Designs, Codes and Cryptography, 4, 221-261 (1994)
© 1994 Kluwer Academic Publishers. Manufactured in The Netherlands.

A Survey of Partial Difference Sets

S.L. MA
Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 0511, Republic of Singapore

Communicated by D. Jungnickel
Received March 20, 1993; Revised October 5, 1993.

Abstract. Let G be a finite group of order v. A k-element subset D of G is called a (v, k, λ, μ)-partial difference set if the expressions gh^{-1}, for g and h in D with $g \neq h$, represent each nonidentity element in D exactly λ times and each nonidentity element not in D exactly μ times. If $e \notin D$ and $g \in D$ iff $g^{-1} \in D$, then D is essentially the same as a strongly regular Cayley graph. In this survey, we try to list all important existence and nonexistence results concerning partial difference sets. In particular, various construction methods are studied, e.g., constructions using partial congruence partitions, quadratic forms, cyclotomic classes and finite local rings. Also, the relations with Schur rings, two-weight codes, projective sets, difference sets, divisible difference sets and partial geometries are discussed in detail.

1. Strongly Regular Graphs and Partial Difference Sets

A graph Γ with v vertices is said to be a (v, k, λ, μ)-*strongly regular graph* if

(i) it is regular of valency k, i.e., each vertex is joined to exactly k other vertices;
(ii) any two adjacent vertices are both joined to exactly λ other vertices and two nonadjacent vertices are both joined to exactly μ other vertices.

The structure of strongly regular graphs was first studied by Bose [1] in connection with partial geometries and symmetric association schemes of class two. The general theory and constructions of strongly regular graphs can be found in Hubaut [2], Cameron [3], Seidel [4], Brouwer and van Lint [5] and Cameron and van Lint [6].

A *Cayley graph* is defined as a graph $\Gamma = (V, E)$ which admits an automorphism group G acting regularly on the vertex set V (see Yap [7] for background on Cayley graphs). If we identify the vertices of Γ with the elements of the regular automorphism group G, then Γ can be generated by a subset D of G such that two vertices $g, h \in G$ are joined if and only if $gh^{-1} \in D$. Note that $e \notin D$ since Γ has no loops, and $g^{-1} \in D$ iff $g \in D$ since Γ is not directed.

Let G be a group of order v and D be a subset of G with k elements. Then D is called a (v, k, λ, μ)-*partial difference set* (PDS) in G if the expressions gh^{-1}, for g and h in D with $g \neq h$, represent each nonidentity element in D exactly λ times and represent each nonidentity element not in D exactly μ times. Furthermore, the PDS is called *abelian* (resp. *nonabelian*) if the group G is abelian (resp. nonabelian).

For a subset S of a group G, let $S^{(t)} = \{g^t : g \in S\}$ for any integer t.

PROPOSITION 1.1. A Cayley graph Γ, generated by a subset D of the regular automorphism group G, is a strongly regular graph if and only if D is a PDS in G with $e \notin D$ and $D^{(-1)} = D$. ■

PDSs were named by Chakravarti [8] but they were introduced by Bose and Cameron [9] in their studies of calibration designs and the bridge tournament problem. Although a systematic study of PDSs was started by Ma [10], [11] as a generalization of difference sets, there were a lot of earlier results written in terms of strongly regular graphs or related topics, e.g., Delsarte [12]–[14], Camion [15], Bridges and Mena [16]–[17] and Calderbank and Kantor [18]. (Readers are warned that the parameters defined in some of the references are different from the definitions in this paper.)

In view of Proposition 1.1, it is natural for us to concentrate on the case when $e \notin D$ and $D^{(-1)} = D$. In the following, such a PDS will be called *regular.* For a PDS D with $D^{(-1)} = D$, we can count the expressions gh instead of the expressions gh^{-1}. Hence, regular PDSs are also called *partial addition sets*, e.g., see Ghinelli and Löwe [19].

Note that the regular condition of PDSs is not restrictive. If D is a PDS with $e \in D$ and $D^{(-1)} = D$, then $D\backslash\{e\}$ is also a PDS. The following proposition shows that $D^{(-1)} = D$ is quite common for PDSs.

PROPOSITION 1.2. (Ma [10]) If D is a (v, k, λ, μ)-PDS with $\lambda \neq \mu$, then $D^{(-1)} = D$. ■

A PDS with $\lambda = \mu$ is just an ordinary difference set and there are a lot of good surveys on this topic, e.g., see Beth, Jungnickel and Lenz [20], Lander [21] and Jungnickel [22].

Usually, the study of PDSs is carried out using the group ring $R[G]$ where $R = \mathbb{Z}$ or $\mathbb{C}$. First, we have the following notation: for $S \subset G$, let $\bar{S} = \Sigma_{g \in S}\, g \in R[G]$; and for $t \in \mathbb{Z}$ and $y = \Sigma_{g \in G} a_g g \in R[G]$ where $a_g \in R$, let $y^{(t)} = \Sigma_{g \in G} a_g g^t$.

THEOREM 1.3. *Let G be a group of order v and D be a subset of G with k elements. Then D is a (v, k, λ, μ)-PDS in G if and only if*

$$\bar{D}\,\bar{D}^{(-1)} = \mu\bar{G} + (\lambda - \mu)\bar{D} + \gamma e \tag{1.1}$$

where $\gamma = k - \mu$ if $e \notin D$ and $\gamma = k - \lambda$ if $e \in D$. Furthermore, if $D^{(-1)} = D$, then

$$\bar{D}^2 = \mu\bar{G} + (\lambda - \mu)\bar{D} + \gamma e. \tag{1.2}$$

■

The following is another useful form of (1.2):

$$(2\bar{D} - \beta e)^2 = 4\mu\bar{G} + \Delta e \tag{1.3}$$

where $\beta = \lambda - \mu$ and $\Delta = \beta^2 + 4\gamma$. Note that the parameters β and Δ are very important in the study of PDSs. As a consequence of (1.2) and (1.3), we have some restrictions on the parameters.

PROPOSITION 1.4. The parameters of a regular (v, k, λ, μ)-PDS satisfy

(a) $(v + \beta)^2 - (\Delta - \beta^2)(v - 1)$ must be a square;
(b) $k = [(v + \beta) \pm \sqrt{(v + \beta)^2 - (\Delta - \beta^2)(v - 1)}]/2$;
(c) β and Δ have the same parity; and
(d) if $D \neq \emptyset$ and $G\backslash\{e\}$, then $0 \leq \lambda \leq k - 1$ and $0 \leq \mu \leq k$. ■

Suppose D is a PDs with $e \in D$ and $D^{(-1)} = D$. If D has parameters $(v, k, \lambda, \mu, \beta, \Delta)$, then $D' = D\backslash\{e\}$ has parameters

$$(v', k', \lambda', \mu', \beta', \Delta') = (v, k - 1, \lambda - 2, \mu, \beta - 2, \Delta).$$

Hence Proposition 1.4 holds for D if we change k to $k - 1$ and β to $\beta - 2$. Throughout this paper, we shall state most of our theorems in terms of regular PDSs. For a PDS D with $e \in D$ and $D^{(-1)} = D$, readers have to transform D to D' as above in order to obtain the corresponding results.

Let G be a finite group. It is easy to see that $\emptyset$, $\{e\}$, $G\backslash\{e\}$ and G are PDSs with $(\beta, \Delta) = (m, m^2)$, $(m + 2, m^2)$, $(m - 2, m^2)$ and (m, m^2), respectively, for any interger m. (For these cases, either λ or μ is not defined in the definition of PDSs and hence can be any number.) Also, if H is a subgroup of G, then $G\backslash H$, $(G\backslash H) \cup \{e\}$, $H\backslash\{e\}$ and H are PDSs with $(\beta, \Delta) = (-w, w^2)$, $(-w + 2, w^2)$, $(w - 2, w^2)$ and (w, w^2), respectively, where w is the order of H. In the following, a subset D of G is called *trivial* if either $D \cup \{e\}$ or $(G\backslash D) \cup \{e\}$ is a subgroup of G (it is equivalent to say that the Cayley graph generated by $D\backslash\{e\}$ is a union of complete graphs or its complement); otherwise, D is called *nontrivial*.

PROPOSITION 1.5. Let D be a regular PDS with parameters $(v, k, \lambda, \mu, \beta, \Delta)$. Then D is nontrivial if and only if $-\sqrt{\Delta} < \beta < \sqrt{\Delta} - 2$. Furthermore, if $D \neq G\backslash\{e\}$, then D is nontrivial if and only if $1 \leq \mu \leq k - 1$. ■

2. Some Examples

In this section, we shall see some nontrivial examples of regular PDSs. The first example can be dated back as early as Paley [23].

THEOREM 2.1. *Let G be the additive group of a finite field $\mathbb{F}_q$ where q is an odd prime power and $q \equiv 1$ mod 4. Then the set D of all nonzero squares in $\mathbb{F}_q$ forms a regular $(q, (q - 1)/2, (q - 5)/4, (q - 1)/4)$-PDS in G. Note that $\beta = -1$* and $\Delta = q$. ■

Theorem 2.1 can be regarded as a particular case of the construction method using cyclotomic classes which we shall discuss in Section 10.

Let G be a group of order n^2. A *partial congruence partition* of G with degree r (an (n, r)-PCP) is a set $\mathcal{P}$ of r subgroups of G of order n such that $U \cap V = \{e\}$ for every pair of distinct elements U, V of $\mathcal{P}$. Sprague [24] has shown that an (n, r)-PCP of G is equivalent to a translation net, see Example 14.2(2). Readers are referred to Bailey and Jungnickel [25] for results of PCPs and Jungnickel [26] for a survey of related topics.

THEOREM 2.2 (Ma [10]) *Let G be a group of order n^2 and $\mathcal{P}$ be an (n, r)-PCP of G. Then $D = \bigcup_{U\in\mathcal{P}}(U\backslash\{e\})$ is a regular $(n^2, r(n-1), n+r^2-3r, r^2-r)$-PDS in G. Note that $\beta = n - 2r$ and $\Delta = n^2$.* ■

Example 2.3.

1. Let $G = H \times K$ where H and K are groups of order n. Then $D = \{(h, e) : h \in H\backslash\{e\}\} \cup \{(e, g) : g \in K\backslash\{e\}\}$ is a regular $(n^2, 2(n-1), n-2, 2)$-PDS in G.
2. Let $G = H \times H$ where H is a group of order n. Then $D = \{(h, e), (e, h), (h, h) : h \in H\backslash\{e\}\}$ is a regular $(n^2, 3(n-1), n, 6)$-PDS in G.
3. Let G be the additive group of a vector space of dimension 2 over a finite field $\mathbb{F}_q$ and $H_1, H_2, \ldots, H_r$ (where $r \leq q + 1$) be r distinct hyperplanes of the vector space. Then $D = (H_1 \cup H_2 \cup \cdots \cup H_r)\backslash\{0\}$ is a regular $(q^2, r(q-1), q+r^2-3r, r^2-r)$-PDS in G. ■

THEOREM 2.4. (Bailey and Jungnickel [25]) *Let G be an abelian group of order n^2 with $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ where $p_1, p_2, \ldots, p_s$ are distinct primes.*

(a) *If $r > min\{p_i^{a_i} + 1\}$, then no (n, r)-PCP exists in G.*
(b) *Suppose all Sylow p_i-subgroups of G are elementary abelian. Then an (n, r)-PCP exists in G if and only if $1 \leq r \leq min\{p_i^{a_i} + 1\}$.* ■

COROLLARY 2.5. *Let $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ where $p_1, p_2, \ldots, p_s$ are distinct primes. Then there exists an abelian regular $(n^2, r(n-1), n+r^2-3r, r^2-r)$-PDS whenever $1 \leq r \leq min\{p_i^{a_i} + 1\}$.* ■

A PDS having parameters $(v, k, \lambda, \mu) = (n^2, r(n-1), n+r^2-3r, r^2-r)$ is called a *Latin square type* PDS. The name comes from the construction of strongly regular graphs by using Latin squares which yield the same type of parameters, see Chapter 8 of Cameron and van Lint [6]. All examples constructed by Theorem 2.2 belong to this type. Another type of parameters which is closely related to the Latin square type is $(v, k, \lambda, \mu) = (n^2, r(n+1), -n+r^2+3r, r^2+r)$. A PDS with these parameters is called a *negative Latin square type* PDS.

Let q be a power of a prime and $\mathbb{F}_q$ be a field of q elements. A function $Q : \mathbb{F}_q^s \to \mathbb{F}_q$ is called a *quadratic form* if

(i) $Q(\alpha x) = \alpha^2 Q(x)$ for all $\alpha \in \mathbb{F}_q$ and $x \in \mathbb{F}_q^s$, and
(ii) the function $B : \mathbb{F}_q^s \times \mathbb{F}_q^s \to \mathbb{F}_q$ defined by $B(x, y) = Q(x+y) - Q(x) - Q(y)$ is bilinear.

Furthermore, Q is called *nondegenerate* if B is nondegenerate, i.e., $B(x, y) = 0$ for all $y \in \mathbb{F}_q^s$ implies $x = 0$. The following is a well-known result, e.g., see Calderbank and Kantor [18] or Cameron and van Lint [6].

THEOREM 2.6. *Let $Q : \mathbb{F}_q^{2m} \to \mathbb{F}_q$ be a nondegenerate quadratic form. Then $D = \{x \in \mathbb{F}_q^{2m}\backslash\{0\} : Q(x) = 0\}$ is a regular $(q^{2m}, q^{2m-1} + \epsilon q^{m-1}(q - 1) - 1, q^{2m-2} + \epsilon q^{m-1}(q - 1) - 2, q^{2m-2} + \epsilon q^{m-1})$-PDS in the additive group of $\mathbb{F}_q^{2m}$, where $\epsilon = \pm 1$ and depends on the choice of Q. Note that $\beta = \epsilon q^{m-1}(q - 2) - 2$ and $\Delta = q^{2m}$.* ■

Example 2.7.

1. When $\epsilon = 1$, the PDSs constructed by Theorem 2.6 have parameters $(v, k, \lambda, \mu) = (q^{2m}, r(q^m - 1), q^m + r^2 - 3r, r^2 - r)$, where $r = q^{m-1} + 1$, which belong to the Latin square type.
2. When $\epsilon = -1$, the PDSs constructed by Theorem 2.6 have parameters $(v, k, \lambda, \mu) = (q^{2m}, r(q^m + 1), -q^m + r^2 + 3r, r^2 + r)$, where $r = q^{m-1} - 1$, which belong to the negative Latin square type. ■

Some other examples of nontrivial PDSs will be given in Sections 8, 9, 10, 11 and 12. Here, we give one particular example which has parameters $v \neq \Delta$. This is also an example of reversible difference sets which will be discussed in Section 12.

Example 2.8. (McFarland [27]) Let V be the additive group of a vector space over $\mathbb{F}_5$ of dimension 3 and $H_1, H_2, \ldots, H_{31}$ be all hyperplanes of the vector space. Let $K = \{g_0, g_1, \ldots, g_{31}\}$ be a group of order 32. Then $D = \{(g_i, h_i) : h_i \in H_i \text{ and } i = 1, 2, \ldots, 31\}$ is a (4000, 775, 150, 150)-PDS in $G = K \times V$ and D is regular when K is elementary abelian and $g_0 = e$. Note that $\beta = 0$ and $\Delta = 2500$. ■

3. Character Values and Duals

For an abelian group G, let G^* denote the group of characters of G. For any $\chi \in G^*$, the induced homomorphism from $\mathbb{C}[G]$ to $\mathbb{C}$ is also denoted by χ, i.e. $\chi(\Sigma_{g\in G} a_g g) = \Sigma_{g\in G} a_g \chi g$ where $a_g \in \mathbb{C}$.

THEOREM 3.1. (*Fourier Inversion Formula*) *Let G be a finite abelian group and $y = \Sigma_{g\in G} a_g g \in \mathbb{C}[G]$ where $a_g \in \mathbb{C}$. Then for every $g \in G$,*

$$a_g = \frac{1}{|G|} \sum_{\chi\in G^*} (\chi y)(\chi g^{-1}). \tag{3.1}$$

■

The proof of Theorem 3.1 can be found in Mann [28]. As a consequence of Theorem 3.1, we have the following results.

COROLLARY 3.2. *Let G be a finite abelian group and $y, z \in \mathbb{C}[G]$. Then $y = z$ if and only if $\chi y = \chi z$ for all $\chi \in G^*$.* ■

A character $\chi \in G^*$ is called *trivial* if $\chi g = 1$ for all $g \in G$; otherwise, it is called *nontrivial*.

COROLLARY 3.3. *Let G be an abelian group of order v and D be a subset of G such that $D^{(-1)} = D$. Suppose k, λ and μ are positive integers satisfying $k^2 = \mu v + (\lambda - \mu)k + \gamma$ where $\gamma = k - \mu$ if $e \notin D$ and $\gamma = k - \lambda$ if $e \in D$. Then D is a (v, k, λ, μ)-PDS in G if and only if*

$$\chi\bar{D} = \begin{cases} k & \text{if } \chi \text{ is trivial;} \\ (\beta \pm \sqrt{\Delta})/2 & \text{if } \chi \text{ is nontrivial.} \end{cases} \tag{3.2}$$

where $\beta = \lambda - \mu$ and $\Delta = \beta^2 + 4\gamma$. ■

Let G be an abelian group of order v and D be a (v, k, λ, μ)-PDS in G with $D^{(-1)} = D$. If $D \neq \emptyset$, $\{e\}$, $G\backslash\{e\}$ and G, then the *dual* of D is defined to be $D^+ = \{\chi \in G^* : \chi$ is nontrivial and $\chi\bar{D} = (\beta + \sqrt{\Delta})/2\}$. Note that if $e \in D$, then $D^+ = (D\backslash\{e\})^+$.

THEOREM 3.4. (Delsarte [14]) *Let G be an abelian group of order v and $D(\neq \emptyset$ and $G)$ be a regular (v, k, λ, μ)-PDS in G. Then the dual D^+ of D is a regular PDS in G^* with parameters*

$$(v^+, k^+, \lambda^+, \mu^+, \beta^+, \Delta^+) = (v, [(\sqrt{\Delta} - \beta)(v - 1) - 2k]/(2\sqrt{\Delta}), \beta^+ + \mu^+,$$
$$[4k^+ - \Delta^+ + (\beta^+)^2]/4, (v - 2k + \beta - \sqrt{\Delta})/\sqrt{\Delta}, v^2/\Delta).$$

Note that

$$\left[2\bar{D}^+ - \left(\frac{v - 2k + \beta - \sqrt{\Delta}}{\sqrt{\Delta}}\right)\chi_0\right]^2 = \frac{v}{\Delta}[(\sqrt{\Delta} - \beta - 1)^2 - 1]\bar{G}^* + \frac{v^2}{\Delta}\chi_0 \tag{3.3}$$

where χ_0 is the trivial character of G. ■

Delsarte [14] obtained Theorem 3.4 in connection with his new approach to coding theory. He had pointed out that Theorem 3.4 could be regarded as a particular case of a theorem on Schur rings obtained by Tamaschke [29]. Schur rings will be studied in Section 5. Now, let us see some examples.

Let G be an abelian group and H a subgroup of G. A character χ is called *principal* on H if $\chi g = 1$ for all $g \in H$. Also, we define

$$H^\perp = \{\chi \in G^* : \chi \text{ is principal on } H\}$$

which is a subgroup of G^* of order $v/|H|$.

Example 3.5.

1. Let G be the additive group of $\mathbb{F}_q^2$ and $H_1, H_2, \ldots, H_r$ (where $r \leq q + 1$) be r distinct hyperplanes of $\mathbb{F}_q^2$. By Example 2.3(3), $D = (H_1 \cup H_2 \cup \cdots \cup H_r)\backslash\{0\}$ is a regular

$(q^2, r(q-1), q+r^2-3r, r^2+r)$-PDS in G. Note that $\beta = q-2r$ and $\Delta = q^2$. Since $H_i^{\perp} \cap H_j^{\perp} = \{\chi_0\}$ where χ_0 is the trivial character, we have

$$\chi\bar{D} = \chi\left[\sum_{i=1}^{r}\bar{H}_i - re\right] = \begin{cases} r(q-1) & \text{if } \chi = \chi_0; \\ (\beta+\sqrt{\Delta})/2 = q-r & \text{if } \chi \in H_i^{\perp}\backslash\{\chi_0\} \text{ for some } i; \\ (\beta-\sqrt{\Delta})/2 = -r & \text{if } \chi \notin H_i^{\perp} \text{ for all } i. \end{cases}$$

Hence $D^+ = (H_1^{\perp} \cup H_2^{\perp} \cup \cdots \cup H_r^{\perp})\backslash\{\chi_0\}$ which is a regular $(q^2, r(q-1), q+r^2-3r, r^2+r)$-PDS in G^*. Note that D^+ has the same structure as D.

2. Let V be the additive group of $\mathbb{F}_5^3$; $H_1, H_2, \ldots, H_{31}$ be all hyperplanes of $\mathbb{F}_5^3$ and $K = \{g_0 = e, g_1, \ldots, g_{31}\}$ be an elementary abelian 2-group of order 32. By Example 2.8, $D = \{(g_i, h_i) : h_i \in H_i \text{ and } i = 1, 2, \ldots, 31\}$ is a regular (4000, 775, 150, 150)-PDS in $G = K \times V$. Note that $\beta = 0$ and $\Delta = 2500$. We have the following observations:

(i) We can identify the elements of G^* with elements of $K^* \times V^*$ such that $\chi \in G^*$ is written as (χ_K, χ_V) where $\chi_K = \chi|_K \in K^*$ and $\chi_V = \chi|_V \in V^*$.

(ii) For any nontrivial character $\chi_V \in V^*$, χ_V is principal on exactly one H_i for $i = 1, 2, \ldots, 31$. Let χ_0 be the trivial character. Then $\{\chi_0\}$, $H_1^{\perp}\backslash\{\chi_0\}$, $H_2^{\perp}\backslash\{\chi_0\}, \ldots,$ $H^{\perp}{}_{31}\backslash\{\chi_0\}$ form a partition of V^*

Hence, for $\chi = (\chi_K, \chi_V) \in G^*$, we have

$$\chi\bar{D} = \chi\left[\sum_{i=1}^{31}\sum_{h_i \in H_i}(g_i, h_i)\right] = \sum_{i=1}^{31}(\chi_K g_i)(\chi_V \bar{H}_i)$$

$$= \begin{cases} 775 & \text{if } \chi \text{ is trivial}; \\ (\beta+\sqrt{\Delta})/2 = 25 & \text{if } \chi_V \in H_i^{\perp}\backslash\{\chi_0\} \text{ and } \chi_K g_i = 1 \text{ for some } i; \\ (\beta-\sqrt{\Delta})/2 = -25 & \text{otherwise.} \end{cases}$$

So $D^+ = \cup_{i=1}^{31}\,[<g_i>^{\perp} \times (H_i^{\perp}\backslash\{\chi_0\})]$ is a regular (400, 1984, 1008, 960)-PDS in G^*. Note that $\beta^+ = 48$ and $\Delta^+ = 6400$. ■

Since the parameters of D^+ and the coefficients of (3.3) are integers, we have the following corollary.

COROLLARY 3.6. *If there exists an abelian regular (v, k, λ, μ)-PDS D such that $D \neq \emptyset$ and $G\backslash\{e\}$, then $v^2 \equiv (2k-\beta)^2 \equiv (\beta^2+2\beta)v \equiv 0 \bmod \Delta$.* ■

Let G be an abelian group. For any $g \in G$, we define X_g to be a character of G^* such that $X_g(\chi) = \chi g$ for all $\chi \in G^*$. Note that the mapping $g \mapsto X_g$ is a one-to-one correspondence between G and $(G^*)^*$, the group of characters of G^*. Thus we can always identify X_g with g for all $g \in G$. The following result is a consequence of Theorem 3.1.

THEOREM 3.7. *Using the notation above, if D is a regular PDS in G, then $(D^+)^+ = D$.* ■

4. Multipliers

Let G be a finite group and D be a subset of G. An automorphism σ of G is called a *multiplier* of D if $\sigma D = D$. Note that the definition of multipliers is different from that for difference sets, see Beth, Jungnickel and Lenz [20] and Lander [21].

Let G be an abelian group of order v and t be an integer relatively prime to v. Then the mapping $g \mapsto g^t$ is an automorphism of G. If the mapping is a multiplier of a subset D of G, i.e., $D^{(t)} = D$, then we say that t is a (*numerical*) *multiplier* of D. As we shall see in the following theorem, abelian PDSs are rich in multipliers.

THEOREM 4.1. *Let G be an abelian group of order v and D a regular (v, k, λ, μ)-PDS in G. Then t^2 is a multiplier of D for any t relatively prime to v. Furthermore, if Δ is a square, then t is a multiplier of D for any t relatively prime to v.* ■

Theorem 4.1 was first obtained by Hughes, van Lint and Wilson [30] but not published and latter was proved independently by Ma [10]. Also, Bridges and Mena [17] had proved implicitly the case when Δ is a square.

Example 4.2.

1. Let G be an abelian group of order n^2. For any PDS D in G constructed from PCP as in Theorem 2.2, it is obvious that $D^{(t)} = D$ for all t relatively prime to n. Also, in this case, $\Delta = n^2$ is a square.
2. Let G be the additive group of the finite field $\mathbb{F}_q$, where $q \equiv 1 \bmod 4$, and D be the set of all nonzero squares. By Theorem 2.1, D is a regular PDS with $\Delta = q$. Let $q = p^r$, where p is a prime, and let t be any integer relatively prime to p. If r is even, i.e., Δ is a square, then t is a multiplier of D. If r is odd, i.e., Δ is not a square, then t is a multiplier of D if and only if t is a square modulo p. ■

Up to now, there is no multiplier theorem for nonabelian PDSs. On the other hand, Ghinelli and Löwe [19] have some related results. A subset D of a group G is called *normal* if D is a union of conjugacy classes of G. Ghinelli and Löwe study when a normal regular (v, k, λ, μ)-PDS D can be fixed by the mapping $g \mapsto g^t$, i.e., $D^{(t)} = D$, where t is an integer relatively prime to v. However, for nonabelian groups, the mapping $g \mapsto g^t$ is not an automorphism. The following is their main result.

THEOREM 4.3. (Ghinelli and Löwe [19]) *Let G be a finite group of exponent w, D a normal regular (v, k, λ, μ)-PDS in G and t an integer relatively prime to w. In the field $\mathbb{Q}[\zeta]$, where ζ is a primitive wth root of unity, let σ be the automorphism which maps ζ to ζ^t. Then $D^{(t)} = D$ if and only if $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$.* ■

5. Schur Rings and Some Nonexistence Results

Let G be a finite group and $D_0, D_1, \ldots, D_d$ be nonempty subsets of G with properties that

(i) $D_0 = \{e\}$;
(ii) $G = D_0 \cup \cdots \cup D_d$ and $D_i \cap D_j = \emptyset$ if $i \neq j$;
(iii) $D_i^{(-1)} = D_j$ for some j depending on i;
(iv) $\bar{D}_i\bar{D}_j = \Sigma_{k=0}^{d} p_{ij}^k\bar{D}_k$ for $i, j = 0, 1, \ldots, d$, where p_{ij}^k's are integers.

Then the subalgebra S of $\mathbb{C}[G]$ spanned by $\bar{D}_0, \bar{D}_1, \ldots, \bar{D}_d$ is called a *Schur ring* of dimension $d + 1$ over G. Furthermore, if

(v) $D_i^{(-1)} = D_i$ for $i = 0, 1, \ldots, d$.

then S is called *symmetric*.

Historically, Schur rings were first studied by Schur [31] and Wielandt [32] in their works concerning permutation groups. For the work done by group theorists, pleas see Wielandt [33], and Scott [34]. Recently, Schur rings had been found to be useful in constructing association schemes which are used in coding theory and experimental designs, see Bose and Mesner [35], Delsarte [14], Bannai, and Ito [36] and Ma [11].

Let G be a finite group. For $y \in \mathbb{C}[G]$, let T_y denote the support of y, i.e., $T_y = \{g \in G :$ The coefficient of g in y is nonzero.$\}$. A Schur ring S over G is called *primitive* if $<T_y> = \{e\}$ or G for all nonzero $y \in S$. If S is spanned by $\bar{D}_0 = e, \bar{D}_1, \ldots, \bar{D}_d$, then S is primitive if and only if each D_i, $i = 1, 2, \ldots, d$, is not contained in any proper subgroup of G.

Proposition 5.1. Let D be a subset of a finite group G such that $D^{(-1)} = D$. Then $\bar{D}_0 = e$, $\bar{D}_1 = \overline{D\backslash\{e\}}$, $\bar{D}_2 = \bar{G} - \bar{D}_1 - e$ span a primitive symmetric Schur ring of dimension 3 over G if and only if D is a nontrivial PDS in G. ■

The existence of primitive Schur rings is a main topic for group theorists working on Schur rings. The following are some of the results.

A Schur ring S over a finite group G is called *trivial* if S is spanned by $\bar{D}_0 = e$ and $\bar{D}_1 = \bar{G} - e$; otherwise, S is called *nontrivial.*

Theorem 5.2. (Wielandt [33]) *Let G be a finite abelian group and P be the Sylow p-subgroup of G. No nontrivial primitive Schur ring exists over G if either* (*a*) *P is cyclic and $o(G) \neq p$ or* (*b*) *$P \cong \mathbb{Z}_{p^s} \times \mathbb{Z}_{p^t}$ with $s \neq t$.* ■

Theorem 5.3. (Wielandt [32]) *No nontrivial primitive Schur ring exists over dihedral groups.* ■

Theorem 5.4. (Scott [37]) *Let H be an abelian group with exactly one element h of order 2 and let G be the generalized dicyclic group generated by H and j where $j^2 = h$ and $jgj^{-1} = g^{-1}$ for all $g \in H$. Then no nontrivial primitive Schur ring exists over G.* ■

THEOREM 5.5. (Scott [34]) *Let G be a group of order $p + 1$ where p is an odd prime. Suppose there exists a nontrivial primitive Schur ring of dimension $d + 1$ over G. Then $p > 37$ and $d \geq 3$.* ■

By Proposition 5.1 and Theorems 5.2, 5.3, 5.4, 5.5, we have the following nonexistence theorem on PDSs.

THEOREM 5.6. *No nontrivial regular PDS exists in each of the following groups:*

(a) *any abelian group G with a cyclic Sylow p-subgroup and $o(G) \neq p$;*
(b) *any abelian group with a Sylow p-subgroup isomorphic to $\mathbb{Z}_{p^s} \times \mathbb{Z}_{p^t}$ where $s \neq t$;*
(c) *any dihedral group;*
(d) *a generalized dicyclic group G generated by H and j where H is an abelian group with exactly one element h of order 2 and j is an element of G satisfying $j^2 = h$ and $jgj^{-1} = g^{-1}$ for all $g \in H$;*
(e) *any group of order $p + 1$ where p is an odd prime.* ■

Let G be a cyclic group of order p, where p is a prime, such that there exists a nontrivial regular PDS D in G. Note that $p \neq 2$ since D is nontrivial. Let g be a generator of G. Then by Theorem 4.1, D is either $Q = \{g^t : t \text{ is a nonzero square modulo } p\}$ or $(G \backslash Q) \backslash \{e\}$. Also, $D^{(-1)} = D$ implies $p \equiv 1 \bmod 4$.

COROLLARY 5.7. *Let G be a cyclic group of order v. The following are all regular PDSs in G:*

(a) *Either $D \cup \{e\}$ or $G \backslash D$ is a subgroup of G.*
(b) *v is an odd prime with $v \equiv 1 \bmod 4$ and D is of the form*

$$\{g^t : t = \omega^{2j+c} \text{ for } j = 0, 1, 2, \ldots, (v-3)/2\}$$

where g is a generator of G, ω is a primitive root modulo v and $c = 0$ or 1. ■

Corollary 5.7 was also proved independently by Bridges and Mena [16] and Ma [10] without knowing the result on Schur rings. Similarly, Bridges and Mena [17] proved a particular case of Theorem 5.6(b); Ma [38] proved Theorem 5.6(c) and de Resmini and Jungnickel [39] proved Theorem 5.6(d) for the case when H is cyclic.

With the results of Corollary 5.7 and Theorem 5.6(b), (c), de Resmini and Jungnickel [39] conjecture that every regular PDS in a group having a cyclic normal subgroup of index 2 is trivial. By Example 5.10 below, we shall see that this is not true. However, we still think that their conjecture is true for almost all such groups, probably with a finite number of exceptional cases.

Problem 5.8. Determine all groups which have a cyclic normal subgroup of index 2 and have a nontrivial regular PDS. ■

The following is a theorem in this direction.

THEOREM 5.9. (de Resmini and Jungnickel [39] and Leung and Ma [40]) *No nontrivial regular PDS exists in any 2-group G with a cyclic subgroup of index 2 except when $G = <g, h : g^8 = h^2 = e, hgh^{-1} = g^3>$ and $G = <g, h : g^8 = h^2 = e, hgh^{-1} = g^5>$.* ■

Examples exists for the two exceptions in Theorem 5.9.

Example 5.10.

1. For $G = <g, h : g^8 = h^2 = e, hgh^{-1} = g^3>$, the subset $D = \{g, g^7, h, gh, g^2h, g^5h\}$ is a regular (16, 6, 2, 2)-PDS in G.
2. For $G = <g, h : g^8 = h^2 = e, hgh^{-1} = g^5>$, the subset $D = \{g, g^3, g^5, g^6, gh, g^3h\}$ is a regular (16, 6, 2, 2)-PDS in G. ■

6. Restrictions on the Parameters

In this section, we shall study some restrictions on the parameters of a regular PDS. First, let us consider a relation between v and Δ.

THEOREM 6.1. (Ma [10]) *If there exists a nontrivial regular (v, k, λ, μ)-PDS in an abelian group, then v, Δ and v^2/Δ must have the same prime divisors.* ■

Next, we study the case when Δ is not a square.

THEOREM 6.2. (Ma [10]) *Suppose there exists a regular (v, k, λ, μ)-PDS in a group G such that Δ is not a square. Then*

(a) *there is a positive integer t such that*

$$(v, k, \lambda, \mu, \beta, \Delta) = (4t + 1, 2t, t - 1, t, -1, 4t + 1);$$

(b) *$v = \Delta = u^2p$ where p is a prime such that $p \equiv 1 \bmod 4$; and*
(c) *$|G/G'|$ is a power of p where G' is the derived subgroup of G.* ■

When G is abelian, $G' = \{e\}$. Thus we have the following corollary.

COROLLARY 6.3. *Suppose there exists an abelian regular (v, k, λ, μ)-PDS such that Δ is not a square. Then*

$$(v, k, \lambda, \mu, \beta, \Delta) = (p^{2s+1}, (p^{2s+1} - 1)/2, (p^{2s+1} - 5)/4, (p^{2s+1} - 1)/4, p^{2s+1})$$

where p is a prime such that $p \equiv 1 \bmod 4$. ■

For the abelian case, we know more about the structure of such a PDS.

THEOREM 6.5. (Ma [41]) *Let G be an abelian group of order $v = p^{2s+1}$ for a prime $p \equiv 1$ mod 4 and D be a regular $(v, (v-1)/2, (v-5)/4, (v-1)/4)$-PDS in G. Then for any integer t relatively prime to p, $D^{(t)} = D$ if t is a square modulo p; and $D^{(t)} \cap D = \emptyset$ if t is not a square modulo p.* ■

Example 6.5. By Theorem 2.1, if G is the additive group of the finite field $\mathbb{F}_{p^{2s+1}}$, then the set of nonzero squares forms a regular PDS with parameters as stated in Corollary 6.3. Note that G is an elementary abelian p-group. Also, for any integer t relatively prime to p, $tD = D$ if t is a square modulo p; and $tD \cap D = \emptyset$ if t is not a square modulo p. ■

Up to now, all known examples with Δ not a square are in elementary abelian p-groups. Ma [42] had asked the following question.

Question 6.6. Is it true that elementary abelian p-groups are the only abelian groups which consist of regular PDSs such that the parameter Δ is not a square ? ■

There is a result related to Question 6.6.

THEOREM 6.7. (Davis [43]) *If there exists a regular $(v, (v-1)/2, (v-5)/4, (v-1)/4)$-PDS D in an abelian group G where $v = p^{2s+1}$ for a prime $p \equiv 1$ mod 4 where $s \geq 1$, then the exponent of G cannot exceed p^s.* ■

Finally, we consider the case when Δ is a square. Most of the known examples are of this type, e.g., Examples 2.3, 2.7 and 2.8. Note that if G is abelian, then by Theorem 4.1, a PDS D in G with $D^{(-1)} = D$ has the property that $D^{(t)} = D$ for all t relatively prime to $v = |G|$.

THEOREM 6.8. *Suppose there exists a regular (v, k, λ, μ)-PDS in an abelian group of order $v = p^s$ where p is a prime. If Δ is a square, then k is a multiple of $p - 1$.* ■

THEOREM 6.9. (Ma [41]) *Let G be an abelian group of order v and exponent w. Let p be a prime such that p^t strictly divides v and p^r strictly divides w. If there exists a nontrivial regular (v, k, λ, μ)-PDS in G such that Δ is a square then p^{2r} divides Δ and $p^{2(t-r+1)}$ does not divide Δ.* ■

By Theorem 6.9, if $2r > t$, then no nontrivial regular PDS exists in G with Δ being a square. Hence this gives another proof of Theorem 5.6(a) and (b) for the case when Δ is a square.

7. Subsets of Abelian Partial Difference Sets

In this section, we study a very interesting phenomenon about abelian PDSs—some subsets of a regular PDs are themselves PDSs.

THEOREM 7.1. (Ma [44]) *Let D be a nontrivial regular (v, k, λ, μ)-PDS in an abelian group G. Suppose Δ is a square, say $\Delta = \delta^2$. If N is a subgroup of G such that g.c.d.$(|N|, |G|/|N|) = 1$ and $|G|/|N|$ is odd, then $D_1 = D \cap N$ is a regular $(v_1, k_1, \lambda_1, \mu_1)$-PDS with*

$$v_1 = |N|, \beta_1 = \lambda_1 - \mu_1 = \beta - 2\theta\pi, \Delta_1 = \beta_1^2 + 4(k_1 - \mu_1) = \pi^2$$

and

$$k_1 = \frac{1}{2}\left[(v_1 + \beta_1) \pm \sqrt{(v_1 + \beta_1)^2 - (\Delta_1 - \beta_1^2)(v_1 - 1)}\right]$$

where $\pi =$ g.c.d. $(|N|, \delta)$ and θ is the integer satisfying $(2\theta - 1)\pi \leq \beta < (2\theta + 1)\pi$. ■

Example 7.2.

1. Let G be an abelian group of order n^2 and $\mathcal{P}$ be an (n, r)-PCP of G. By Theorem 2.2, $D = \bigcup_{U \in \mathcal{P}}(U \backslash \{e\})$ is a regular $(n^2, r(n - 1), n + r^2 - 3r, r^2 - r)$-PDS in G with $\beta = n - 2r$ and $\Delta = n^2$. Suppose $n = uw$ where g.c.d.$(u, w) = 1$ and w is odd. Let N be the subgroup in G of order u^2. Since $|U \cap N| = u$ for all $U \in \mathcal{P}$, $\mathcal{P}_1 = \{U \cap N : U \in \mathcal{P}\}$ is a (u, r)-PCP of G. By Theorem 2.4(a), we have $1 \leq r \leq u + 1$.

   (i) Suppose $1 \leq r \leq u$. Then $D_1 = D \cap N = \bigcup_{U_1 \in \mathcal{P}_1}(U_1 \backslash \{e\})$ is a regular $(u^2, r(u - 1), u + r^2 - 3r, r^2 - r)$-PDS in N with $\beta_1 = u - 2r$ and $\Delta_1 = u^2$. Note that $\pi =$ g.c.d.$(u, n) = u$ and $\theta = (w - 1)/2$.

   (ii) Suppose $r = u + 1$. Then $D_1 = D \cap N = N \backslash \{e\}$. Since there is no nonidentity element in D_1 not contained in N, the value μ_1 is undefined from the definition of PDSs. Thus we can always regard D_1 as a $(u^2, u^2 - 1, u^2 - u, u^2 - 2)$-PDS in N with $\beta_1 = u - 2$ and $\Delta_1 = u^2$. Note that $\pi = u$ and $\theta = (w - 3)/2$.

2. Let V be the additive group of $\mathbb{F}_5^3$; $H_1, H_2, \ldots, H_{31}$ be all hyperplanes of $\mathbb{F}_5^3$ and $K = \{g_0 = e, g_1, \ldots, g_{31}\}$ be an elementary abelian 2-group of order 32. By Example 2.8, $D = \{(g_i, h_i) : h_i \in H_i$ and $i = 1, 2, \ldots, 31\}$ is a regular (4000, 775, 150, 150)-PDS in $G = K \times V$ with $\beta = 0$ and $\Delta = 2500$. Let $N = K \times \{0\}$ which is a subgroup of G of order 32. Since $D_1 = D \cap N = N \backslash \{(e, 0)\}$, it can be regarded as a (32, 31, 30, 30)-PDS in N with $\beta_1 = 0$ and $\Delta_1 = 4$. Here, $\pi = 2$ and $\theta = 0$. ■

Theorem 7.1 can be used as a nonexistence theorem, see Theorems 12.3, 13.1, 15.1 and Table 15.3. Now, let us have a theorem describing the structural relation between D and D_1.

THEOREM 7.3. (Ma 44]) *Let D be a nontrivial regular (v, k, λ, μ)-PDS in an abelian group G. Let p be an odd prime divisor of v, say $v = p^t u$ and $\Delta = p^{2r}\pi^2$ where u, π are relatively prime to p. Let P and N be the subgroups of G of order p^t and u, respectively, and let $D_1 = D \cap N$ which is a regular $(v_1, k_1, \lambda_1, \mu_1)$-PDS in N.*

(a) Let $\rho : G \to N$ be a projection with Ker $\rho = P$. Then

$$\rho\bar{D} \equiv \bar{D}_1 \bmod (p - 1) \tag{7.1}$$

and

$$2\rho\bar{D} - \beta e = p^r[a\bar{N} + 2\epsilon\bar{D}_1 + be] \tag{7.2}$$

where $\epsilon = \pm 1$ and a, b are integers. If $D_1 \neq \emptyset$ and $N\backslash\{e\}$, then $a = [(2k - \beta) - \epsilon p^r(2k_1 - \beta_1)]/(p^r u)$ and $b = -\epsilon\beta_1$.

(b) Regard the subgroup $P^\perp$ of G^* as the group of characters of N. Let $R = D^+ \cap P^\perp$ and $\rho' : G^* \to P^\perp$ be a projection with Ker $\rho' = N^\perp$. Then

$$\rho'\bar{D}^+ \equiv \bar{R} \bmod (p - 1) \tag{7.3}$$

and

$$2\rho'\bar{D}^+ - \beta^+\chi_0 = p^{t-r}[(p^r - \epsilon - 2\theta)\bar{P}^\perp + 2\epsilon\bar{R} + d\chi_0] \tag{7.4}$$

where χ_0 is the trivial character of N, d is an integer and ϵ is the same as in (7.2). Furthermore, if $D_1 \neq \emptyset$ and $N\backslash\{e\}$, then

$$D_1^+ = \begin{cases} R & \text{if } \epsilon = 1 \\ (P^\perp\backslash R)\backslash\{\chi_0\} & \text{if } \epsilon = -1. \end{cases}$$

(c) If $p \geq 5$ and $D_1 \neq \emptyset$ and $N\backslash\{e\}$, then the value of ϵ in (7.2) is equal to 1; and either (i) r is even and $\theta \equiv 0 \bmod (p - 1)$ or (ii) r is odd and $\theta \equiv (p - 1)/2 \bmod (p - 1)$. ■

Finally, we want to point out that not too many examples of regular PDSs are known when v is not a prime power. All of them are either of the PCP type (see Section 2) or related to reversible difference sets (see Section 12).

8. Two-Weight Codes

In this section, we study the relation between regular PDSs and error-correcting codes. Readers are referred to MacWilliams and Sloane [45], van Lint [46] and Pless [47] for an introduction to coding theory. Let q be a power of a prime p. An *(n, s)-linear code* C over $\mathbb{F}_q$ is a s-dimensional subspace of $\mathbb{F}_q^n$. Vectors in C are called *codewords*. The *dual code* of C is the $(n, n - s)$-linear code $C^\perp = \{u \in \mathbb{F}_q^n : u \cdot v = 0 \text{ for all } v \in C\}$. The *weight* $w(x)$ of a vector $x \in \mathbb{F}_q^n$ is the number of nonzero entries in x. The *distance* $d(x, y)$

of two vectors x, $y \in \mathbb{F}_q^n$ is the number of coordinate positions in which x and y differ. Note that $d(x, y) = w(x - y)$. The *minimum weight* of a code C is the minimum weight of all nonzero codewords in C. If C is a linear code with minimum weight d, then C is an *α-error-correcting code* where $\alpha = \lfloor (d - 1)/2 \rfloor$. A code C is called a *two-weight code* if $|\{w(u) : u \in C\backslash\{0\}\}| = 2$.

Let C be an (n, s)-linear code over $\mathbb{F}_q$. Then there exist $y_1, y_2, \ldots, y_n$ in $\mathbb{F}_q^2$ such that

$$C = \{(x \cdot y_1, x \cdot y_2, \ldots, x \cdot y_n) : x \in \mathbb{F}_q^n\}.$$

We say that C is *generated* by $y_1, y_2, \ldots, y_n$. If no two of the vectors $y_1, y_2, \ldots, y_n$ are dependent, then the code C is said to be *projective*. Note that C is projective if and only if the minimum weight of the dual code $C^\perp$ is at least 3. The following theorem gives the relation between a two-weight projective code and a PDS in an elementary abelian group.

THEOREM 8.1. *Let $y_1, y_2, \ldots, y_n$ be pairwise independent vectors in $\mathbb{F}_q^n$. Then $y_1, y_2, \ldots, y_n$ generate a two-weight (n, s)-projective code C if and only if*

$$D = \{ty_i : t \in \mathbb{F}_q\backslash\{0\} \quad \text{and} \quad i = 1, 2, \ldots, n\}$$

is a regular PDS in the additive group of $\mathbb{F}_q^s$. Furthermore, if the two nonzero weights of C are w_1 and w_2, then the parameters of the PDS D are

$$(v, k, \lambda, \mu, \beta, \Delta) = (q^s, n(q - 1), k^2 + 3k - q(k + 1)(w_1 + w_2) + q^2w_1w_2,$$
$$k^2 + k - qk(w_1 + w_2) + q^2w_1w_2, 2k - q(w_1 + w_2), q^2(w_1 - w_2)^2). \quad \blacksquare$$

Theorem 8.1 was first proved by Delsarte [12]–[14] in terms of strong regular graphs and it was written in terms of difference sets by Camion [15].

Given a vector $x \in \mathbb{F}_q^n$, the sphere $S_r(x)$ with center at x and radius r is given by $S_r(x) = \{v \in \mathbb{F}_q^n : d(v, x) \leq r\}$. If C is an α-error-correcting code, then the $S_\alpha(u)$, $u \in C$, are pairwise disjoint. The code C is called *perfect* if the union of the spheres $S_\alpha(u)$, $u \in C$, covers $\mathbb{F}_q^n$.

THEOREM 8.2. (MacWilliams [48], [49]) *Let C be an α-error-correcting code. Then C is perfect if and only if $C^\perp$ has exactly α nonzero weights.* $\blacksquare$

Example 8.3.

1. Let $C = \{00000, 11111\}$ be a binary repetition code. Then $C^\perp$ is generated by 1000, 1100, 0110, 0011, 0001 over $\mathbb{F}_2$. The PDS corresponding to $C^\perp$ has parameters $(v, k, \lambda, \mu) = (16, 5, 0, 2)$.
2. Golay [50] constructed a perfect 2-error-correcting $(11, 6)$-linear code C over $\mathbb{F}_3$. Since $C^\perp$ is a two-weight $(11, 5)$-projective code with nonzero weights 6 and 9, by Theorem 8.1, a regular $(243, 22, 1, 2)$-PDS D exists in the additive group of $\mathbb{F}_3^5$. Note that $(\mathbb{F}_3^5\backslash D)\backslash\{0\}$ is a regular $(243, 220, 199, 200)$-PDS. $\blacksquare$

Perfect codes have been classified by Tietäväinen [51] and van Lint [52]. The only perfect 2-error-correcting codes are the binary repetition code and the ternary Golay code mentioned above.

Let C be an α-error-correcting code. For $x \in \mathbb{F}_q^n$, let $d(x, C)$ denote the minimum distance of x from the codewords of C; and let $B(x, i)$, where i is a nonnegative integer, denote the number of codewords in C with distance i from x. As a generalization of perfect codes, Semakov, Zinovjev and Zaitzev [53] introduced the concept of uniformly packed codes. C is called *uniformly packed* with parameters a and b if the followings hold for all $x \in \mathbb{F}_q^n$.

(i) if $d(x, C) = \alpha$, then $B(x, \alpha + 1) = a$; and
(ii) if $d(x, C) \geq \alpha + 1$, then $B(x, \alpha + 1) = b$

where $a < (n - \alpha)(q - 1)/(\alpha + 1)$. Note that for an arbitrary α-error-correcting code, a counting argument proves that if $d(x, C) = \alpha$, then $B(x, \alpha + 1) \leq (n - \alpha)(q - 1)/(\alpha + 1)$. Also, Goethals and van Tilborg [54] have proved that C is perfect if and only if (i) and (ii) hold and $a = (n - \alpha)(q - 1)/(\alpha + 1)$.

Theorem 8.4. (Goethals and van Tilborg [54]) *Let C be an α-error-correcting code. Then C is uniformly packed if and only if $C^\perp$ has exactly $\alpha + 1$ nonzero weights.* ■

Van Tilborg [55] proved that there are no uniformly packed α-error-correcting code for $\alpha \geq 4$ and the extended binary Golay code is the only binary uniformly packed 3-error-correcting code. However, many examples exist when $\alpha = 1$.

Corollary 8.5. *Let C be a 1-error-correcting code over $\mathbb{F}_q$. Then C is uniformly packed with parameters a and b if and only if $C^\perp$ is a two-weight projective code with nonzero weights w_1 and w_2 where*

$$2a = (n - 1)(q - 1) + [P(w_1) + 1][P(w_2) + 1] \text{ and}$$

$$2b = n(q - 1) + P(w_1)P(w_2)$$

with $P(x) = n(q - 1) - qx$. (If C is a uniformly packed (n, s)-linear code with parameters a and b, then the corresponding PDS as in Theorem 8.1 has parameters $(v, k, \lambda, \mu) = (q^{n-s}, n(q - 1), q - 2 + 2a, 2b)$.) ■

Example 8.6.

1. Let $D = \mathbb{F}_q^m \backslash H$ where H is an r-dimensional subspace of $\mathbb{F}_q^m$ with $1 \leq r < m$. Note that D is a trivial $(q^m, q^m - q^r, q^m - 2q^r, q^m - q^r)$-PDS in the additive group of $\mathbb{F}_q^m$ with $tD = D$ for all $t \in \mathbb{F}_q\backslash\{0\}$. We choose vectors $y_1, y_2, \ldots, y_n \in \mathbb{F}_q^m$, where $n = (q^m - q^r)/(q - 1)$, by picking one representative from each of the sets $\{ty : t \in \mathbb{F}_q\backslash\{0\}\}$, $y \in D$. Then $y_1, y_2, \ldots, y_n$ generate a two-weight (n, m)-projective code with nonzero weights q^{r-1} and $q^{m-1} - q^{r-1}$. The dual code is a uniformly packed code with parameters $a = (q^m - 2q^r - q + 2)/2$ and $b = (q^m - q^r)/2$. When $r = 1$, the uniformly packed code obtained is a shortened Hamming code, see van Lint [46].

2. Let $q_1 = q^m$ where q is a prime power. By Example 2.3(3), there exists a regular $(q_1^2, r(q_1 - 1), q_1 + r^2 - 3r, r^2 + r)$-PDS D in the additive group of $\mathbb{F}_{q_1}^2 \cong \mathbb{F}_q^{2m}$ of PCP type for each $r \leq q_1 + 1$. Note that $tD = D$ for all $t \in \mathbb{F}_q \backslash \{0\} \subset \mathbb{F}_{q_1} \backslash \{0\}$. Regarding D as a subset of $\mathbb{F}_q^{2m}$, by the same method as above, we obtain a two-weight $(r(q^m - 1)/(q - 1), 2m)$-projective code with nonzero weights $(r - 1)q^{m-1}$ and rq^{m-1}. The dual code is a uniformly packed code with parameters $a = (q^m - q + r^2 - 3r + 2)/2$ and $b = (r^2 - r)/2$.
3. Delsarte [12] has constructed a two-weight (276,11)-projective code with nonzero weights 128 and 144 obtained from the extended binary Golay code, see also Calderbank and Kantor [18]. The dual code is a uniformly packed code with parameters $a = 22$ and $b = 18$. The corresponding regular PDS has parameters $(v, k, \lambda, \mu, \beta, \Delta) = (2048, 276, 44, 36, 8, 1024)$. ■

Readers are referred to Calderbank and Kantor [56] for a list of two-weight codes. In Sections 9 and 10, we shall also study other construction methods of two-weight codes and regular PDSs. The following result is a consequence of Corollary 3.6 and Theorems 6.1, 8.1.

THEOREM 8.7. *Let q be a power of a prime p. Then a two-weight projective code in $\mathbb{F}_q^n$ has nonzero weights $w_1 = p^j t$ and $w_2 = p^j(t + 1)$ for some integers j and t.* ■

9. Projective Sets

Let q be a prime power. An (n, s, h_1, h_2)*-projective set* $\mathcal{O}$ is a proper, nonempty set of n points of the projective space $PG(s - 1, q)$ with the property that every hyperplane meets $\mathcal{O}$ in either h_1 or h_2 points. (In some articles, $\mathcal{O}$ is also called a two-intersection set in $PG(s - 1, q)$ or an *n-set of type* (h_1, h_2) in $PG(s - 1, q)$.) The complement of $\mathcal{O}$ is a $([(q^s - 1)/(q - 1)]\text{-}n, s, [(q^{s-1} - 1)/(q - 1)] - h_1, [(q^{s-1} - 1)/(q - 1)] - h_2)$-projective set. Calderbank and Kantor [18] have a detailed discussion of projective sets. In the following, for $y \in \mathbb{F}_q^s$, we use $<y>$ to denote the point $\{\lambda y : \lambda \in \mathbb{F}_q\}$ in $PG(s - 1, q)$.

PROPOSITION 9.1. (Delsarte [13]) Let $\mathcal{O} = \{<y_i> : i = 1, 2, \ldots, n\}$, where $y_i \in \mathbb{F}_q^s$, be a set of n points in $PG(s - 1, q)$. Then $\mathcal{O}$ is an (n, s, h_1, h_2)-projective set that spans $PG(s - 1, q)$ if and only if $y_1, y_2, \ldots, y_n$ generate a two-weight (n, s)-projective code with nonzero weights $w_1 = n - h_1$ and $w_2 = n - h_2$. ■

By making use of Proposition 9.1, we can construct two-weight projective codes by some known results in projective spaces. By results in Section 8, new regular PDSs are constructed.

Examples 9.2.

1. Let $\mathcal{O}$ be a *hyperoval* in $PG(2, 2^m)$ (see Hirschfeld [57]), i.e., $\mathcal{O}$ is a set of $n = 2^m + 2$ points, no three collinear, and with the property that $|L \cap \mathcal{O}| = 0$ or 2 for any line L in $PG(2, 2^m)$. There are unique examples when $m = 1$, 2 and 3 but many

different examples for larger m. The code over $\mathbb{F}_{2^m}$ obtained from $\mathcal{O}$ is a two-weight $(2^m + 2, 3)$-projective code with nonzero weights 2^m and $2^m + 2$. The corresponding regular PDS has parameters $(v, k, \lambda, \mu, \beta, \Delta) = (2^{3m}, (2^m + 2)(2^m - 1), (2^m - 1), 2^m - 2, 2^m + 2, -4, 2^{2m+2})$.

2. Let $\mathcal{O}$ be an *ovoid* in $PG(3, q)$ (see Dembrowski [58] and Hirschfeld [57]), i.e., $\mathcal{O}$ is a set of $q^2 + 1$ points, no three collinear, and with the property that $|H \cap \mathcal{O}| = 1$ or $q + 1$ for any plane H in $PG(3, q)$. The code over $\mathbb{F}_q$ obtained from $\mathcal{O}$ is a two-weight $(q^2 + 1, 4)$-projective code with nonzero weights $q^2 - q$ and q^2. The corresponding regular PDS has parameters $(v, k, \lambda, \mu, \beta, \Delta) = (q^4, r(q^2 + 1), -q^2 + r^2 + 3r, r^2 + r, -q^2 + 2r, q^4)$, where $r = q - 1$, which belongs to the negative Latin square type.
3. Let $Q : \mathbb{F}_q^{2m} \to \mathbb{F}_q$ be a nondegenerate quadratic form. By Theorem 2.6, $\mathcal{O} = \{<y> : Q(y) = 0\}$, which is called a *quadric* in $PG(2m - 1, q)$, is a projective set which gives us a two-weight $((q^m - \epsilon)(q^{m-1} + \epsilon)/(q - 1), 2m)$-projective code with nonzero weights q^{2m-2} and $q^{2m-2} + \epsilon q^{m-1}$ where $\epsilon = \pm 1$. Elliptic quadrics in $PG(3, q)$ are ovoids which is a particular case of (2), see chapter 16 of Cameron and van Lint [6]. ■

THEOREM 9.3. (Denniston [59]) *Let $Q : \mathbb{F}_{2^m}^2 \to \mathbb{F}_{2^m}$ be a quadratic form such that $Q(x) = 0$ iff $x = 0$, and let K be a subgroup of the additive group of $\mathbb{F}_q$ with 2^r elements where $1 \leq r < m$. Then $\mathcal{O} = \{<1, a, b)> : Q(a, b) \in K\}$ is a $(2^{m+r} - 2^m + 2^r, 3, 2^r, 0)$-projective set that spans $PG(2, 2^m)$.* ■

Example 9.4. The regular PDSs constructed above have parameters

$$\begin{aligned}(v, k, \lambda, \mu, \beta, \Delta) = (&2^{3m}, (2^{m+r} - 2^m + 2^r)(2^m - 1), 2^m - 2^r \\ &+ (2^{m+r} - 2^m + 2^r)(2^r - 2), (2^{m+r} - 2^m \\ &+ 2^r)(2^r - 1), -2^{m+r} + 2^{m+1} - 2^{r+1}, 2^{2m+2r}).\end{aligned}$$

When $r = 1$, this yields the PDSs in Example 9.2(1). ■

Let $q_1 = q^m$ for $m \geq 1$. Regard $\mathbb{F}_q$ as a subfield of $\mathbb{F}_{q_1}$. Let $tr : \mathbb{F}_{q_1} \to \mathbb{F}_q$ be the trace map, i.e., $tr(x) = x + x^q + \cdots + x^{q^{m-1}}$. Let V be the vector space of dimension d over $\mathbb{F}_{q_1}$ and V_0 be the same vector space but now regarded as a vector space of dimension dm over $\mathbb{F}_q$. Note that if $Q : V \to \mathbb{F}_{q_1}$ is a quadratic form on V, then $tr \circ Q$ is a quadratic form on V_0.

THEOREM 9.5. (BROUWER [60]) *Use the notation above. Let Q be a quadratic form on V such that $tr \circ Q$ is a nondegenerate quadratic form on V_0. Let $\mathcal{O} = \{<y> : y \in V_0 (= V), Q(y) \neq 0$ and $tr(Q(y)) = 0\}$ be a set of points in $PG(dm - 1, q)$. If d is even, say $d = 2t$, then $\mathcal{O}$ is a $(n, 2tm, n - w_1, n - w_2)$-projective set that spans $PG(dm - 1$, q) with*

$$n = (q^{m-1} - 1)(q^{2tm-m} - \epsilon q^{tm-m})/(q - 1),$$
$$w_1 = (q^{m-1} - 1)q^{2tm-m-1} \text{ and } w_2 = (q^{m-1} - 1)q^{2tm-m-1} - \epsilon q^{tm-1}$$

where $\epsilon = \pm 1$ and depends on the choice of Q. ■

Example 9.6.

1. If $\epsilon = 1$, then the corresponding regular PDSs have parameters $(v, k, \lambda, \mu, \beta, \Delta) = (q^{2tm}, r(q^{tm} - 1), q^{tm} + r^2 - 3r, r^2 - r, q^{tm} - 2r, q^{2tm})$, where $r = (q^{m-1} - 1)q^{tm-m}$, which belong to the Latin square type.
2. If $\epsilon = -1$, then the corresponding regular PDSs have parameters $(v, k, \lambda, \mu, \beta, \Delta) = (q^{2tm}, r(q^{tm} + 1), - q^{tm} + r^2 + 3r, r^2 + r, -q^{tm} + 2r, q^{2tm})$, where $r = (q^{m-1} - 1)q^{tm-m}$, which belong to the negative Latin square type. ■

THEOREM 9.7. (de Resmini [61], [62]) and de Resmini and Migliori [63] *$((m+q)(q^2 - q + 1), 3, m + q, m)$-projective sets in $PG(2, q^2)$ exist in each of the following cases:*

(a) *q is a square and $m = s(q + \sqrt{q} + 1) - q$ where $s = 1, 2, \ldots, q - \sqrt{q}$.*
(b) *$(q, m) = (3, 2)$ and $(4, 2)$.*

The corresponding PDSs have parameters $(v, k, \lambda, \mu, \beta, \Delta) = (q^6, r(q^3 + 1), -q^3 + r^2 + 3r, r^2 + r, -q^3 + 2r, q^6)$, where $r = (q - 1)(m + q)$, which belong to the negative Latin square type. ■

There are some other sporadic examples of projective sets, see Calderbank and Kantor [18] For example, Segre [64] and Hill [65] had studied a (56, 6, 20, 11)-projective set in $PG(5, 3)$ which gave us a (729, 112, 1, 20)-PDS.

The following are some characterization theorems of projective sets.

THEOREM 9.8. (Calderbank [56]) *Let $s \geq 3$ and $\mathcal{O}$ be an $(n, s, n - w_1, n - w_2)$-projective set in $PG(s - 1, q)$. Suppose no three points of $\mathcal{O}$ are collinear.*

(a) If $q = 2$, then either
  1. $\mathcal{O}$ is the complement of a hyperplane in $PG(s - 1, 2)$, or
  2. $\mathcal{O}$ is an ovoid in $PG(3, 2)$.

(b) If $q \neq 2$, then either
  3. q is a power of 2 and $\mathcal{O}$ is a hyperoval in $PG(2, q)$,
  4. $\mathcal{O}$ is an ovoid in $PG(3, q)$,
  5. $n(q - 1) = t(q^{s/2} + 1)$, $w_1 = tq^{(s-2)/2}$, $w_2 = (t + 1)q^{(s-2)/2}$ where t is a positive integer and $(2t + 3)^2 = 4q^{s/2} + 4q + 1$, or
  6. $2n(q - 1) = (2t + 1)q^{(s-1)/2} + (q - 2) - (t^2 + t)/q$, $w_1 = tq^{(s-3)/2}$, $w_2 = (t + 1)q^{(s-3)/2}$ where t is a positive integer and $(2t + 2q + 1)^2 = 4q^{(s+1)/2} + 4q + 1$. ■

Tzanakis and Wolfskill [66] solved the diophantine equation $x^2 = 4q^{a/2} + 4q + 1$ which appeared in (5) and (6) of Theorem 9.8 and gave us the following result.

THEOREM 9.9. (Tzanakis and Wolfskill [66]) *Let $s \geq 3$ and $\mathcal{O}$ be an $(n, s, n - w_1, n - w_2)$-projective set in $PG(s - 1, q)$. Suppose no three points of $\mathcal{O}$ are collinear. Then only the following values of k, n, w_1, w_2 are possible:*

(a) For any q, $s = 2, n = 2, w_1 = 1, w_2 = 2$;
$s = 4, n = q^2 + 1, w_1 = (q - 1)q, w_2 = q^2$.
(b) For $q = 2, n = 2^{s-1}, w_1 = 2^{s-2}, w_2 = 2^{s-1}$.
(c) For $q = 3, s = 5, n = 11, w_1 = 6, w_2 = 9$;
$s = 6, n = 56, w_1 = 1, w_2 = 2$.
(d) For $q = 4, s = 6, n = 78, w_1 = 56, w_2 = 64$;
$s = 7, n = 430, w_1 = 320, w_2 = 352$.
(e) For $q = 2^m, s = 3, n = 2^m + 2, w_1 = 2^m, w_2 = 2^m + 2$. ■

The next two theorems consider (n, s, h, i)-projective sets with a given integer i. The readers are reminded that an $(n, s, h, 0)$-projective set is the complement of a hyperplane if $s \geq 4$.

THEOREM 9.10. (Thas [67]) *If $\mathcal{O}$ is an $(n, s, h, 1)$-projective set in $PG(s - 1, q)$ where $s \geq 4$, then $\mathcal{O}$ is either a line in $PG(s - 1, q)$ or an ovoid in $PG(3, q)$.* ■

THEOREM 9.11. (Calderbank and Kantor [18]) *If $\mathcal{O}$ is an (n, s, h, i)-projective set that spans $PG(s - 1, q)$ where $i \geq 1$ and $s \geq 4$, then $s \leq (q + 1)i + 1$, $h \leq (q + 1)i$, and $h = (q + 1)i$ if and only if $\mathcal{O}$ is an ovoid in $PG(3, q)$.* ■

10. Cyclotomic Classes

In this section, we consider the construction of PDSs using cyclotomic classes in a finite field. Readers can obtain the background knowledge from Storer [68]. Let $q = p^\gamma = \alpha f + 1$ where p is a prime and let ω be a primitive element in $\mathbb{F}_q$. Then the *αth cyclotomic classes* $C_0, C_1, \ldots, C_{\alpha-1}$ are defined by

$$C_i = \{\omega^{\alpha j+i} : j = 0, 1, \ldots, f - 1\}.$$

In particular, the elements of C_0 are called the *αth power residues*. The *cyclotomic numbers* of order α are the numbers

$$(i, j)_\alpha = |\{(x, y) \in C_i \times C_j : x + 1 = y\}|$$

where $i, j = 0, 1, \ldots, \alpha - 1$. Storer [68] had listed the values of $(i, j)_\alpha$ for $\alpha = 2, 3, 4, 6$ and 8.

THEOREM 10.1. *Use the notation above. Let $I \subset \{0, 1, \ldots, \alpha - 1\}$ and $D = \bigcup_{i\in I} C_i$. If for each $m = 0, 1, \ldots, \alpha - 1$,*

$$\sum_{i,j \in I} (m - j, i - j)_\alpha = \begin{cases} \lambda & \text{if } m \in I \\ \mu & \text{if } m \notin I, \end{cases}$$

then D is a (q, k, λ, μ)-PDS in the additive group of $\mathbb{F}_q$ where $k = f|I|$. Furthermore, if f is even, then D is regular. ■

Example 10.2.

1. When $\alpha = 2$ and f is even, $(0, 0)_2 = (f - 2)/2$ and $(0, 1)_2 = f/2$. Hence the set C_0 of the 2nd power residues is a regular $(q, (q - 1)/2, (q - 5)/4, (q - 1)/4)$-PDS. This gives us the result of Theorem 2.1.
2. When $\alpha = 4$ and f is even, by the values of $(0, m)_4$ from Storer [68], we know that the set C_0 of the 4th power residues is a regular $(q, (q - 1)/4, (q - 11 - 6s)/16, (q - 3 + 2s/16)$-PDS if and only if $q = p^{2m}$ for a prime $p \equiv 3 \bmod 4$, where $s = (-p)^m$. ■

Baumert, Mills and Ward [69] has obtained an interesting result that gives us the values of the αth cyclotomic numbers when -1 is a power of the characteristic p of $\mathbb{F}_q$ modulo α.

THEOREM 10.3. (Baumert, Mills and Ward [69] *Let q be a power of a prime p and $\alpha \geq 3$ be a divisor of $q - 1$. Suppose -1 is a power of p modulo α. Then either $p = 2$ or $f = (q - 1)/\alpha$ is even; and $q = s^2$ with $s \equiv 1$ mod α such that*

$$(0, 0)_\alpha = \eta^2 - (e - 3)\eta - 1;$$

$$(0, i)_\alpha = (i, 0)_\alpha = (i, i)_\alpha = \eta^2 + \eta \text{ for } i \not\equiv 0;$$

$$(i, j)_\alpha = \eta^2 \text{ for } i, j \not\equiv 0 \text{ and } i \not\equiv j$$

where $\eta = (s - 1)/\alpha$. ■

COROLLARY 10.4. (Calderbank and Kantor [18]) *Let q be a prime power and $C_0, C_1, \ldots, C_q$ be the $(q + 1)$th cyclotomic classes in $\mathbb{F}_{q^{2m}}$. For any $I \subset \{0, 1, \ldots, q\}$, $D = \bigcup_{i \in I} C_i$ is a regular $(q^{2m}, u(q^{2m} - 1)/(q + 1), u^2\eta^2 + (3u - q - 1)\eta - 1, u^2\eta^2 + u\eta)$-PDS in the additive group of $\mathbb{F}_{q^{2m}}$ where $u = |I|$ and $\eta = [(-q)^m - 1]/(q + 1)$. Note that $\beta = (2u - q - 1)\eta - 1$ and $\Delta = q^{2m}$.* ■

Example 10.5.

1. If m is odd, say $m = 2t + 1$, then the PDSs constructed by Corollary 10.4 have parameters $(v, k, \lambda, \mu, \beta, \Delta) = (q^{4t+2}, r(q^{2t+1} - 1), q^{2t+1} + r^2 - 3r, r^2 - r, q^{2t+1} - 2r, q^{2t+1})$, where $r = u(q^{2t-1} + 1)/(q + 1)$, which belong to the Latin square type.
2. If m is even, say $m = 2t$, then the PDSs constructed by Corollary 10.4 have parameters $(v, k, \lambda, \mu, \beta, \Delta) = (q^{4t}, r(q^{2t} + 1), -q^{2t} + r^2 + 3r, r^2 + r, -q^{2t} + 2r, q^{2t})$, where $r = u(q^{2t} - 1)/(q + 1)$, which belong to the negative Latin square type. ■

Calderbank and Kantor [18] proved Corollary 10.4 directly using arguments concerning projective sets, see Section 9. Note that Example 10.2(2) is a particular case of Corollary 10.4 since the 4th power residues is a union of $(p + 1)$th cyclotomic classes when $p \equiv 3 \bmod 4$. Examples constructed by Corollary 10.4 also cover other known families of PDSs, e.g., the family found by van Lint and Schrijver [70].

The following are some PDSs constructed by using cyclotomic classes which do not belong to examples from Corollary 10.4.

Example 10.6.

1. (van Lint and Schrijver [70]) $D = C_0 \cup C_1 \cup C_3$, where the C_i are the 8th cyclotomic classes in $\mathbb{F}_{3^4}$ is a (81, 30, 9, 12)-PDS, see also Example 14.2(4).
2. (Hill [71] $D = C_0 \cup C_7$, where the C_i are the 35th cyclotomic classes in $\mathbb{F}_{2^{12}}$, is a (4096, 234, 2, 14)-PDS. ■

Other constructions of PDSs using cyclotomic classes has been reported by de Lange [72]. In particular, new PDSs are constructed with $(v, k, \lambda, \mu) = (6561, 2296, 787, 812)$, (6561, 2870, 1249, 1260), (4096, 273, 20, 28) and (4096, 1911, 950, 840). The last two are dual of each other.

11. Finite Local Rings

In Sections 8, 9 and 10, we have seen a lot of examples of PDSs in elementary abelian p-groups. Now, let us see a construction method for PDSs in abelian p-groups which are not elementary abelian. Let p be a prime and R be a finite local ring of characteristic p with its maximal ideal I generated by a prime element π. Note that R is a finite evaluation ring such that every element in R can be written as $\pi^r u$ where u is a unit in R.

Proposition 11.1. Let R, I and π be as defined above. Then

(a) $R/I \cong \mathbb{F}_{p^d}$ for some integer d;
(b) $|I^{s-1}| = p^d$ where s is the smallest positive integer such that $I^s = (\pi^s) = 0$; and
(c) if $p = \pi^t u_1$ and $s = qt + s'$, where u_1 is a unit in R and $0 \leq s' < t$, then $R \cong \mathbb{Z}_{p^{q+1}}^{ds'} \times \mathbb{Z}_{p^q}^{d(t-s')}$ as an additive group. ■

Let ϕ be a mapping from R to R such that $\phi(\pi^r u) = \pi^r u^{-1}$ where $r = 0, 1, \ldots s - 1$ and u is a unit in R. Let A be a subset of R such that $|A \cap (a + I^{s-1})| = m$ for all $a \in R$ where m is a positive integer less than p^d. Such a subset A of R can always be found since $\{a + I^{s-1} : a \in R\}$ is a partition of R with $|a + I^{s-1}| = p^d$ for every $a \in R$.

THEOREM 11.2. (Leung and Ma [73]) *Using the notation above,*

$$D = \{(a, b) \in R \times R : \phi(a)b \in A\}$$

is a PDS in the additive group of $R \times R$ with parameters

$$(v, k, \lambda, \mu, \beta, \Delta) = \begin{cases} (n^2, r(n-1), n+r^2-3r, r^2-r, n-2r, n^2) & \text{if } 0 \notin A \\ (n^2, n+r(n-1), n+r^2-r, r^2+r, n-2r, n^2) & \text{if } 0 \in A, \end{cases}$$

where $n = p^{sd}$ and $r = mp^{(s-1)d}$. ■

When $0 \notin A$, the PDSs constructed above are regular and they belong to the Latin square type.

Example 11.3.

1. Let $R = \mathbb{Z}_9$. Then $I = (3)$, $R/I \cong \mathbb{F}_3$ and $I^2 = (0)$, i.e., $d = 1$ and $s = 2$. Since $I^{s-1} = I = \{0, 3, 6\}$. $A = \{1, 2, 3\}$ satisfies the required condition with $m = 1$. Note that
$$\begin{aligned} \phi(a)b = 1 &\Leftrightarrow (a, b) \in S_1 = \{(1, 1), (2, 2), (4, 4), (5, 5), (7, 7), (8, 8)\}; \\ \phi(a)b = 2 &\Leftrightarrow (a, b) \in S_2 = \{(1, 2), (2, 4), (4, 8), (5, 1), (7, 5), (8, 7)\}; \\ \phi(a)b = 3 &\Leftrightarrow (a, b) \in S_3 = \{(1, 3), (2, 6), (3, 1), (3, 4), (3, 7), (4, 3), \\ &\qquad (5, 6), (6, 2), (6, 5), (6, 8), (7, 3), (8, 6)\}. \end{aligned}$$
Then $D = S_1 \cup S_2 \cup S_3$ is a regular (81, 24, 9, 6)-PDS in $\mathbb{Z}_9 \times \mathbb{Z}_9$.
2. Let $R = \mathbb{Z}_4[\xi]/(2\xi) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{\xi}, \overline{1+\xi}, \overline{2+\xi}, \overline{3+\xi}\}$ where $\xi^2 = 2$. Then $I = (\xi)$, $R/I \cong \mathbb{F}_2$ and $I^3 = (\overline{0})$, i.e., $d = 1$ and $s = 3$. Since $I^{s-1} = I^2 = \{\overline{0}, \overline{2}\}$, the subset $A = \{\overline{2}, \overline{3}, \overline{2+\xi}, \overline{3+\xi}\}$ satisfies the required condition with $m = 1$. Note that
$$\begin{aligned} \phi(a)b = \overline{2} &\Leftrightarrow (a, b) \in S_1 = \{(\overline{1}, \overline{2}), (\overline{2}, \overline{1}), (\overline{2}, \overline{3}), (\overline{2}, \overline{1+\xi}), (\overline{2}, \overline{3+\xi}), \\ &\qquad (\overline{3}, \overline{2}), (\overline{\xi}, \overline{\xi}), (\overline{\xi}, \overline{2+\xi}), (\overline{1+\xi}, \overline{2})\ (\overline{2+\xi}, \overline{\xi}), \\ &\qquad (\overline{2+\xi}, \overline{2+\xi}), (\overline{3+\xi}, \overline{2})\}; \\ \phi(a)b = \overline{3} &\Leftrightarrow (a, b) \in S_2 = \{(\overline{1}, \overline{3}), (\overline{3}, \overline{1}), (\overline{1+\xi}, \overline{3+\xi}), (\overline{3+\xi}, \overline{1+\xi})\}; \\ \phi(a)b = \overline{2+\xi} &\Leftrightarrow (a, b) \in S_3 = \{(\overline{1}, \overline{2+\xi}), (\overline{3}, \overline{2+\xi}), (\overline{\xi}, \overline{1+\xi}), (\overline{\xi}, \overline{3+\xi}); \\ &\qquad (\overline{1+\xi}, \overline{\xi}), (\overline{2+\xi}, \overline{1}), (\overline{2+\xi}, \overline{3}), (\overline{3+\xi}, \overline{\xi})\}; \\ \phi(a)b = \overline{3+\xi} &\Leftrightarrow (a, b) \in S_4 = \{(\overline{1}, \overline{3+\xi}), (\overline{3}, \overline{1+\xi}), (\overline{1+\xi}, \overline{1}), (\overline{3+\xi}, \overline{3})\}; \end{aligned}$$
Then $D = S_1 \cup S_2 \cup S_3 \cup S_4$ is a regular (64, 28, 12, 12)-PDS in $(R \times R, +) \cong (\mathbb{Z}_4 \times \mathbb{Z}_2) \times (\mathbb{Z}_4 \times \mathbb{Z}_2)$. ■

Dillon [74] proved a special case of Theorem 11.2 when $R = \mathbb{Z}_{2^s}$ and $m = 1$. The PDSs in this case have parameters $(v, k, \lambda, \mu) = (2^{2s}, 2^{2s-1} \pm 2^{s-1}, 2^{2s-2} \pm 2^{s-1}, 2^{2s-2} \pm 2^{s-1})$ and hence each of them is a reversible difference set in $\mathbb{Z}_{2^s} \times \mathbb{Z}_{2^s}$, see Example 12.4(3).

Let C be a regular $(p^4, mp(p^2 - 1), p^2 + mp^2 - 3mp, (mp)^2 - mp)$-PDS in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, where $1 \leq m \leq p - 1$, obtained by Theorem 11.2. We can always find a $(p^4, t(p^2 - 1), p^2 + t^2 - 3t, t^2 - t)$-PDS E of PCP type in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ (see Theorem 2.2), where $1 \leq t \leq p + 1$, such that $C \cap E = \emptyset$ and $D = C \cup E$ is a PDS:

THEOREM 11.4. (Davis [43]) *There exists a regular* $(p^4, r(p^2-1), p^2+r^2-3r, r^2-r)$-*PDS in* $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, *where* $r = t + mp$, $1 \le t \le p+1$ *and* $1 \le m \le p-1$.

As pointed out by Davis [43], other PDSs in the additive groups of $R \times R$ can be constructed in a similar manner.

12. Reversible Difference Sets

Let G be a group of order v and D a subset of G with k elements. Then D is called a (v, k, λ)-*difference set* in G if the expressions gh^{-1}, for g and h in D with $g \neq h$, represent each nonidentity element in G exactly λ times, i.e.,

$$\bar{D}\,\bar{D}^{(-1)} = \lambda\bar{G} + ne \tag{12.1}$$

where $n = k - \lambda$ is called the *order* of D. Note that D is a (v, k, λ)-difference set if and only if D is a (v, k, λ, λ)-PDS. Difference sets are well-known combinatorial configurations and have applications in various fields of studies. For detailed descriptions of difference sets, please consult Beth, Jungnickel and Lenz [20] and Lander [21]. Jungnickel [22] has a survey of the recent development.

Let D be a difference set in a group G. Then D is called *reversible* if $D^{(-1)} = D$. A reversible difference set D with $e \notin D$ is a regular PDS. Here, $\beta = 0$ and $\Delta = 4n$. A lot of work has been done on this topic, especially when G is abelian (see Jungnickel [22]).

First, we examine some nonexistence results on abelian reversible difference sets.

THEOREM 12.1. *Let D be a nontrivial reversible* (v, k, λ)-*difference set in an abelian group G. Then one has the following results:*

(a) *v is a multiple of 4, λ is even and n is a square.*
(b) *v and n have the same odd prime divisors.*
(c) *If p is a prime divisor of n such that $p^{2r}|n$, then $p^r|k$, $p^r|\lambda$ and $p^{r+1}|v$.*
(d) $D^{(t)} = D$ *for any integer t relatively prime to v.* ■

Theorem 12.1(a) was first proved by Johnsen [75]. Theorem 12.1(b), a particular case of Theorem 6.1., was given by Ghinelli [76] in terms of difference sets. Theorem 12.1(c) was independently proved by Jungnickel [77] and Lander [21]. Finally, Theorem 12.1(d) follows from Theorem 4.1 and n is a square. All these results are well-known and various proofs are provided in the literature, e.g., see McFarland and Ma [78].

By Theorem 12.1, we can set $n = u^2$, $\lambda = ua$, $k = ub$ and $v = uc$ for some integers a, b, c. Substitute into the parameter relations $n = k - \lambda$ and $k^2 = \lambda v + n$. We obtain the following corollary.

COROLLARY 12.2. (Johnsen [75]) *Suppose a nontrivial reversible* (v, k, λ)-*difference set exists in an abelian group. Then*

$$(v, k, \lambda, n) = (u(u + \alpha - 1)(u + \alpha + 1)/\alpha, u(u + \alpha), u\alpha, u^2)$$

where α, u are positive integers of opposite parity and α is a divisor of $u^2 - 1$. ■

As a consequence of Theorem 7.1, we have a result on subsets of reversible difference sets.

THEOREM 12.3. *Suppose there exists a nontrivial reversible difference set of order n in an abelian group G; and let N be a subgroup of G such that g.c.d.$(|N|, |G|/|N|) = 1$ and $|N|$ is even. Then there exists a reversible difference set in N of order n_1 = g.c.d.$(|N|^2, n)$.* ■

Theorem 12.3 was first proved by McFarland [79] for abelian reversible difference sets with parameters $(v, k, \lambda) = (4u^2, 2u^2 - u, u^2 - u)$, u $\in \mathbb{Z}$. Later, Ma [80] generalized it to all abelian reversible difference sets. Now, let us see some examples of abelian reversible difference sets.

Example 12.4.

1. Let $G = \mathbb{Z}_2^2$ or $\mathbb{Z}_4$. Then $D = \{x\}$, where $x \in G$ with $2x = 0$, is a reversible (4, 1, 0)-difference set and $G \backslash D$ is a reversible (4, 3, 2)-difference set.
2. Let $G = \mathbb{Z}_6^2 \cong \mathbb{Z}_2^2 \times \mathbb{Z}_3^2$. By example 2.3(2), $D = \{(x, 0), (0, x), (x, x) : x = 1, 2, 3, 4, 5\}$ is a reversible (36, 15, 6)-difference set and $G \backslash D$ is a reversible (36, 21, 12)-difference set.
3. In Theorem 11.2, if $p = 2$ and $m = 2^{d-1}$, then D is a reversible $(2^{2sd}, 2^{2sd-1} \pm 2^{sd-1}, 2^{2sd-2} \pm 2^{sd-1})$-difference set in the additive group of $R \times R$. In particular, there exist reversible $(2^{2s}, 2^{2s-1} \pm 2^{s-1}, 2^{2s-2} + 2^{s-1})$-difference sets in $\mathbb{Z}_{2^s}^2$.
4. The set D in Example 2.8 is a reversible (4000, 775, 150)-difference set in $G \cong \mathbb{Z}_2^5 \times \mathbb{Z}_5^3$ and $G \backslash D$ is a reversible (4000, 3225, 2600)-difference set. ■

Note that Example 12.4(1), (2) and (3) have parameters of the form $(v, k, \lambda) = (4u^2, 2u^2 - u, \mathrm{u}^2 - u)$ where u is an integer. A difference set with these parameters is called a *Menon difference set* (in some literature, it is called a *Hadamard difference set.*)

For Menon difference sets, we have further construction methods.

THEOREM 12.5. (Xia [81]) *Let p be a prime such that $p \equiv 3 \bmod 4$; $q = p^{2r} = 4m + 1$ and $q^2 = \alpha f + 1$ where $\alpha = 8m + 4$ and $f = 2m$. Let ω be a primitive element in $\mathbb{F}_{q^2}$ and $C_i = \{\omega^{\alpha j + 1} : j = 0, 1, \ldots, f - 1\}$, $i = 0, 1, \ldots, \alpha - 1$, be the αth cyclotomic classes. Let G be the additive group of $\mathbb{F}_{q^2}$; $K = \{g_1, g_2, g_3, g_4\}$ be a Klein four group and*

$$D = (g_1, G \backslash E) \cup (g_2, \omega^{\alpha/4}E) \cup (g_3, \omega^{\alpha/2}E) \cup (g_4, \omega^{3\alpha/4}E),$$

where

$$E = \left[\bigcup_{i=0}^{2m} C_{4i+2}\right] \cup \left[\bigcup_{i=0}^{m-1} C_{4i+(2m+1)}\right] \cup \left[\bigcup_{i=0}^{m-1} C_{4i+(6m+3)}\right].$$

Then D is a reversible $(4q^2, 2q^2 - q, q^2 - q)$-difference set in $K \times G$. ■

THEOREM 12.6. (Menon [82]) *Let D_1 and D_2 be reversible Menon difference sets in groups G_1 and G_2, respectively. Then*

$$D = (D_1 \times D_2) \cup (G_1 \backslash D_1 \times G_2 \backslash D_2)$$

is a reversible Menon difference set in the group $G = G_1 \times G_2$. ■

THEOREM 12.7. (Turyn [83]) *Let $K = \{g_1, g_2, g_3, g_4\}$ be a Klein four group. Let $D_1 = \bigcup_{i=1}^{4} (g_i, A_i)$* and *$D_2 = \bigcup_{i=1}^{4} (g_i, B_i)$ be reversible Menon difference sets in groups $G_1 = K \times H_1$ and $G_2 = K \times H_2$, respectively, where $A_i \subset H_1$ and $B_i \subset H_2$. Define*

$$D = (g_1, \nabla(A_1, A_2; B_1, B_2)) \cup (g_2, \nabla(A_1, A_2; B_3, B_4)) \cup$$
$$(g_3, \nabla(A_3, A_4; B_1, B_2)) \cup (g_4, \nabla(A_3, A_4; B_3, B_4))$$

where

$$\nabla(W, X; Y, Z) = [(W \cap X) \times Y] \cup [(W' \cap X') \times Y']$$
$$\cup [(W \cap X') \times Z] \cup [(W' \cap X) \times Z']$$

with $W' = H_1 \backslash W$, $X' = H_1 \backslash X$, $Y' = H_2 \backslash Y$ and $Z' = H_2 \backslash Z$. Then D is a reversible Menon difference set in the group $G = K \times H_1 \times H_2$. ■

Example 12.8. By applying Theorems 12.6 and 12.7 to Example 12.4(1), (2), (3) and Theorem 12.5, reversible $(4u^2, 2u^2 - u, u^2 - u)$-difference sets are constructed in abelian groups

$$G = \mathbb{Z}_2^{2a} \times \mathbb{Z}_4^b \times \left(\mathbb{Z}_{2^{q_1}}^{2c_1} \times \cdots \times \mathbb{Z}_{2^{q_s}}^{2c_s}\right) \times \mathbb{Z}_3^{2d} \times \left(\mathbb{Z}_{p_1}^{4\alpha_1} \times \cdots \times \mathbb{Z}_{p_t}^{4\alpha_t}\right)$$

with $u = \pm 2^{a+b+c_1+\cdots+c_s-1} \cdot 3^d \cdot p_1^{2\alpha_1} \ldots p_t^{2\alpha_t}$, where $p_i \equiv 3 \bmod 4$ are primes; a, b, c_i, d, α_i, s, t are nonnegative integers; and if $d + \alpha_1 + \cdots + \alpha_t > 0$, then $a > 0$. Let D be such a reversible difference set. It can be checked that there exists elements x and y in G such that $2x = 2y = 0$ and $x \in D$ while $y \notin D$. Hence $D + y$ is an abelian regular $(4u^2, 2u^2 - u, u^2 - u, u^2 - u)$-PDS in G and $(D + x)\backslash\{0\}$ is an abelian regular $(4u^2, 2u^2 - u - 1, u^2 - u - 2, u^2 - u)$-PDS. Note that a $(4u^2, 2u^2 - u$, u$^2 - u, u^2 - u)$-PDS belongs to the Latin square type if $u > 0$ and belongs to the negative Latin square type if $u < 0$. ■

The following is a restriction on the parameters of an abelian reversible Menon difference set. Readers can compare it with Theorem 7.3(c).

THEOREM 12.9. (McFarland [79]) *If the square free part of u is not equal to $\pm 2^a 3^b$, then no reversible $(4u^2, 2u^2 - u, u^2 - u)$-difference set exists in any abelian group of order $4u^2$.* ■

With Example 12.8, it is natural to ask the following question.

Question 12.10. If u has a prime factor $p \equiv 1 \bmod 4$, does there exist a reversible $(4u^2, 2u^2 - u, u^2 - u)$-difference set in any abelian group of order $4u^2$? In particular, does there exist a reversible $(4p^4, 2p^4 \pm p^2, p^4 + p^2)$-difference set in any abelian group of order $4p^4$ if $p \equiv 1 \bmod 4$ is a prime? ■

We have a theorem on the structure of the groups.

THEOREM 12.11. (Ma [42]) *Suppose G is an abelian group which contains a reversible Menon difference set. Let q be the exponent of the Sylow p-subgroup P of G. If $q \neq 4$, then P contains a subgroup isomorphic to $\mathbb{Z}_q \times \mathbb{Z}_q$.* ■

For non-Menon type reversible difference sets, Example 12.4(4) is the only known nontrivial abelian example. The following is the McFarland Conjecture, see Arasu [84] or Jungnickel [22].

CONJECTURE 12.12. If a nontrivial reversible difference set of order n exists in an abelian group of order v, then either $v = 4n$ or $v = 4000$, $n = 625$. (When $v = 4n$, the difference set belongs to the Menon type.) ■

McFarland and Ma [78] and Ma [80] have shown that Conjecture 12.12 is valid for $n \leq 10^8$. By a result by Mann [85], all nontrivial difference sets in abelian 2-groups belong to the Menon type. Together with Theorem 12.3, we have the following theorem.

THEOREM 12.13. (Ma [80]) *Suppose there exists a nontrivial reversible difference set of order n in an abelian group of order v. If 2^{2a} strictly divides n, then either $a = 0$ or 2^{2a+2} strictly divides v.* ■

By applying Theorems 12.1 and 12.13 to the case when v has only one odd prime divisor and using the observation that $v^2 + 4n(v - 1)$ is a square, Ma [80] proposed the following conjecture which implies Conjecture 12.12.

CONJECTURE 12.14. Let p be an odd prime, $a \geq 0$ and $b, t, r \geq 1$. Then

(i) $Y = 2^{2a+2}p^{2t} - 2^{2a+2}p^{t+r} + 1$ is a square if and only if $t = r$ (i.e., $Y = 1$);
(ii) $Z = 2^{2b+2}p^{2t} - 2^{b+2}p^{t+r} + 1$ is a square if and only if $p = 5$, $b = 3$, $t = 1$, $r = 2$ (i.e., $Z = 2401$). ■

For Case (i) of Conjecture 12.14, $Y = 1$ corresponds to the parameters of the Menon type. For Case (ii), $Z = 2401$ yields the parameters of Example 12.4(4).

It is interesting to see that the nonabelian case is completely different from the abelian case. For example, we have a reversible $(4u^2, 2u^2 - u, u^2 - u)$-difference set for $u = 5$ which violates Theorem 12.9.

Example 12.15. (Smith [86]) Let

$$G = < a, b, c : a^5 = b^5 = c^4 = [a, b] = cac^{-1}a^{-2} = cbc^{-1}b^{-2} = e >.$$

Then

$$\begin{aligned}\bar{D} = {} & [(e + a + a^4) + (e + a)b + (e + a^2 + a^3 + a^4)b^2 + \\ & \qquad (e + a + a^2 + a^3)b^3 + (e + a^4)b^4] + \\ & [(a^2 + a^4) + a^4b + a^3b^2 + (e + a^2)b^3 + (a + a^2 + a^3 + a^4)b^4]c + \\ & [a^4 + (a + a^2 + a^4)b + (a + a^4)b^2 + (e + a^2 + a^4)b^3 + a^3b^4]c^2 + \\ & [(a^3 + a^4) + (e + a^4)b + a^3b^2 + (a + a^2 + a^3 + a^4)b^3 + ab^4]c^3\end{aligned}$$

is a reversible (100, 45, 20)-difference set in G and $G\setminus D$ is a reversible (100, 65, 30)-difference set. ■

Also, we have a family of non-Menon type reversible difference sets which do not agree with Theorem 12.1.

THEOREM 12.16. (Miyamoto [87] and Ma [88]) *Let E be the additive group of $\mathbb{F}_{3^{s+1}}$. Suppose 2^t strictly divides $(3^{s+1} - 1)/2$. Let M be an elementary abelian 2-group of order 2^t and K be the cyclic subgroup of the multiplicative group of order $(3^{s+1} - 1)/2^{t+1}$ in $\mathbb{F}_{3^{s+1}}\setminus\{0\}$. Define $G = \{(x, y, z) : x \in M, y \in E \text{ and } z \in K\}$ to be a group with the operation $(x_1, y_1, z_1)(x_2, y_2, z_2) = (x_1x_2, y_1 + z_1y_2, z_1z_2)$ for all $(x_1, y_1, z_1), (x_2, y_2, z_2) \in G$. Let $H_1, H_2, \ldots, H_{2^t}$ be hyperplanes in $\mathbb{F}_{3^{s+1}}$ such that for $i \neq j$, $H_i \neq gH_j$ for all $g \in K$. Let $M = \{h_1, h_2, \ldots, h_w\}$ and $K = \{g_1, g_2, \ldots, g_r\}$ where $w = 2^t$ and $r = (3^{s+1} - 1)/2^{t+1}$. Then*

$$D = (h_1, E\setminus H_1, e) \cup \left[\bigcup_{\substack{i=1,2,\ldots,r \\ j=1,2,\ldots,w \\ (i,j)\neq(1,1)}} (h_j, g_iH_j, g_i^2) \right]$$

is a reversible $(3^{s+1}(3^{s+1} - 1)/2,\ 3^s(3^{s+1} + 1)/2,\ 3^s(3^s + 1)/2)$-difference set in G. ■

Finally, we conclude this section with a generalization of some of the results in theorem 12.1 to the nonabelian case.

THEOREM 12.17. (Ghinelli [89]) *Let D be a reversible (v, k, λ)-difference set in a finite group G. Then*

(a) n $(= k - \lambda)$ *is a square, say* $n = m^2$;
(b) $v \equiv k \equiv \lambda$ *mod* m; *and*
(c) *for every* $g \in G$, $|C_G(g)||D \cap g^G| \equiv k$ *mod* m *where* $C_G(g)$ *and* g^G *denote the centralizer of* g *in* G *and the conjugacy class of* g, *respectively.* ■

13. The Case When $\lambda - \mu = -1$

In Section 12, we have seen PDSs with $\lambda - \mu = 0$ and -2. It is natural to ask what will happen if $\lambda - \mu = -1$. In fact, this kind of PDSs is closely related to certain types of divisible difference sets which we shall discuss later in this section. By using Theorems 7.1, 7.3(c) and some results concerning diophantine equations, we have the following characterization of abelian regular PDSs with $\lambda - \mu = -1$.

THEOREM 13.1. (Arasu, Jungnickel, Ma and Pott [90]) *The following are all possible parameters for a nontrivial abelian regular* (v, k, λ, μ)-*PDS* D *to exist with* $\lambda - \mu = -1$:

(a) $(v, k, \lambda, \mu) = (v, (v - 1)/2, (v - 5)/4, (v - 1)/4)$ *where* $v \equiv 1$ *mod* 4;
(b) $(v, k, \lambda, \mu) = (243, 22, 1, 2)$ *or* $(243, 220, 199, 220)$. ■

As to existence, Theorem 2.1 gives us regular $(v, (v - 1)/2, (v - 5)/4, (v - 1)/4)$-PDSs when $v \equiv 1$ mod 4 is a power of an odd prime. Also, Example 8.3(2) yields regular (243, 22, 1, 2) and (243, 220, 199, 200)-PDSs.

Let G be a group of order mn with a normal subgroup N of order n. An $(m, n, k, \lambda_1, \lambda_2)$-*divisible difference set* in G with respect to N is a k-element subset B of G such that the expressions gh^{-1}, for g and h in B with $g \neq h$, represent each nonidentity element in N exactly λ_1 times and each element in $G \backslash N$ exactly λ_2 times. It is known that a divisible difference set is equivalent to a symmetric divisible design that admits a normal Singer group, see Jungnickel [91]. An $(m, n, k, \lambda_1, \lambda_2)$-divisible difference set is called *proper* if $\lambda_1 \neq \lambda_2$, $m \neq 1$, $n \neq 1$ and $\lambda_2 \neq 0$, $2k - mn$. A divisible difference set B is called *reversible* if $B^{(-1)} = B$. Two divisible difference sets B_1 and B_2 are called *equivalent* if $B_1 = gB_2$ for some $g \in G$.

Divisible difference sets satisfying $k - \lambda_1 = 1$ were investigated by Arasu, Jungnickel and Pott [92], [93]. In particular, they showed that any proper abelian divisible difference set with $k - \lambda_1 = 1$ is either reversible or has (up to complementation and equivalence) parameters

$$(m, n, k, \lambda_1, \lambda_2) = \left(q, n, n\left(\frac{q-1}{2}\right) + 1, n\left(\frac{q-1}{2}\right), n\left(\frac{q-3}{4}\right) + 1\right)$$

where $q \equiv 3$ mod 4 is a prime power. One can construct examples for the parameters in the latter case for all values of n and q, see Arasu, Jungnickel and Pott [93]. For the reversible case, the existence question reduces to that for abelian regular PDSs.

Theorem 13.2. (Arasu, Jungnickel and Pott [92]) *Let G be an abelian group with a subgroup N of order 2, let $H = G/N$ and ρ be the natural epimorphism from G to H. If D is a regular $(m, h, \lambda, \lambda - 1)$-PDS in H, then $B = \rho^{-1}(D) \cup \{e\}$ is a proper reversible $(m, 2, 2h + 1, 2h, 2\lambda)$-divisible difference set in G with respect to N. Moreover, up to complementation and equivalence, every proper reversible divisible difference set with $k - \lambda_1 = 1$ arises in this way.* ■

As a consequence of Theorems 13.1 and 13.2, we have the following corollary.

Corollary 13.3 *Suppose there exists a proper $(m, n, k, \lambda_1, \lambda_2)$-divisible difference set in an abelian group G with $k - \lambda_1 = 1$. Up to complementation and equivalence, one of the following cases is true:*

(a) B is reversible and $(m, n, k, \lambda_1, \lambda_2) = (243, 2, 45, 44, 4)$ *or* $(m, 2, m, m - 1, (m - 1)/2)$ *where* $m \equiv 1 \bmod 4$.
(b) $(m, n, k, \lambda_1, \lambda_2) = (q, n, [n(q - 1)/2] + 1, n(q - 1)/2, [n(q - 3)/4] + 1)$ *where* $q \equiv 3$ *mod* 4 *is a prime power.* ■

In the following a regular $(v, (v - 1)/2, (v - 5)/4, (v - 1)/4)$-PDS, where $v \equiv 1 \bmod 4$, is called a *Paley* PDS. Arasu, Jungnickel, Ma and Pott [90] have asked the following questions.

Questions 13.4. Suppose G is an abelian group of order $v \equiv 1 \bmod 4$. If v is not a prime power, does there exist a Paley PDS in G? If v is a prime power, does G need to be elementary abelian? ■

The first question is still open. However, we have counter examples for the second question. By Theorem 11.4, if we put $t = m = (p - 1)/2$, then we obtain a Paley PDS in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$. Recently, with a similar but more complicated construction, Leung and Ma [94] obtained examples of Paley PDSs in some abelian groups of higher exponent.

There is an exponent bound for an abelian group to have a Paley PDS. If $v = p^{2s}$ or p^{2s+1} for some odd prime p, then by Theorems 6.7 and 6.9, except the case $v = p$ (i.e., $G \cong \mathbb{Z}_p$), the exponent of G cannot exceed p^s.

14. Partial Geometries

A *partial geometry* with parameters s, t, α (a $pg(s + 1, t + 1, \alpha)$) is an incidence structure having the following properties:

(i) every line has $s + 1$ points and every point lies on $t + 1$ lines;
(ii) any two lines intersect at most one point (and any two points are incident with at most one line);
(iii) if a point x is not on a line L, then there are α lines through x which intersect L.

Partial geometries were introduced by Bose [1] in order to provide a setting and generalization for known characterization theorems for strongly regular graphs. There are several surveys on partial geometries, e.g., see Thas [95], Brouwer and van Lint [5] and Cameron and van Lint [6].

Suppose we have a $pg(s+1, t+1, \alpha)$ with a regular automorphism group G acting regularly on the points and we identify the points with the elements of G. Let L_0, L_1, $\ldots$, L_t be the $t+1$ lines through e, the identity element in G. Then $\{gL_i : g \in G$ and $i = 0, 1, \ldots, t\}$ is the set of all lines and for any $g \in G$, $gL_0, gL_1, \ldots, gL_t$ are the $t+1$ lines through g. By the axioms of partial geometries, we have

$$|L_i| = s + 1 \text{ for } i = 0, 1, \ldots, t; \tag{14.1}$$

$$|L_i \cap gL_j| \leq 1 \text{ if } L_i \neq gL_j; \text{ and} \tag{14.2}$$

$$\left| \left(\bigcup_{i=0}^{t} L_i \right) \cap gL_j \right| = \alpha \text{ if } g^{-1} \notin L_j. \tag{14.3}$$

THEOREM 14.1. *With the notation above, $D = (\bigcup_{i=0}^{t} L_i)\backslash\{e\}$ is a regular PDS with parameters*

$$(v, k, \lambda, \mu, \beta, \Delta) = ((s+1)(\alpha+st)/\alpha, s(t+1), s+t(\alpha-1)-1, \alpha(t-1),$$
$$s-\alpha-t-1, (s-\alpha+t+1)^2).$$

Furthermore,

$$\bar{L}_i\bar{D} = \alpha\bar{G} + (s-\alpha)\bar{L}_i \text{ for } i = 0, 1, \ldots, t. \tag{14.4}$$

■

Example 14.2

1. The projective plane $PG(2, q)$, where q is a prime power, is a $pg(q+1, q+1, q+1)$ which gives us the trivial PDS $D = G\backslash\{e\}$ where G is the cyclic Singer group of $PG(2, q)$, see Baumert [96].
2. Let G be a group of order n^2 and $\mathcal{P}$ be an (n, r)-*PCP*, see Section 2. Let the elements in G be points and gU, $U \in \mathcal{P}$ and $g \in G$, be lines. Then we obtain a $pg(n, r, r-1)$. Note that a partial geometry with $\alpha = t$ is called a *net*. Lines of a net can be partitioned into parallel classes, see Chapter 7 of Cameron and van Lint [6]. A net with an automorphism group acting regularly on the points and fixing each parallel class is called a *translation net*, see Jungnickel [26] and Bailey and Jungnickel [25]. Sprague [24] has shown that all translation nets are obtained from PCPs.
3. Let G be a group of order n^2, N be a normal subgroup of order n in G and R be an $(n, n, n, 1)$-relative difference set in G relative to N, see Jungnickel [91]. A $pg(n, n, n-1)$ can be obtained by regarding the elements of G as points and gR, $g \in G$, as

lines. It is a net but the action of G does not fix any parallel class. The corresponding PDS is $D = G\backslash N$. Furthermore, if a parallel class of lines, $\{gN : g \in G\}$, is added, we get an affine plane which is a $pg(n, n+1, n)$.

4. (van Lint and Schrijver [70]) Let γ be a primitive 5th root of unity in $\mathbb{F}_{3^4}$ and $S = \{0, 1, \gamma, \gamma^2, \gamma^3, \gamma^4\}$. Let the elements in $\mathbb{F}_{3^4}$ be points and $S + b$, $b \in \mathbb{F}_{3^4}$, be lines. Then we obtain a $pg(6, 6, 2)$. The PDS constructed is the regular (81, 30, 9, 12)-PDS of Example 10.6(1). ■

Using projective sets in Section 9, we can construct partial geometries which have regular automorphism groups acting regularly on the points, see Chapter 7 of Cameron and van Lint [6].

THEOREM 14.3. *Let $\mathcal{O}$ be an $(n, 3, h, 0)$-projective set in $PG(2, q)$. Let the elements in $\mathbb{F}_q^3$ be points and $\{\lambda y : \lambda \in \mathbb{F}_q\} + x$, $\langle y \rangle \in \mathcal{O}$ and $x \in \mathbb{F}_q^3$, be lines. Then the incidence structure is a $pg(q, n, h-1)$.* (Note that $n = (q+1)(h-1)+1$.) ■

Example 14.4. By Theorem 9.3, for $1 \le r < m$, there exists a $(2^{m+r} - 2^m + 2^r, 3, 2^r, 0)$-projective set in $PG(2, 2^m)$. Hence there exists a $pg(2^m, 2^{m+r} - 2^m + 2^r, 2^r - 1)$ such that the additive group of $\mathbb{F}_{2^m}^3$ acts regularly on the points. The PDS constructed from the partial geometry is exactly the same as the PDS constructed from the projective set, see Example 9.4. ■

Recently, Ma [97] has obtained the following result for the case when $s = t$ and G is abelian.

THEOREM 14.5. (Ma [97]) *Suppose $L_0, L_1, \ldots, L_s$ be distinct subsets of an abelian group G such that $|L_i| = s + 1$ and $e \in L_i$ for all i. If a $pg(s+1, s+1, \alpha)$ is obtained by regarding the elements of G as points and gL_i, $0 \le i \le s$ and $g \in G$, as lines, then*

(a) *either $L_i^{(-1)} = L_i$ for all i or $L_i \cap L_i^{(-1)} = \{e\}$ for all i;*
(b) *if $L_i^{(-1)} = L_i$ for all i, then $\alpha = s$ and the partial geometry is a translation net (see Example* 14.2(2)); *and*
(c) *if $L_i \cap L_i^{(-1)} = \{e\}$ for all i, then $\{g^{-1}L_0 : g \in G\} = \{L_0, L_1, \ldots, L_s\}$ and*

$$\bar{L}_0\bar{L}_0^{(-1)} = \bar{D} + (s+1)e \tag{14.5}$$

and

$$\bar{L}_0^2\bar{L}_0^{(-1)} = \alpha\bar{G} + (2s - \alpha + 1)\bar{L}_0 \tag{14.6}$$

where $D = (\cup_{i=0}^{s} L_i)\backslash\{e\}$ (see Example 14.2(1), (3) *and* (4)). ■

Furthermore, Ma [97] has conjectured the following and proved that it is true for $s \le 500$.

CONJECTURE 14.6. If a $pg(s+1, s+1, \alpha)$ admits an abelian automorphism groups acting regularly on the points, then $(s, \alpha) = (s, s+1)$, (s, s) or $(5, 2)$. ■

A $pg(s+1, t+1, \alpha)$ with $\alpha = 1$ is called a *generalized quadrangle* of order s and t (*a* $GQ(s, t)$). There is an extensive literature on generalized quadrangles, see Payne and Thas [98]. In Example 14.4, if $r = 1$, then we have a $GQ(2^m - 1, 2^m + 1)$ such that the additive group of $\mathbb{F}_{2^m}^3$ acts regularly on the points. Löwe [99] has constructed some examples of $GQ(q-1, q+1)$ admitting regular automorphism groups for odd prime power q.

For $s = t$, Ghinelli [89] has studied the existence problem in detail. The only known example is the $GQ(1, 1)$ obtained from Example 14.2(3) with $n = r = 2$.

CONJECTURE 14.7. A $GQ(s, s)$ with $s > 1$ does not admit a regular automorphism group acting regularly on the points. ■

Suppose there is a $GQ(s, s)$ which has an automorphism group G acting regularly on the points. By Theorem 14.1, we get a regular $((s+1)(s^2+1), s^2+s, s-1, s+1)$-*PDS* D. Then $D \cup \{e\}$ is a reversible $((s+1)(s^2+1), s^2+s+1, s+1)$-difference set in G. Note that if $s > 1$, then G must be nonabelian. The following theorem is obtained by studying this nonabelian reversible difference set, see also Theorem 12.17.

THEOREM 14.8. (Ghinelli [89]) *Suppose s is even. In each of the following cases, a group G of order $(s+1)(s^2+1)$ cannot be a regular automorphism group of a $GQ(s, s)$.*

(a) *G has a nontrivial center.*
(b) *G is a Frobenius group.*
(c) *s^2+1 is square-free.* ■

Ghinelli [89] has also pointed out that if s is odd, then the problem is more difficult since G may not be solvable. For this case, the Suzuki groups and the Sylow 3-subgroups of line stabilizers will play an important role.

15. A Table of Parameters

In table 15.3, we give a list of possible parameters $(v, k, \lambda, \mu, \beta, \Delta)$ for which nontrivial abelian regular PDSs may exist with $k \leq 100$. First, we obtain a list of possible values of k, λ, μ with

$$2 \leq k \leq 100,\ 0 \leq \lambda \leq k-1 \text{ and } 1 \leq \mu \leq k-1. \qquad (15.1)$$

Other parameters are computed by the formulae

$$\beta = \lambda - \mu,\ \Delta = \beta^2 + 4(k-\mu) \text{ and } v = (k^2 - \beta k - k + \mu)/\mu. \qquad (15.2)$$

Then the parameters are tested with the following criterions drawn from Proposition 1.4, Corollaries 3.6, 6.3 and Theorems 3.4, 6.1, 6.9.

(i) β and Δ have the same parity;
(ii) $v^2 \equiv (2k - \beta)^2 \equiv (\beta^2 + 2\beta)v \equiv 0 \bmod \Delta$;
(iii) v, Δ, v^2/Δ have same prime divisors;
(iv) if Δ is not a square, then there exists an odd prime $p \equiv 1 \bmod 4$ such that $(v, k, \lambda, \mu, \beta, \Delta) = (p^{2s+1}, (p^{2s+1} - 1)/2, (p^{2s+1} - 5)/4, (p^{2s+1} - 1)/4, -1, p^{2s+1})$; and
(v) if $v = p^s$, where p is a prime, and Δ is a square, then k is a multiple of $p - 1$.

If D is a nontrivial abelian regular PDS with parameters $(v, k, \lambda, \mu, \beta, \Delta)$, then $D' = (G\backslash D)\backslash\{e\}$ is a regular PDS with parameters

$$(v', k', \lambda', \mu', \beta', \Delta') = (v, v - k - 1, v - 2k - 2 + \mu, v - 2k + \lambda, -\beta - 2, \Delta)$$

and the dual D^+ is a regular PDS with parameters

$$(v^+, k^+, \lambda^+, \mu^+, \beta^+, \Delta^+) = (v, [(\sqrt{\Delta} - \beta)(v - 1) - 2k]/(2\sqrt{\Delta}), \beta^+ + \mu^+,$$
$$[4k^+ - \Delta^+ + (\beta^+)^2]/4, [v - 2k + \beta - \sqrt{\Delta}]/\sqrt{\Delta}, v^2/\Delta).$$

Hence we only list those parameters with

$$k \leq (v - 1)/2 \text{ and } \Delta \leq v \tag{15.3}$$

since the case $k > (v - 1)/2$ can be obtained by the complement and the case $\Delta > v$ can be obtained by the dual.

The following theorem is a particular case of Theorems 7.1 and 7.3(c) which is useful in determining the existence of nontrivial abelian PDSs.

THEOREM 15.1. *Suppose there exists a nontrivial regular (v, k, λ, μ)-PDS in an abelian group where v is not a prime power. Let p be an odd prime divisor of v, say $v = p^t u$ and $\Delta = p^{2r}\pi^2$ where $p \nmid u$ and $p \nmid \pi$. Let $\beta_1 = \beta - 2\theta\pi$ where $(2\theta - 1)\pi \leq \beta < (2\theta + 1)\pi$. Then*

(a) *$A = (u + \beta_1)^2 - (\pi^2 - \beta_1^2)(u - 1)$ is a square*; *and*
(b) *either $k_1 = (u + \beta_1 - \sqrt{A})/2$ or $k_1 = (u + \beta_1 + \sqrt{A})/2$ satisfies all the following*:
  (i) $0 \leq k_1 < min\ \{k, u\}$;
  (ii) *if $k_1 \neq 0$ and $u - 1$, then $\lambda_1, \mu_1, u - 2k_1 + \lambda_1, u - 2k_1 - 2 + \mu_1$ are nonnegative where where $\mu_1 = k_1 - [(\pi^2 - \beta_1^2)/4]$ and $\lambda_1 = \beta_1 + \mu_1$; and*
  (iii) *if $p \geq 5$ and $k_1 \neq 0$, $u - 1$, then either* (1) *r is even and $\theta \equiv 0 \bmod (p - 1)$ or* (2) *r is odd and $\theta \equiv (p - 1)/2 \bmod (p - 1)$.* ■

The following is a result that we need in Table 15.3.

Remark 15.2. Brouwer and Neumaier [100] have proved that there is no (1944, 67, 10, 2)-strongly regular graph and hence no abelian regular (1944, 67, 10, 2)-PDS. Readers are referred to the survey by Brouwer and van Lint [5]. ■

Table 15.3. We give a table of parameters (v, k, λ, μ, β, Δ) satisfying (15.1), (15.2), (15.3) and criterions (i), (ii), (iii), (iv), (v). In the following, *Paley* refers to regular PDSs constructed by Theorem 2.1; *PCP* refers to regular PDSs constructed by Theorem 2.2; and *?* means the existence of such a regular PDS is still unknown.

No.	v	k	λ	μ	β	Δ		Examples/Remark
1	5	2	0	1	−1	5	—	Paley.
2	9	4	1	2	−1	9	—	Paley.
3	16	5	0	2	−2	16	—	Example 12.8.
4	16	6	2	2	0	16	—	(4, 2)-PCP.
5	13	6	2	3	−1	13	—	Paley.
6	25	8	3	2	1	25	—	(5, 2)-PCP.
7	17	8	3	4	−1	17	—	Paley.
8	36	10	4	2	2	36	—	(6, 2)-PCP.
9	49	12	5	2	3	49	—	(7, 2)-PCP.
10	25	12	5	6	−1	25	—	Paley.
11	36	14	4	6	−2	36	—	Example 12.8.
12	64	14	6	2	4	64	—	(8, 2)-PCP.
13	29	14	6	7	−1	29	—	Paley.
14	36	15	6	6	0	36	—	(6, 3)-PCP.
15	81	16	7	2	5	81	—	(9, 2)-PCP.
16	64	18	2	6	−4	64	—	Example 9.2(1).
17	49	18	7	6	1	49	—	(7, 3)-PCP.
18	100	18	8	2	6	100	—	(10, 2)-PCP.
19	37	18	8	9	−1	37	—	Paley.
20	81	20	1	6	−5	81	—	Example 2.7(2).
21	121	20	9	2	7	121	—	(11, 2)-PCP.
22	41	20	9	10	−1	41	—	Paley.
23	64	21	8	6	2	64	—	(8, 3)-PCP.
24	100	22	0	6	−6	100	—	?
25	243	22	1	2	−1	81	—	Example 8.3(2).
26	144	22	10	2	8	144	—	(12, 2)-PCP.
27	81	24	9	6	3	81	—	(9, 3)-PCP.
28	169	24	11	2	9	169	—	(13, 2)-PCP.
29	49	24	11	12	−1	49	—	Paley.
30	196	26	12	2	10	196	—	(14, 2)-PCP.
31	53	26	12	13	−1	53	—	Paley.
32	100	27	10	6	4	100	—	(10, 3)-PCP.
33	64	27	10	12	−2	64	—	Example 12.8.
34	64	28	12	12	0	64	—	(8, 4)-PCP.
35	225	28	13	2	11	225	—	(15, 2)-PCP.
36	81	30	9	12	−3	81	—	Example 10.6(1).
37	121	30	11	6	5	121	—	(11, 3)-PCP.
38	256	30	14	2	12	256	—	(16, 2)-PCP.
39	61	30	14	15	−1	61	—	Paley.
40	81	32	13	12	1	81	—	(9, 4)-PCP.
41	289	32	15	2	13	289	—	(17, 2)-PCP.

Table 15.3. (Continued).

No.	v	k	λ	μ	β	Δ		Examples/Remark
42	100	33	8	12	−4	100	—	?
43	144	33	12	6	6	144	—	(12, 3)-PCP.
44	324	34	16	2	14	324	—	(18, 2)-PCP.
45	169	36	13	6	7	169	—	(13, 3)-PCP.
46	100	36	14	12	2	100	—	?
47	361	36	17	2	15	361	—	(19, 2)-PCP.
48	73	36	17	18	−1	73	—	Paley.
49	400	38	18	2	16	400	—	(20, 2)-PCP.
50	144	39	6	12	−6	144	—	?
51	196	39	14	6	8	196	—	(14, 3)-PCP.
52	216	40	4	8	−4	144	—	?
53	121	40	15	12	3	121	—	(11, 4)-PCP.
54	441	40	19	2	17	441	—	(21, 2)-PCP.
55	81	40	19	20	−1	81	—	Paley.
56	288	41	4	6	−2	144	—	NOT EXIST by Theorem 15.1 with $p = 3$.
57	288	42	6	6	0	144	—	NOT EXIST by Theorem 15.1 with $p = 3$.
58	225	42	15	6	9	225	—	(15, 3)-PCP.
59	484	42	20	2	18	484	—	(22, 2)-PCP.
60	216	43	10	8	2	144	—	?
61	144	44	16	12	4	144	—	(12, 4)-PCP.
62	100	44	18	20	−2	100	—	NOT EXIST by Theorem 12.9.
63	529	44	21	2	19	529	—	(23, 2)-PCP.
64	89	44	21	22	−1	89	—	Paley.
65	196	45	4	12	−8	196	—	?
66	256	45	16	6	10	256	—	(16, 3)-PCP.
67	100	45	20	20	0	100	—	NOT EXIST by Theorem 12.9.
68	392	46	0	6	−6	196	—	?
69	576	46	22	2	20	576	—	(24, 2)-PCP.
70	225	48	3	12	−9	225	—	?
71	289	48	17	6	11	289	—	(17, 3)-PCP.
72	169	48	17	12	5	169	—	(13, 4)-PCP.
73	625	48	23	2	21	625	—	(25, 2)-PCP.
74	97	48	23	24	−1	97	—	Paley.
75	121	50	21	20	1	121	—	(11, 5)-PCP.
76	676	50	24	2	22	676	—	(26, 2)-PCP.
77	101	50	24	25	−1	101	—	Paley.
78	256	51	2	12	−10	256	—	Example 2.7(2).
79	392	51	10	6	4	196	—	?
80	324	51	18	6	12	324	—	(18, 3)-PCP.
81	144	52	16	20	−4	144	—	?
82	196	52	18	12	6	196	—	?
83	729	52	25	2	23	729	—	(27, 2)-PCP.
84	361	54	19	6	13	361	—	(19, 3)-PCP.
85	784	54	26	2	24	784	—	(28, 2)-PCP.
86	109	54	26	27	−1	109	—	Paley.
87	144	55	22	20	2	144	—	?
88	225	56	19	12	7	225	—	(15, 4)-PCP.
89	841	56	27	2	25	841	—	(29, 2)-PCP.
90	113	56	27	28	−1	113	—	Paley.
91	324	57	0	12	−12	324	—	?

Table 15.3. (Continued).

No.	v	k	λ	μ	β	Δ		Examples/Remark
92	400	57	20	6	14	400	—	(20, 3)-PCP.
93	900	58	28	2	26	900	—	(30, 2)-PCP.
94	196	60	14	20	−6	196	—	?
95	256	60	20	12	8	256	—	(16, 4)-PCP.
96	441	60	21	6	15	441	—	(21, 3)-PCP.
97	169	60	23	20	3	169	—	(13, 5)-PCP.
98	961	60	29	2	27	961	—	(31, 2)-PCP.
99	121	60	29	30	−1	121	—	Paley.
100	1024	62	30	2	28	1024	—	(32, 2)-PCP.
101	125	62	30	31	−1	125	—	Paley.
102	484	63	22	6	16	484	—	(22, 3)-PCP.
103	225	64	13	20	−7	225	—	NOT EXIST by Theorem 15.1 with $p = 5$.
104	289	64	21	12	9	289	—	(17, 4)-PCP.
105	1089	64	31	2	29	1089	—	(33, 2)-PCP.
106	196	65	24	20	4	196	—	?
107	144	65	28	30	−2	144	—	Example 12.8.
108	529	66	23	6	17	529	—	(23, 3)-PCP.
109	144	66	30	30	0	144	—	Example 12.8.
110	1156	66	32	2	30	1156	—	(34, 2)-PCP.
111	1944	67	10	2	8	324	—	NOT EXIST by Remark 15.2.
112	256	68	12	20	−8	256	—	Example 9.6(2).
113	324	68	22	12	10	324	—	?
114	1225	68	33	2	31	1225	—	(35, 2)-PCP.
115	137	68	33	34	−1	137	—	Paley.
116	576	69	24	6	18	576	—	(24, 3)-PCP.
117	512	70	6	10	−4	256	—	Example 9.2(1).
118	225	70	25	20	5	225	—	NOT EXIST by Theorem 15.1 with $p = 5$.
119	1296	70	34	2	32	1296	—	(36, 2)-PCP.
120	361	72	23	12	11	361	—	(19, 4)-PCP.
121	625	72	25	6	19	625	—	(25, 3)-PCP.
122	169	72	31	30	1	169	—	(13, 6)-PCP.
123	1369	72	35	2	33	1369	—	(37, 2)-PCP.
124	512	73	12	10	2	256	—	?
125	1444	74	36	2	34	1444	—	(38, 2)-PCP.
126	149	74	36	37	−1	149	—	Paley.
127	676	75	26	6	20	676	—	(26, 3)-PCP.
128	256	75	26	20	6	256	—	(16, 5)-PCP.
129	196	75	26	30	−4	196	—	?
130	324	76	10	20	−10	324	—	?
131	400	76	24	12	12	400	—	(20, 4)-PCP.
132	1521	76	37	2	35	1521	—	(39, 2)-PCP.
133	729	78	27	6	21	729	—	(27, 3)-PCP.
134	196	78	32	30	2	196	—	?
135	1600	78	38	2	36	1600	—	(40, 2)-PCP.
136	157	78	38	39	−1	157	—	Paley.
137	441	80	25	12	13	441	—	(21, 4)-PCP.
138	225	80	25	30	−5	225	—	?
139	289	80	27	20	7	289	—	(17, 5)-PCP.
140	1681	80	39	2	37	1681	—	(41, 2)-PCP.
141	784	81	28	6	22	784	—	(28, 3)-PCP.

Table 15.3. (Continued).

No.	v	k	λ	μ	β	Δ		Examples/Remark
142	1764	82	40	2	38	1764	—	(42, 2)-PCP.
143	400	84	8	20	−12	400	—	?
144	484	84	26	12	14	484	—	?
145	841	84	29	6	23	841	—	(29, 3)-PCP.
146	225	84	33	30	3	225	—	?
147	1849	84	41	2	39	1849	—	(43, 2)-PCP.
148	169	84	41	42	−1	169	—	Paley.
149	800	85	0	10	−10	400	—	NOT EXIST by Theorem 15.1 with $p = 5$.
150	256	85	24	30	−6	256	—	Example 10.5(2).
151	324	85	28	20	8	324	—	?
152	1936	86	42	2	40	1936	—	(44, 2)-PCP.
153	173	86	42	43	−1	173	—	Paley.
154	900	87	30	6	24	900	—	(30, 3)-PCP.
155	441	88	7	20	−13	441	—	NOT EXIST by Theorem 15.1 with $p = 7$.
156	529	88	27	12	15	529	—	(23, 4)-PCP.
157	2025	88	43	2	41	2025	—	(45, 2)-PCP.
158	361	90	29	20	9	361	—	(19, 5)-PCP.
159	961	90	31	6	25	961	—	(31, 3)-PCP.
160	256	90	34	30	4	256	—	(16, 6)-PCP.
161	196	90	40	42	−2	196	—	NOT EXIST by Theorem 12.9.
162	2116	90	44	2	42	2116	—	(46, 2)-PCP.
163	181	90	44	45	−1	181	—	Paley.
164	196	91	42	42	0	196	—	NOT EXIST by Theorem 12.9.
165	484	92	6	20	−14	484	—	?
166	576	92	28	12	16	576	—	(24, 4)-PCP.
167	2209	92	45	2	43	2209	—	(47, 2)-PCP.
168	4000	93	8	2	6	400	—	NOT EXIST by Theorem 15.1 with $p = 5$.
269	1024	93	32	6	26	1024	—	(32, 3)-PCP.
170	800	94	18	10	8	400	—	NOT EXIST by Theorem 15.1 with $p = 5$.
171	2304	94	46	2	44	2304	—	(48, 2)-PCP.
172	324	95	22	30	−8	324	—	?
173	400	95	30	20	10	400	—	(20, 5)-PCP.
174	625	96	29	12	17	625	—	(25, 4)-PCP.
175	1089	96	33	6	27	1089	—	(33, 3)-PCP.
176	289	96	35	30	5	289	—	(17, 6)-PCP.
177	225	96	39	42	−3	225	—	?
178	2401	96	47	2	45	2401	—	(49, 2)-PCP.
179	193	96	47	48	−1	193	—	Paley.
180	225	98	43	42	1	225	—	?
181	2500	98	48	2	46	2500	—	(50, 2)-PCP.
182	197	98	48	49	−1	197	—	Paley.
183	1156	99	34	6	28	1156	—	(34, 3)-PCP.
184	576	100	4	20	−16	576	—	?
185	676	100	30	12	18	676	—	?
186	441	100	31	20	11	441	—	NOT EXIST by Theorem 15.1 with $p = 7$.
187	2601	100	49	2	47	2601	—	(51, 2)-PCP.

Acknowledgment

The author wants to thank Professor Dr. A.E. Brouwer for telling him the new PDSs constructed by de Resmini and Migliori [63], de Resmini [62] and de Lange [72].

Note Added in Proof

Recently, Q. Xiang (preprint, Note on Paley type partial difference sets) proved a new exponent bound for abelian groups having $(p^{2s+1}, (p^{2s+1} - 1)/2, (p^{2s+1} - 5)/4, (p^{2s+1} - 1)/4)$-PDSs, see Questions 6.6 and 13.4. His result says that if p^e is the exponent of the abelian group and $e \geq 2$, then $e \leq (s + 1)/2$. This bound is better than Theorem 6.7.

References

1. R.C. Bose. 1963. Strongly regular graphs, partial geometries and partially balanced designs. *Pacific J. Math.* 13: 389–419.
2. X.L. Hubaut. 1975. Strongly regular graphs. *Discrete Math.* 13: 357–381.
3. P.J. Cameron. 1978. Strongly regular graphs. *Selected Topics in Graph Theory,* (L.W. Beineke and R.J. Wilson, eds.). New York: Academic Press. pp. 337–360.
4. J.J. Seidel. 1979. Strongly regular graphs. *Surveys in Combinatorics,* (B. Bollabás, ed.). Cambridge: Cambridge University Press. pp. 157–180.
5. A.E. Brouwer and J.H. van Lint. 1984. Strongly rgular graphs and partial geometries. *Enumeration and Designs,* (D.M. Jackson and S.A. Vanstone, eds.). New York: Academic Press. pp. 85–122.
6. P.J. Cameron and J.H. van Lint. 1991. *Designs, Graphs, Codes and Their Links.* Cambridge: Cambridge University Press.
7. H.P. Yap. 1986. *Some Topics in Graph Theory.* Cambridge: Cambridge University Press.
8. I.M. Chakravarti. 1969. Partial difference sets, calibration designs and error correcting codes. *Bull. Inter. Stat. Inst.* 43(2): 104–106.
9. R.C. Bose and J.M. Cameron. 1965. The bridge tournament problem and calibration designs for comparing pairs of objects. *Journal of Research of the NBS-B, Maths. and Math. Phys.* 69: 323–332.
10. S.L. Ma. 1984. Partial difference sets. *Discrete Math.* 52: 75–89.
11. S.L. Ma. 1989. On association schemes, Schur rings, strongly regular graphs and partial difference sets. *Ars. Combinatoria.* 27: 211–220.
12. P. Delsarte. 1971. Two-weight linear codes and strongly regular graphs. Brussels: MBLE Res. Lab. Report R160.
13. P. Delsarte. 1972. Weights of linear codes and strongly regular normed spaces. *Discrete Math.* 3: 47–64.
14. P. Delsarte. 1973. An algebraic approach to the association schemes of coding theory. *Philips Research Report.* Suppl. No. 10.
15. P. Camion. 1979. *Difference Sets in Elementary Abelian Groups.* Montreal: Les Presses de l'Université de Montréal.
16. W.G. Bridges and R.A. Mena. 1979. Rational spectra and cyclic strongly regular graphs. *Ars Combinatoria.* 8: 143–161.
17. W.G. Bridges and R.A. Mena. 1982. Rational G-matrices with rational eigenvalues. *J. Combin. Theory Ser. A.* 32: 264–280.
18. R. Calderbank and W.M. Kantor. 1986. The geometry of two-weight codes. *Bull. London Math. Soc.* 18: 97–122.
19. D. Ghinelli and S. Löwe. 1991. On multiplier of partial addition sets. *Geometriae Dedicata.* 40: 53–58.
20. T. Beth, D. Jungnickel, and H. Lenz. 1986. *Design Theory.* Cambridge: Cambridge University Press.
21. E.S. Lander. 1983. *Symmetric Designs: An Algebraic Approach.* Cambridge: Cambridge University Press.
22. D. Jungnickel. 1992. Difference sets. *Contemporary Design Theory,* (J.H. Dinitz and D.R. Stinson, eds.). New York: Wiley. pp. 241–324.
23. R.E.A.C. Paley. 1933. On orthogonal matrices. *J. Math. Phys.* 12: 311–320.

24. A.P. Sprague. 1982. Translation nets. *Mitt. Math. Sem Giessen.* 157: 46–68.
25. R.A. Bailey and D. Jungnickel. 1990. Translation nets and fixed-point-free group automorphisms. *J. Combin. Theory Ser. A.* 55: 1-13.
26. D. Jungnickel. 1990. Latin squares, their geometries and their groups. A survey. *Coding Theory and Design Theory Part II: Design Theory,* (D. Ray-Chaudhuri, ed.). New York: Springer-Verlag. pp. 166–225.
27. R.L. McFarland. 1973. A family of difference sets in non-cyclic groups. *J. Combin. Theory Ser. A.* 15: 1-10.
28. H.B. Mann. 1965. *Addition Theorems.* New York: Wiley.
29. O. Tamaschke. 1963. Zur Theorie der Permutationsgruppen mit regulärer Untergruppe. *Math. Z.* 80: 328-352.
30. D.R. Hughes, J.H. van Lint and R.M. Wilson. 1979. Announcement at the Seventh British Combinatorial Conference, Cambridge. Unpublished.
31. I. Schur. 1933. Zur Theorie der enfach transitiven Permutationsgruppen. *Sitz. Preuss. Akad. Wiss. Berlin. Phys-math. Kl.* pp. 598-623.
32. H. Wielandt. 1949. Zur Theorie der einfach transitiven Permutationsgruppen II. *Math. Zeit.* 52: 384-393.
33. H. Wielandt. 1964. *Finite Permutation Groups.* New York: Academic Press.
34. W. Scott. 1964. *Group Theory.* New Jersey: Prentice Hall.
35. R.C. Bose and D.M. Mesner. 1959. On linear association algebras corresponding to association schemes of partially balanced incomplete block designs, *Ann. Math. Stat.* 30: 21–38.
36. E. Bannai and T. Ito. 1984. *Algebraic Combinatorics I: Association Schemes.* Menlo Park: Benjamin/Cumming.
37. W. Scott. 1957. Solvable factorizable groups. *Illinois J. Math.* 1: 389-394.
38. S.L. Ma. 1987. Partial difference sets in dihedral groups. *South East Asian Bull. Math.* 11: 53–59.
39. M.J. de Resmini and D. Jungnickel. 1992. Strongly regular semi-Cayley graphs. *J. Alg. Comb.* 1: 171-195.
40. K.H. Leung and S.L. Ma. 1993. Partial difference triples. *J. Alg. Comb.* 2: 397–409.
41. S.L. Ma. 1985. *Polynomial Addition Sets.* University of Hong Kong. Thesis.
42. S.L. Ma. 1990. Polynomial addition sets and symmetric difference sets. *Coding Theory and Design Theory Part II: Design Theory,* (D. Ray-Chaudhuri, ed.). New York: Springer-Verlag. pp. 273-279.
43. J.A. Davis, Preprint. Partial difference sets in p-groups.
44. S.L. Ma. 1994. On subsets of partial difference sets. *Discrete Math.*
45. F.J. MacWilliams and N.J.A. Sloane. 1977. *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland.
46. J.H. van Lint. 1982. *Introduction to Coding Theory.* New York: Springer-Verlag.
47. V. Pless. 1989. *The Theory of Error-Correcting Codes.* Second Edition. New York: Wiley.
48. F.J. MacWilliams. 1962. *Combinatorial Problems in Elementary Abelian Groups.* Harvard University. Thesis.
49. F.J. MacWilliams. 1963. A thoerem on the distribution of weights in a systematic code. *Bell System Tech. J.* 42: 79-94.
50. M.J.E. Golay. 1949. Notes on digital coding. *Proc. IRE.* 37: 657.
51. A. Tietäväinen. 1974. A short proof for the non-existence of unknown perfect codes over GF(q), q > 2. *Ann. Acad. Sci. Fenn. Ser. A I. Math.* 580: 1-6.
52. J.H. van Lint. 1975. A survey of perfect codes. *Rocky Mountain J. Math.* 5: 199-224.
53. N.V. Semakov, V.A. Zinovjev and G.V. Zaitzev. 1971. Uniformly packed codes. *Problems Inform. Transmission.* 7 (no. 1): 30-39.
54. J.M. Goethals and H.C.A. van Tilborg. 1975. Uniformly packed codes. *Philips Research Reports.* 30: 9–36.
55. H.C.A. van Tilborg. 1976. *Uniformly Packed Codes.* Tech. Univ. Eindhoven. Thesis.
56. R. Calderbank. 1982. On uniformly packed [n, n − k, 4] codes over GF(q) and a class of caps in PG(k − 1, q). *J. London Math. Soc.* 26: 365-384.
57. J.W.P. Hirschfeld. 1979. *Projective Geometries Over Finite Fields.* Oxford: Oxford University Press.
58. P. Dembowski. 1968. *Finite Geometries.* New York: Springer-Verlag.
59. L.E. Denniston. 1969. Some maximal arcs in finite projective planes. *J. Combin. Theory.* 6: 317-319.
60. A.E. Brouwer. 1985. Some new two-weight codes and strongly regular graphs. *Discrete Applied Math.* 10: 111-114.
61. M.J. de Resmini. 1983. An infinite family of type (m, n) sets in PG(2, q^2), q a square. *J. Geom.* 20: 36–43.
62. M.J. de Resmini. 1987. A 35-set of type (2, 5) in PG(2, 9). *J. Combin. Theory Ser. A.* 45: 303-305.
63. M.J. de Resmini and G. Migliori. 1986. A 78-set of type (2, 6) in PG(2, 16). *Ars Combinatoria.* 22: 73–75.
64. B. Segre. 1965. Forme e geometrie hermitiane, con particolare riguardo al caso finito. *Ann. Mat. Pura Appl.* 70: 1-202.

65. R. Hill. 1973. On the largest size cap in $S_{5,3}$. *Rend. Accad. Naz. Lincei (8)*. 54: 378–384.

66. N. Tzanakis and J. Wolfskill. 1987. The diophantine equation $x^2 = 4q^{a/2} + 4q + 1$ with an application to coding theory. *J. Number Theory*. 26: 96–116.

67. J.A. Thas. 1973. A combinatorial problem. *Geometriae Dedicata*. 1: 236–240.

68. J. Storer. 1967. *Cyclotomy and Difference Sets*. Chicago: Markham.

69. L.D. Baumert, W.H. Mills, and R.L. Ward. 1982. Uniformly cyclotomy. *J. Number Theory*. 14: 67–82.

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

71. R. Hill. 1976. Caps and groups. *Atti dei Convegni Lincei, Colloquio Internazionale sulle Teorie Combinatorie (Roma 1973)*. no. 7. Accad. Naz. Lincei. pp. 384–394.

72. C.L.M. de Lange. 1990. *Cyclotomic Graphs*. Tech. Univ. Eindhoven. Thesis.

73. K.H. Leung and S.L. Ma. 1990. Constructions of partial difference sets and relative difference sets on p-groups. *Bull. London Math. Soc.* 22: 533–539.

74. J.F. Dillon. 1987. Difference sets in 2-groups. *Proc. NSA Math. Sci. Meeting*. pp. 165–172.

75. E.C. Johnsen. 1964. The inverse multiplier for abelian group difference sets. *Can. J. Math.* 16: 787–796.

76. D. Ghinelli. 1987. A new result on difference sets with −1 as multiplier. *Geometriae Dedicata*. 23: 309–317.

77. D. Jungnickel. 1982. Difference sets with multiplier −1. *Arch. Math.* 38: 511–513.

78. R.L. McFarland and S.L. Ma. 1990. Abelian difference sets with multiplier minus one. *Arch. Math.* 54: 610–623.

79. R.L. McFarland. 1990. Sub-difference sets of Hadamard difference sets. *J. Combin. Theory Ser. A.* 54: 112–122.

80. S.L. Ma. 1992. McFarland's conjecture on abelian difference sets with multiplier −1. *Designs, Codes and Cryptography.* 1: 321–332.

81. M. Xia. 1992. Some infinite classes of special Williamson matrices and difference sets. *J. Combin. Theory Ser. A.* 61: 230–242.

82. P.K. Menon. 1962. On difference sets whose parameters satisfy a certain relation. *Proc. Amer. Math. Soc.* 13: 739–745.

83. R.J. Turyn. 1984. A special class of Williamson matrices and difference sets. *J. Combin. Theory Ser. A.* 36: 111–115.

84. K.T. Arasu. 1990. Recent results on difference sets. *Coding Theory and Design Theory Part II: Design Theory*, (Ray-Chaudhuri, D. ed.). New York: Springer-Verlag, pp. 1–23.

85. H.B. Mann. 1965. Difference sets in elementary abelian groups. *Ill. J. Math.* 17: 541–542.

86. K.W. Smith. Preprint. Non-abelian Hadamard difference sets.

87. M. Miyamoto. 1983. A family of difference sets having −1 as an invariant. *Hokkaido Math. J.* 12: 24–26.

88. S.L. Ma. 1989. A family of difference sets having −1 as an invariant. *Europ. J. Combinatorics*. 10: 273–274.

89. D. Ghinelli. 1992. Regular groups on generalized quadrangles and nonabelian difference sets with multiplier −1. *Geometriae Dedicata*. 41: 165–174.

90. K.T. Arasu, D. Jungnickel, S.L. Ma, and A. Pott. To appear. Strongly regular Cayley graphs with $\lambda - \mu = -1$. *J. Combin. Theory Ser. A.*

91. D. Jungnickel. 1982. On automorphism groups of divisible designs. *Canad. J. Math.* 34: 257–297.

92. K.T. Arasu, D. Jungnickel, and A. Pott. 1990. Divisible difference sets with multiplier-1, *J. Algebra* 133: 35–62.

93. K.T. Arasu, D. Jungnickel, and A. Pott. 1991. Symmetric divisible designs with $k - \lambda_1 - 1$. *Discrete Math.* 97: 25–38.

94. K.H. Leung and S.L. Ma. Preprint. Partial difference sets with Paley parameters.

95. J.A. Thas. 1977. Combinatorics of partial geometries and generalized quadrangles. *Higher Combinatorics*, (M. Aigner, ed.). Dordrecht: Reidel. pp. 183–199.

96. L.D. Baumert. 1971. *Cyclic Difference Sets*. New York: Springer-Verlag.

97. S.L. Ma. Preprint. Regular automorphism groups on partial geometries.

98. S.E. Payne and J.A. Thas. 1984. *Finite Generalized Quadrangles*. Boston: Pitman.

99. S. Löwe. Preprint. Constructions of GQs.

100. A.E. Brouwer and A. Neumaier. 1981. Strongly regular graphs where $\mu = 2$ and λ is large. Amsterdam: Math. Centrum. Report 151/81.