two $m_j$-ovoids $\mathcal{M}_j$, $j=1,2$, if $\mathcal{M}_2 \subseteq \mathcal{M}_1$, then $\mathcal{M}_1 \setminus \mathcal{M}_2$ is an $(m_1-m_2)$-ovoid. On the other hand, if $\mathcal{M}_1$ and $\mathcal{M}_2$ are disjoint, then $\mathcal{M}_1 \cup \mathcal{M}_2$ is an $(m_1+m_2)$-ovoid.

For a point $P$ of a polar space $S$, the set $P^\perp$ of points of $S$ collinear with $P$ is the intersection of the tangent hyperplane at $P$ with $S$. Let $\mathcal{M}$ be an $m$-ovoid of $S$. It is known that $|P^\perp \cap \mathcal{M}|$ takes exactly two values according to $P \in \mathcal{M}$ or not [5]. Furthermore, if $S$ is either $\mathsf{H}(2r,q^2)$, $\mathsf{Q}^-(2r-1,q)$, or $\mathsf{W}(2r-1,q)$, the sizes of $H \cap \mathcal{M}$, where $H$ are nontangent hyperplanes, can also be computed exactly. In fact, the following theorem is known.

**Theorem 4.20.** ([5, Theorem 11]) *Let $S$ be one of the polar spaces $\mathsf{H}(2r,q^2)$, $\mathsf{Q}^-(2r-1,q)$, or $\mathsf{W}(2r-1,q)$ and let $\mathcal{M}$ be an $m$-ovoid in $S$. Then $\mathcal{M}$ is a projective two-intersection set in the ambient projective space of $S$; in other words, letting $D = \{xy : y \in \mathbb{F}_q^*, \langle x\rangle \in \mathcal{M}\}$ and $V$ be the underlying vector space of $S$, the graph* $\mathrm{Cay}(V,D)$ *is*

*an srg with negative Latin square type parameters* $(u^2, s(u+1), -u+s^2+3s, s^2+s)$, *where* $(u,s) = (q^{2r+1}, m(q^2-1))$, $(q^r, m(q-1))$, *or* $(q^r, m(q-1))$ *according as* $S = \mathsf{H}(2r,q^2)$, $\mathsf{Q}^-(2r-1,q)$, *or* $\mathsf{W}(2r-1,q)$, *respectively.*

**Remark 4.21.**

*(1) A partial converse to the above theorem holds. That is, if* $\mathcal{M}$ *is a projective two-intersection set in the ambient projective space of* $S$, *and* $\mathcal{M}$ *satisfies certain conditions, then* $\mathcal{M}$ *is an* $m$*-ovoid in* $S$. *We refer the reader to [7] for the precise statement of the partial converse. This partial converse provides an approach to constructing* $m$*-ovoids in the polar spaces mentioned in Theorem 4.20.*

*(2) A* $(q+1)/2$*-ovoid in* $\mathsf{Q}^-(5,q)$ *can be interpreted as a set of lines in* $\mathsf{H}(3,q^2)$ *containing exactly half of the lines on every point via the duality of generalized quadrangles. Such a set of lines in* $\mathsf{H}(3,q^2)$ *is called a hemisystem, which was first studied by Segre [91]. Constructions of hemisystems can be found in [4, 7, 29, 63].*

To obtain a similar theorem for srgs of Latin square type, we need to introduce the concept of $i$-tight sets. Let $S$ be a polar space of rank $r \geqslant 2$ over $\mathbb{F}_q$. An *$i$-tight set* is a set $\mathcal{M}$ of points of $S$ such that

$$|P^\perp \cap \mathcal{M}| = \begin{cases} i\frac{q^{r-1}-1}{q-1} + q^{r-1}, & \text{if } P \in \mathcal{M}, \\ i\frac{q^{r-1}-1}{q-1}, & \text{otherwise.} \end{cases}$$

For example, each maximal is a 1-tight set. In [5], it was shown that if a set $\mathcal{M}$ of points in a polar space $S$ meets $P^\perp$ in exactly two different sizes according to $P \in \mathcal{M}$ or not, then $\mathcal{M}$ is either an $m$-ovoid or an $i$-tight set for some $m$ or $i$. Similarly to the situation with $m$-ovoids, the following basic properties hold. For two $i_j$-tight sets $\mathcal{M}_j$ in $S$, $j = 1,2$, if $\mathcal{M}_2 \subseteq \mathcal{M}_1$, then $\mathcal{M}_1 \setminus \mathcal{M}_2$ is an $(i_1 - i_2)$-tight set. On the other hand, if $\mathcal{M}_1$ and $\mathcal{M}_2$ are disjoint, then $\mathcal{M}_1 \cup \mathcal{M}_2$ is an $(i_1+i_2)$-tight set. Furthermore, if $S$ is either $\mathsf{H}(2r-1,q^2)$, $\mathsf{Q}^+(2r-1,q)$, or $\mathsf{W}(2r-1,q)$, the size of $H \cap \mathcal{M}$ for nontangent hyperplanes can be also computed exactly. In fact, the following theorem is known.

**Theorem 4.22.** ([5, Theorem 12]) *Let* $S$ *be one of the polar spaces* $\mathsf{H}(2r-1,q^2)$, $\mathsf{Q}^+(2r-1,q)$, *or* $\mathsf{W}(2r-1,q)$ *and let* $\mathcal{M}$ *be an* $i$*-tight set in* $S$. *Then* $\mathcal{M}$ *is a projective two-intersection set in the ambient projective space of* $S$; *In other words, letting* $D := \{xy : y \in \mathbb{F}_q^*, \langle x \rangle \in \mathcal{M}\}$ *and* $V$ *be the underlying vector space of* $S$, *the graph* $\mathrm{Cay}(V,D)$ *is an srg with Latin square type parameters* $(u^2, s(u-1), u+s^2-3s, s^2-s)$, *where* $(u,s) = (q^{2r}, i)$, $(q^r, i)$, *or* $(q^r, i)$ *according as* $S = \mathsf{H}(2r-1,q^2)$, $\mathsf{Q}^+(2r-1,q)$, *or* $\mathsf{W}(2r-1,q)$, *respectively.*

**Remark 4.23.**

*(1) Again, a partial converse to the above theorem holds. For the detailed statement, see [45]. This partial converse provides an approach to constructing Cameron-Liebler lines classes in* $\mathsf{PG}(3,q)$ *(see definition below).*

*(2) A tight set in* $\mathsf{Q}^+(5,q)$ *can be interpreted as a set* $\mathcal{L}$ *of lines in* $\mathsf{PG}(3,q)$ *such that the size of* $\mathcal{L}\cap S$ *is constant for all spread* $S$ *via the Klein correspondence. Such a set of lines in* $\mathsf{PG}(3,q)$ *is called a Cameron-Liebler line class, which was first studied by Cameron and Liebler [19]. Constructions of Cameron-Liebler line classes can be found in [16, 32, 45, 50, 88].*

Known results on $m$-ovoids and $i$-tight sets are surveyed in [5, 6]. See [22, 26, 28, 34, 78, 71] for recent constructions of $m$-ovoids and $i$-tight sets.

## Bibliography

[1] K. T. Arasu, *Sequences and arrays with desirable correlation properties*, Information security, coding theory and related combinatorics, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. 29, IOS, Amsterdam, 2011, pp. 136–171.

[2] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar and H. M. Martinsen, Almost difference sets and their sequences with optimal autocorrelation, *IEEE Trans. Inform. Theory* 47 (2001), 2934–2943.

[3] L. Babai, A. Gál and A. Wigderson, Superpolynomial lower bounds for monotone span programs, *Combinatorica* 19 (1999), 301–319.

[4] J. Bamberg, M. Giudici and G. F. Royle, Every flock generalized quadrangle has a hemisystem, *Bull. Lond. Math. Soc.* 42 (2010), 795–810.

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

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

[7] J. Bamberg, M. Lee, K. Momihara and Q. Xiang, A new infinite family of Hemisystems of the Hermitian surface, *Combinatorica* 38 (2018), 43–66.

[8] L. M. Batten and J. M. Dover, Some sets of type $(m,n)$ in cubic order planes, *Des. Codes Cryptogr.* 16 (1999), 211–213.

[9] L. D. Baumert, W. H. Mills and Robert L. Ward, Uniform cyclotomy, *J. Number Theory* 14 (1982), 67–82.

[10] L. D. Baumert, *Cyclic difference sets*, Lecture Notes in Mathematics, Vol. 182, Springer-Verlag, Berlin, 1971.

[11] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998.

[12] T. Beth, D. Jungnickel and H. Lenz, *Design theory. Vol. II*, second ed, Encyclopedia of Mathematics and its Applications 78, Cambridge University Press, Cambridge, 1999.

[13] A. E. Brouwer, Some new two-weight codes and strongly regular graphs, *Discrete Appl. Math.* 10 (1985), 111–114.

[14] A. E. Brouwer, R. M. Wilson and Q. Xiang, Cyclotomy and strongly regular graphs, *J. Algebraic Combin.* 10 (1999), 25–28.

[15] A. E. Brouwer and W. H. Haemers, *Spectra of graphs*, Universitext, Springer, New York, 2012.

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

[17] Y. Cai and C. Ding, Binary sequences with optimal autocorrelation, *Theoret. Comput. Sci.* 410 (2009), 2316–2322.

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

[19] P. J. Cameron and R. A. Liebler, Tactical decompositions and orbits of projective groups, *Linear Algebra Appl.* 46 (1982), 91–102.

[20] S. Chowla, A property of biquadratic residues, *Proc. Nat. Acad. Sci. India. Sect. A.* 14 (1944), 45–46.

[21] F. R. K. Chung, R. L. Graham and R. M. Wilson, Quasi-random graphs, *Combinatorica* 9 (1989), 345–362.

[22] A. Cossidente, C. Culbert, G. L. Ebert and G. Marino, On $m$-ovoids of $W_3(q)$, *Finite Fields Appl.* 14 (2008), 76–84.

[23] A. Cossidente, The classical 1-system of $Q^-(7, q)$ and two-character sets, *Des. Codes Cryptogr.* 54 (2010), 1–9.

[24] A. Cossidente, N. Durante, G. Marino, T. Penttila and A. Siciliano, The geometry of some two-character sets, *Des. Codes Cryptogr.* 46 (2008), 231–241.

[25] A. Cossidente and O. H. King, Some two-character sets, *Des. Codes Cryptogr.* 56 (2010), 105–113.

[26] A. Cossidente and F. Pavese, Intriguing sets of $W(5, q)$, $q$ even, *J. Combin. Theory Ser. A* 127 (2014), 303–313.

[27] ———, Sets of even type on $H(5, q^2)$, $q$ even, *Discrete Appl. Math.* 181 (2015), 280–282.

[28] ———, Intriguing sets of quadrics in PG$(5, q)$, *Adv. Geom.* 17 (2017), 339–345.

[29] A. Cossidente and T. Penttila, Hemisystems on the Hermitian surface, *J. London Math. Soc. (2)* 72 (2005), 731–741.

[30] ———, Two-character sets arising from gluings of orbits, *Graphs Combin.* 29 (2013), 399–406.

[31] T. W. Cusick, C. Ding and A. Renvall, *Stream ciphers and number theory*, revised ed, North-Holland Mathematical Library 66, Elsevier Science B.V., Amsterdam, 2004.

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

[33] B. De Bruyn, Two-character sets as subsets of parabolic quadrics, *Ars Combin.* 127 (2016), 125–132.

[34] ———, On some 2-tight sets of polar spaces, *Ars Combin.* 133 (2017), 115–131.

[35] C. L. M. de Lange, Some new cyclotomic strongly regular graphs, *J. Algebraic Combin.* 4 (1995), 329–330.

[36] A. De Wispelaere and H. Van Maldeghem, Some new two-character sets in $\mathrm{PG}(5, q^2)$ and a distance-2 ovoid in the generalized hexagon $\mathrm{H}(4)$, *Discrete Math.* 308 (2008), 2976–2983.

[37] R. H. F. Denniston, Some maximal arcs in finite projective planes, *J. Combinatorial Theory* 6 (1969), 317–319.

[38] C. Ding, Pattern distributions of Legendre sequences, *IEEE Trans. Inform. Theory* 44 (1998), 1693–1698.

[39] C. Ding, T. Helleseth and K. Y. Lam, Several classes of binary sequences with three-level autocorrelation, *IEEE Trans. Inform. Theory* 45 (1999), 2606–2612.

[40] C. Ding, T. Helleseth and H. Martinsen, New families of binary sequences with optimal three-level autocorrelation, *IEEE Trans. Inform. Theory* 47 (2001), 428–433.

[41] R. Evans and M. Van Veen, Nonexistence of twenty-fourth power residue addition sets, *Finite Fields Appl.* 46 (2017), 139–146.

[42] R. Evans, Nonexistence of twentieth power residue difference sets, *Acta Arith.* 89 (1999), 397–402.

[43] W. Feit, Finite projective planes and a question about primes, *Proc. Amer. Math. Soc.* 108 (1990), 561–564.

[44] K. Q. Feng, J. Yang and S. X. Luo, Gauss sum of index 4. I. Cyclic case, *Acta Math. Sin. (Engl. Ser.)* 21 (2005), 1425–1434.

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

[46] ———, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, *Combinatorica* 35 (2015), 413–434.

[47] T. Feng, B. Wen, Q. Xiang and J. Yin, *Partial difference sets from quadratic forms and p-ary weakly regular bent functions*, Number theory and related areas, Adv. Lect. Math. (ALM) 27, Int. Press, Somerville, MA, 2013, pp. 25–40.

[48] T. Feng and Q. Xiang, Cyclotomic constructions of skew Hadamard difference sets, *J. Combin. Theory Ser. A* 119 (2012), 245–256.

[49] ———, Strongly regular graphs from unions of cyclotomic classes, *J. Combin. Theory Ser. B* 102 (2012), 982–995.

[50] A. L. Gavrilyuk, I. Matkin and T. Penttila, Derivation of Cameron-Liebler line classes, *Des. Codes Cryptogr.* 86 (2018), 231–236.

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

[52] S. W. Golomb, *Shift register sequences*, Aegean Park Press, 1982.

[53] S. W. Golomb and G. Gong, *Signal design for good correlation*, Cambridge University Press, Cambridge, 2005, For wireless communication, cryptography, and radar.

[54] M. Hall, Jr., A survey of difference sets, *Proc. Amer. Math. Soc.* 7 (1956), 975–986.

[55] ———, *Combinatorial theory*, second ed, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons, Inc., New York, 1986, A Wiley-Interscience Publication.

[56] H. S. Hayashi, Computer investigation of difference sets, *Math. Comp.* 19 (1965), 73–78.

[57] T. Helleseth and P. V. Kumar, *Sequences with low correlation*, Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1765–1853.

[58] D. G. Higman and J. E. McLaughlin, Geometric $ABA$-groups, *Illinois J. Math.* 5 (1961), 382–397.

[59] R. Hill, Caps and groups, (1976), 389–394. Atti dei Convegni Lincei, No. 17.

[60] S. Innamorati, M. Zannetti and F. Zuanni, On two character $(q^7 + q^5 + q^2 + 1)$-sets in $\mathrm{PG}(4, q^2)$, *J. Geom.* 106 (2015), 287–296.

[61] D. Jungnickel and A. Pott, Perfect and almost perfect sequences, *Discrete Appl. Math.* 95 (1999), 331–359.

[62] W. M. Kantor, Primitive permutation groups of odd degree, and an application to finite projective planes, *J. Algebra* 106 (1987), 15–45.

[63] G. Korchmáros, G. P. Nagy and P. Speziali, Hemisystems of the Hermitian Surface, *arXiv preprint arXiv:1710.06335* (2017).

[64] S. M. Krone and D. V. Sarwate, Quadriphase sequences for spread-spectrum multiple-access communication, *IEEE Trans. Inform. Theory* 30 (1984), 520–529.

[65] E. S. Lander, *Symmetric designs: an algebraic approach*, London Mathematical Society Lecture Note Series 74, Cambridge University Press, Cambridge, 1983.

[66] P. Langevin, *A new class of two weight codes*, Finite fields and applications (Glasgow, 1995), London Math. Soc. Lecture Note Ser. 233, Cambridge Univ. Press, Cambridge, 1996, pp. 181–187.

[67] E. Lehmer, On residue difference sets, *Canadian J. Math.* 5 (1953), 425–432.

[68] A. Lempel, M. Cohn and W. L. Eastman, A class of balanced binary sequences with optimal autocorrelation properties, *IEEE Trans. Information Theory* IT-23 (1977), 38–42.

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

[70] R. J. McEliece, Irreducible cyclic codes and Gauss sums, (1974), 179–196. Math. Centre Tracts, No. 55.

[71] K. Metsch, Small tight sets in finite elliptic, parabolic and Hermitian polar spaces, *Combinatorica* 36 (2016), 725–744.

[72] J. Michel and Q. Wang, Some new balanced and almost balanced quaternary sequences with low autocorrelation, *Cryptogr. Commun.* (2018).

[73] K. Momihara, Inequivalence of skew Hadamard difference sets and triple intersection numbers modulo a prime, *Electron. J. Combin.* 20 (2013), Paper 35, 19.

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

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

[76] ———, Strongly regular Cayley graphs from partitions of subdifference sets of the Singer difference sets, *Finite Fields Appl.* 50 (2018), 222–250.

[77] J. B. Muskat and A. L. Whiteman, The cyclotomic numbers of order twenty, *Acta Arith.* 17 (1970), 185–216.

[78] A. Nakić and L. Storme, Tight sets in finite classical polar spaces, *Adv. Geom.* 17 (2017), 109–129.

[79] V. Napolitano, On sets of type $(q+1,n)_2$ in finite three-dimensional projective spaces, *J. Geom.* 104 (2013), 557–562.

[80] ———, On sets of type $(m,h)_2$ in P$G(3,q)$ with $m \leq q$, *Note Mat.* 35 (2015), 109–123.

[81] P. Ó Catháin, Inequivalence of difference sets: on a remark of Baumert, *Electron. J. Combin.* 20 (2013), Paper 38, 19.

[82] U. Ott, Sharply flag-transitive projective planes and power residue difference sets, *J. Algebra* 276 (2004), 663–673.

[83] R. E. A. C. Paley, On orthogonal matrices, *Studies in Applied Mathematics* 12 (1933), 311–320.

[84] F. Pavese, Geometric constructions of two-character sets, *Discrete Math.* 338 (2015), 202–208.

[85] T. Penttila and G. F. Royle, Sets of type $(m,n)$ in the affine and projective planes of order nine, *Des. Codes Cryptogr.* 6 (1995), 229–245.

[86] A. Pott and Q. Wang, Difference balanced functions and their generalized difference sets, *J. Combin. Theory Ser. A* 131 (2015), 61–70.

[87] ———, *Some results on difference balanced functions*, Arithmetic of finite fields, Lecture Notes in Comput. Sci. 9061, Springer, Cham, 2015, pp. 111–120.

[88] M. J. Rodgers, *On some new examples of Cameron-Liebler line classes*, Ph.D. Thesis, University of Colorado at Denver, 2012.

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

[90] K.-U. Schmidt, Sequences with small correlation, *Des. Codes Cryptogr.* 78 (2016), 237–267.

[91] B. Segre, Forme e geometrie hermitiane, con particolare riguardo al caso finito, *Ann. Mat. Pura Appl. (4)* 70 (1965), 1–201.

[92] V. M. Sidelnikov, Some $k$-valued pseudo-random sequences and nearly equidistant codes, *Problemy Peredači Informacii* 5 (1969), 16–22.

[93] R. G. Stanton and D. A. Sprott, A family of difference sets, *Canad. J. Math.* 10 (1958), 73–77.

[94] T. Storer, *Cyclotomy and difference sets*, Lectures in Advanced Mathematics, No. 2, Markham Publishing Co., Chicago, Ill., 1967.

[95] P. Sziklai, A lemma on the randomness of $d$-th powers in GF$(q)$, $d \mid q-1$, *Bull. Belg. Math. Soc. Simon Stevin* 8 (2001), 95–98.

[96] T. Szönyi, Note on the existence of large minimal blocking sets in Galois planes, *Combinatorica* 12 (1992), 227–235.

[97] K. Thas and D. Zagier, Finite projective planes, Fermat curves, and Gaussian periods, *J. Eur. Math. Soc. (JEMS)* 10 (2008), 173–190.

[98] A. Thomason, *Pseudorandom graphs*, Random graphs '85 (Poznań, 1985), North-Holland Math. Stud. 144, North-Holland, Amsterdam, 1987, pp. 307–331.

[99] R. Turyn, *Sequences with small correlation*, Error Correcting Codes (Proc. Sympos. Math. Res. Center, Madison, Wis., 1968), John Wiley, New York, 1968, pp. 195–228.

[100] E. R. van Dam, Strongly regular decompositions of the complete graph, *J. Algebraic Combin.* 17 (2003), 181–201.

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

[102] G. Weng, W. Qiu, Z. Wang and Q. Xiang, Pseudo-Paley graphs and skew Hadamard difference sets from presemifields, *Des. Codes Cryptogr.* 44 (2007), 49–62.

[103] A. Winterhof, On the distribution of powers in finite fields, *Finite Fields Appl.* 4 (1998), 43–54.

[104] B. Xia, Cyclotomic difference sets in finite fields, *Mathematics of Computation*, **87** (2018), 2461–2482.

[105] Q. Xiang, *Recent results on difference sets with classical parameters*, Difference sets, sequences and their correlation properties (Bad Windsheim, 1998), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. 542, Kluwer Acad. Publ., Dordrecht, 1999, pp. 419–437.

[106] ———, *Cyclotomy, Gauss sums, difference sets and strongly regular Cayley graphs*, Sequences and their applications—SETA 2012, Lecture Notes in Comput. Sci. 7280, Springer, Heidelberg, 2012, pp. 245–256.

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

[108] P. Yuan and Y. Hu, A note on power residue difference sets, *J. Algebra* 291 (2005), 269–273.

## Author information

Koji Momihara, Division of Natural Science, Faculty of Advanced Science and Technology, Kumamoto University, 2-40-1 Kurokami, Kumamoto 860-8555, Japan.
E-mail: momihara@educ.kumamoto-u.ac.jp

Qi Wang, Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen, Guangdong 518055, China.
E-mail: wangqi@sustc.edu.cn

Qing Xiang, Department of Mathematical Sciences, University of Delaware, Newark DE 19716, USA.
E-mail: qxiang@udel.edu