Des. Codes Cryptogr. (2009) 50:93–105
DOI 10.1007/s10623-008-9216-4

Some results on skew Hadamard difference sets

Guobiao Weng · Lei Hu

Received: 1 July 2007 / Revised: 13 March 2008 / Accepted: 22 April 2008 /
Published online: 30 May 2008

Abstract In this paper, we present two constructions of divisible difference sets based on skew Hadamard difference sets. A special class of Hadamard difference sets, which can be derived from a skew Hadamard difference set and a Paley type regular partial difference set respectively in two groups of orders v_1 and v_2 with $|v_1 - v_2| = 2$, is contained in these constructions. Some result on inequivalence of skew Hadamard difference sets is also given in the paper. As a consequence of Delsarte's theorem, the dual set of skew Hadamard difference set is also a skew Hadamard difference set in an abelian group. We show that there are seven pairwisely inequivalent skew Hadamard difference sets in the elementary abelian group of order 3^5 or 3^7, and also at least four pairwisely inequivalent skew Hadamard difference sets in the elementary abelian group of order 3^9. Furthermore, the skew Hadamard difference sets deduced by Ree-Tits slice symplectic spreads are the dual sets of each other when $q \leq 3^{11}$.

Keywords Skew Hadamard difference sets · Hadamard difference sets · Partial difference sets

AMS Classification 05B10

1 Introduction

Let G be a finite group of order v and with identity e. A k-element subset D of G is called a (v, k, λ) *difference set* if the list of "differences" xy^{-1} ($x, y \in D$ and $x \neq y$) represents each non-identity element in G exactly λ times. The study of difference sets is one of the central

Communicated by Q. Xiang.

G. Weng (✉) · L. Hu
State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences,
Beijing 100049, People's Republic of China
e-mail: gbweng@is.ac.cn

L. Hu
e-mail: hu@is.ac.cn

problems in discrete mathematics, and is with interest from not only pure mathematics but also applied sciences, for example signal design in the communication theory.

When G is abelian, the character theory of finite groups can be applied and it is a powerful tool to study difference sets. In this paper, we present some results on different sets which are related to skew Hadamard different sets. We discuss these results in the view of character theory and prove them in terms of *two-character-valued sets* (TCVS). TCVS are subsets of G that take exactly two values for all nontrivial character of G.

This paper is organized as follows. In Sect. 2, we give preliminaries on difference set, partial difference set, and divisible difference set, and summarize known results on TCVS. In Sect. 3, along the way of Menon's construction, we derive two skew Hadamard difference set based constructions for divisible difference sets. A construction of Hadamard difference sets is also given in both cases of G being abelian and nonabelian. In Sect. 4, we discuss the equivalence of skew Hadamard difference sets, and moreover, we discuss the classification of known skew Hadamard difference sets that are defined in elementary abelian groups of small order $q = 3^5, 3^7, 3^9$, and 3^{11}.

2 Preliminaries

A k-element subset D of G is called a (v, k, λ) *difference set* if the list of "differences" xy^{-1}, $x, y \in D$, represents each nonidentity element in G exactly λ times. A k-element subset D of G is called a (v, k, λ, μ) *partial difference set* if the list of "differences" xy^{-1}, $x, y \in D$, represents each non-identity element in D exactly λ times and each non-identity element in $G\backslash D$ exactly μ times. A k-element subset D of G is called a $(m, n, k, \lambda_1, \lambda_2)$ *divisible difference set* relative to N if the list of "differences" xy^{-1}, $x, y \in D$, represents each element in $G\backslash N$ exactly λ_2 times and each non-identity element in N exactly λ_1 times, where N is a subgroup of order n with $v = mn$.

A difference set D in a finite group G is called a *Hadamard difference set* if its corresponding parameters are $(v, \frac{v-1}{2}, \frac{v-3}{4})$, and is called a *Menon difference set* if its parameters are $(4h^2, 2h^2 \pm h, h^2 \pm h)$. They are most important classes of difference sets with plentiful results. A difference set D in group G is called a *skew Hadamard difference set* (SHDS) if G is the disjoint union of D, $D^{(-1)}$, and $\{e\}$. A partial difference set D in a finite group G is of *Paley type* if its parameters are $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$. A subset D is called *reversible* if $D^{(-1)} = D$, and further called *regular* if $e \notin D$ and $D^{(-1)} = D$. Two subsets D and E of G are *equivalent* if there exist an automorphism σ of G and an element $g \in G$ such that $D = g\sigma(E) := \{g\sigma(x) \mid x \in G\}$. Let D be a subset in an abelian group G of order v. An automorphism $g \mapsto g^t$ of G for an integer t prime with v is called a (numerical) *multiplier* of D, if there is an element $g \in G$ such that $D^{(t)} = gD = \{gd \mid d \in D\}$, where $D^{(t)} := \{x^t \mid x \in D\}$.

As an example of difference sets, let $\mathbf{F}_q$ be the finite field of order q, the set of all nonzero squares of $\mathbf{F}_q$ is a SHDS when $q \equiv 3 \bmod 4$, and is a regular Paley type partial difference set when $q \equiv 1 \bmod 4$.

Let R be a communicative ring with identity 1. The group ring $R[G] = \left\{ \sum_{g\in G} a_g g \mid a_g \in R \right\}$ with the multiplication rule "·" as

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{h\in G} b_h g\right) = \sum_{g\in G} \sum_{h\in G} (a_h b_{h^{-1}g}) g$$

is a free R-module of rank v. Obviously, e is the identity of $R[G]$. We use the same symbol D to denote the element $\sum_{g\in D} g$ in $R[G]$ for a subset D of G.

Usually, R is taken as the ring $\mathbf{Z}$ of integers, the field $\mathbf{Q}$ of rational numbers, or the complex field $\mathbf{C}$. Employing notion in $\mathbf{Z}[G]$, D is a (v, k, λ) difference set if and only if

$$DD^{(-1)} = (k-\lambda)e + \lambda G,$$

D is a (v, k, λ, μ) partial difference set if and only if

$$DD^{(-1)} = se + \mu G + (\lambda - \mu)D,$$

and D is a $(m, n, k, \lambda_1, \lambda_2)$ divisible difference set relative to N if and only if

$$DD^{(-1)} = (k-\lambda_1)e + \lambda_2 G + (\lambda_1 - \lambda_2)N,$$

where $s = k(k-\lambda) - \mu(v-k)$.

When G is abelian, we can make use the notion of character. A character of G is a group homomorphism $\chi\colon G \to \mathbf{C}^*$, where $\mathbf{C}^*$ is the multiplicative group of $\mathbf{C}$. The set $\widehat{G}$ of all characters of G is a group and is isomorphic to G. For the sake of completeness, we list the following two well known fundamental results on characters.

Lemma 2.1 (Orthogonality relations) *Let G be a finite abelian group of order v and with identity e. Then*

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} 0, & \text{if } g \neq e, \\ v, & \text{if } g = e, \end{cases}$$

$$\sum_{g\in G} \chi(g) = \begin{cases} 0, & \text{if } \chi \neq \chi_0, \\ v, & \text{if } \chi = \chi_0, \end{cases}$$

where χ_0 is the trivial character of G, that is, $\chi_0(g) = 1$ for all $g \in G$.

Lemma 2.2 (Inversion formula) *Let G be a finite abelian group of order v. Let $A = \sum_{g\in G} a_g g \in \mathbf{C}[G]$, and $\chi(A) := \sum_{g\in G} a_g \chi(g)$. Then we can recover the coefficients of A as follows:*

$$a_g = \frac{1}{v} \sum_{\chi\in\widehat{G}} \chi(A)\chi(g^{-1}).$$

Hence, if $A, B \in \mathbf{C}[G]$ satisfy $\chi(A) = \chi(B)$ for all characters χ of G, then $A = B$.

Using Lemma 2.2 and the fact that $\chi(D^{(-1)}) = \overline{\chi(D)}$, we have another description on difference sets and partial difference sets as follows.

Lemma 2.3 *Let D be a k-subset of an abelian group G of order v. Then D is a (v, k, λ) difference set if and only if the condition*

$$|\chi(D)| = \sqrt{k-\lambda}$$

holds for every nontrivial character χ of G.

Lemma 2.4 *Let D be a k-subset of an abelian group G of order v. Then D is a (v, k, λ, μ) partial difference set if and only if the condition*

$$\chi(D) = \frac{\beta \pm \sqrt{\Delta}}{2}$$

holds for every nontrivial character χ of G, where $\beta = \lambda - \mu$ and $\Delta = \beta^2 + 4\gamma$ with $\gamma = k - \mu$ if $e \notin D$ and $\gamma = k - \lambda$ if $e \in D$.

In view of the above lemma, we see that β and Δ are another two important parameters, so D is usually called a $(v, k, \lambda, \mu, \beta, \Delta)$ partial difference set.

Lemma 2.5 *Let D be a k-subset of an abelian group G of order v. Then D is a skew Hadamard difference set if and only if the condition*

$$\chi(D) = \frac{-1 \pm \sqrt{-v}}{2}$$

holds for every nontrivial character χ of G.

Let $D \in \mathbf{C}[G]$. By Lemma 2.2, $\chi(D)$ is a constant for all nontrivial character χ if and only if

$$D = ae + bG.$$

If D is a subset of abelian group G, and $\chi(D) = a$ or b, $a \neq b$, for all nontrivial character χ, then we call D a *two-character-valued set* (TCVS). By Lemmas 2.4 and 2.5, if D is a SHDS, reversible difference set, or partial difference set, then D is a TCVS.

Let D be a TCVS in an abelian group G. If $e \in D$, then $D\backslash\{e\}$ and $G\backslash D$ are also TCVS. Thus in the sequel, when D is a TCVS, we always assume $e \notin D$ and $\chi(D) = a$ or b, for every nontrivial character χ.

Let D be a TCVS. Then the subset of $\widehat{G}$,

$$\{\chi \mid \chi(D) = a\},$$

is called the *dual set* of D, denoted by D^*. Set a map ϕ_g from $\widehat{G}$ to $\mathbf{C}^*$ as

$$\phi_g(\chi) = \chi(g), \quad \forall \chi \in \widehat{G}.$$

Then $\{\phi_g : \forall g \in G\}$ is the set of all characters since $\widehat{G}$ is abelian and isomorphic to G. We have the following theorem, which is due to Delsarte.

Theorem 2.6 (Delsarte [6]) *Let D be a k-element subset in an abelian group G of order v, and assume the identity of G is not in D. Suppose that for every nontrivial character χ, $\chi(D) = a$ or b. Then the dual set D^* is a k^*-element subset in $\widehat{G}$, and for every nontrivial character ϕ of $\widehat{G}$, $\phi(D^*) = a^*$ or b^*, where $k^* = \frac{-k+b-bv}{a-b}$, $a^* = \frac{v-k+b}{a-b}$, and $b^* = \frac{-k+b}{a-b}$. Furthermore $D^{(-1)}$ is the dual set of D^*.*

When D is a SHDS, set $a = \frac{-1+\sqrt{-v}}{2}$, $b = \frac{-1-\sqrt{-v}}{2}$. Then $k^* = k = \frac{v-1}{2}$, $a^* = b$, and $b^* = a$. Hence,

Corollary 2.7 *Let D be a SHDS in abelian group G, and D^* be the dual set of D. Then D^* is again a SHDS in $\widehat{G}$.*

Now let D be an arbitrary TCVS in G. Set $E = D((a+b)e - D) \in \mathbf{C}[G]$. Then we easily have for every nontrivial character χ of G,

$$\chi(E) = ab.$$

Thus $E = abe + tG$, namely,

$$D^2 = -abe - tG + (a+b)D.$$

By comparing the coefficients of both sides, we find $a+b$ and ab are all integers. Thus, a is either an integer or an algebraic number of degree 2, that is, $\mathbf{Q}(a)/\mathbf{Q}$ is an extension of fields of degree 2. By the properties of cyclotomic fields, the multipliers of TCVS can be easily determined. The following theorem is partially listed in the works of [4,9–11,15,16].

Theorem 2.8 *Let D be a two-character-valued subset of an abelian group G of order v, $\chi(D) = a$ or b, and $e \notin D$. Then D is a SHDS or a regular partial difference set. Furthermore,*

(1) *If a is an integer, then any t with $gcd(t, v) = 1$ is a multiplier of D; and*
(2) *If a is not an integer, then $v = p^h$ for an odd prime p and an odd integer h. Furthermore, an integer t with $gcd(t, v) = 1$ is a multiplier of D if and only if t is a quadric residue modulo v; and $a, b = \frac{-1 \pm \sqrt{(-1)^{\frac{p-1}{2}} v}}{2}$.*

In [5,21], it was further proved that $exp(G) \le p^{\frac{h+1}{4}}$ holds in the case $a \notin \mathbf{Q}$. All known examples in this case exist in elementary abelian groups, and it was conjectured that $exp(G)=p$. An important case is that $a + b = -1$, which is determined as follows.

Theorem 2.9 [1] *Let D be a two-character-valued set of an abelian group G, $e \notin D$, and $\chi(D) = a$ or $-1-a$. Then*

(1) *D is a SHDS;*
(2) *D is a $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$ partial difference set; or*
(3) *D is a $(243, 22, 1, 2)$ or $(243, 220, 199, 200)$ partial difference set.*

3 Divisible difference sets from skew Hadamard difference sets

In this section, we modify Menon's method to give two constructions of divisible difference sets. Firstly, we give the character distribution of divisible difference sets.

Lemma 3.1 *A subset D of an abelian group G is a $(m, n, k, \lambda_1, \lambda_2)$ divisible difference sets relative to N if and only if*

$$|\chi(D)| = \begin{cases} k, & \text{if } \chi \text{ is trivial character,} \\ \sqrt{k^2 - \lambda_2 mn}, & \text{if } \chi \text{ is nontrivial but trivial over } N, \\ \sqrt{k - \lambda_1}, & \text{if } \chi \text{ is nontrivial over } N. \end{cases}$$

Let D_1 and D_2 be two subset in abelian groups H_1 and H_2, respectively, set

$$D_1 \times D_2 = \{(x, y) \mid x \in D_1, y \in D_2\}$$

be a subset in the abelian group $G = H_1 \times H_2$, and simplify $e \times H_2$ as H_2 and $H_1 \times e$ as H_1, where e is the identity of H_1 and H_2. Suppose D_i is a (v_i, k_i, λ_i) difference set in H_i for $i = 1, 2$, and we set

$$D = D_1 \times D_2 \cup (H_1 - D_1) \times (H_2 - D_2).$$

Note that any character χ of G can be written as $\chi = (\chi_1, \chi_2)$, where χ_i is a character of H_i, $i = 1, 2$. So

$$|\chi(D)| = \begin{cases} |(2k_1 - v_1)|\sqrt{k_2 - \lambda_2}, & \text{if } \chi_1 \text{ is trivial,} \\ |(2k_2 - v_2)|\sqrt{k_1 - \lambda_1}, & \text{if } \chi_2 \text{ is trivial,} \\ 2\sqrt{k_1 - \lambda_1}\sqrt{k_2 - \lambda_2}, & \text{if both } \chi_1 \text{ and } \chi_2 \text{ are nontrivial.} \end{cases}$$

Menon gave the following construction.

Theorem 3.2 (Menon [17]) *Let D_1 be a Menon difference set in an abelian group H_1, and D_2 be a difference set in an abelian group H_2. Then the subset D in the group $G = H_1 \times H_2$ defined by*

$$D = D_1 \times D_2 \cup (H_1 - D_1) \times (H_2 - D_2)$$

is a divisible difference set relative to H_2. Furthermore, if D_2 is a Menon difference set, then D is also a Menon difference set, and D is reversible if and only if both D_1 and D_2 are reversible.

Below we assume D_1 does not contain the identity e. Set

$$D = D_1 \times D_2 \cup (H_1 - D_1 - e) \times (H_2 - D_2).$$

Then we have

$$\chi(D) = \begin{cases} (2k_1 + 1 - v_1)\chi_2(D_2), & \text{if } \chi_1 \text{ is trivial,} \\ (2k_2 - v_2)\chi_1(D_1) + k_2 - v_2, & \text{if } \chi_2 \text{ is trivial,} \\ (2\chi_1(D_1) + 1)\chi_2(D_2), & \text{if } \chi_1 \text{ and } \chi_2 \text{ are nontrivial,} \end{cases}$$

for any nontrivial character (χ_1, χ_2) of G. Generally, $(2k_2 - v_2)\chi_1(D_1) + k_2 - v_2$ and $(2\chi_1(D_1) + 1)\chi_2(D_2)$ are not of constant magnitude, they are of constant magnitude when D_1 is a certain TCVS.

Theorem 3.3 *Let D_1 be a SHDS in an abelian group H_1 of order v_1, and D_2 be a (v_2, k_2, λ_2) difference set in an abelian group H_2. Then the subset D in the group $G = H_1 \times H_2$ given by*

$$D = D_1 \times D_2 \cup (H_1 - D_1 - e) \times (H_2 - D_2)$$

and the subset $D \cup H_2$ are both divisible difference sets relative to H_1, provided $v_1 = v_2$ and H_2 is a Hadamard difference set.

Similarly, when $e \notin D_i$, $i = 1, 2$, we have

Theorem 3.4 *Let D_1 be a SHDS in an abelian group H_1 of order v_1, and D_2 be a $(v_2, k, \lambda, \mu, -1, \Delta)$ regular partial difference set in an abelian group H_2. Let D be a subset in the group $G = H_1 \times H_2$ defined by*

$$D = D_1 \times D_2 \cup (H_1 - D_1 - e) \times (H_2 - D_2 - e).$$

(1) *If $v_1 = \Delta + 2$, then D, $D \cup H_2$, $D \cup (H_1 \backslash e)$, and $D \cup H_2 \cup H_1$ are divisible difference sets relative to H_2. Furthermore, if $\Delta = v_2$, $D \cup H_2$ is a Hadamard difference set.*
(2) *If $v_1 = \Delta - 2$, then $D \cup H_1$ and $D \cup (H_2 \backslash e)$ are divisible difference sets relative to H_2. Furthermore, if $\Delta = v_2$, $D \cup H_1$ is a Hadamard difference set, and D and $D \cup H_2 \cup H_1$ are divisible difference sets relative to H_1.*

These three theorems can be proved in a similar way by using the character theory. Below we just give the proof of Theorem 3.4.

Proof Let $v_1 = |H_1|$. For any nontrivial character χ_1 of H_1 and nontrivial character χ_2 of H_2, $\chi_1(D_1) = \frac{-1\pm\sqrt{-v_1}}{2}$, and $\chi_2(D_2) = \frac{-1\pm\sqrt{\Delta}}{2}$, then

$$\begin{aligned}(\chi_1, \chi_2)(D) &= \chi_1(D_1)\chi_2(D_2) + (-\chi_1(D_1) - 1)(-\chi_2(D_2) - 1)\\ &= \tfrac{1}{2}((2\chi_1(D_1) + 1)(2\chi_2(D_2) + 1) + 1)\\ &= \tfrac{1\pm\sqrt{-v_1\Delta}}{2}.\end{aligned}$$

For the trivial character χ_0 of H_1 and any nontrivial character χ_2 of H_2, we have

$$\begin{aligned}(\chi_0, \chi_2)D &= \tfrac{v_1-1}{2}\chi_2(D_2) + \tfrac{v_1-1}{2}(-\chi_2(D_2) - 1)\\ &= -\tfrac{v_1-1}{2}.\end{aligned}$$

Finally, for any nontrivial character χ_1 of H_1 and the trivial character χ_0 of H_2, we have

$$\begin{aligned}(\chi_1, \chi_0)D &= k\chi_1(D_1) + (v_2 - k - 1)(-\chi_1(D_1) - 1)\\ &= (2k + 1 - v_2)\chi_1(D_1) - (v_2 - k - 1)\\ &= -\tfrac{v_2-1}{2} \pm \tfrac{(2k+1-v_2)\sqrt{-v_1}}{2}.\end{aligned}$$

If $v_1 = \Delta + 2$, $v_1 - 1 = |1 \pm \sqrt{-v_1\Delta}|$, then D, $D \cup H_2$, $D \cup (H_1\backslash e)$, and $D \cup H_2 \cup H_1$ are all divisible difference sets relative to H_2. Furthermore, if $\Delta = v_2$, then $v_2 = 2k + 1$ follows Theorem 2.9. Hence, $D \cup H_2$ is a Hadamard difference set.

If $v_1 = \Delta - 2$, $v_1 + 1 = |1 \pm \sqrt{-v_1\Delta}|$, then $D \cup H_1$ and $D \cup (H_2\backslash e)$ are divisible difference sets relative to H_2. Furthermore, if $\Delta = v_2$, then $v_2 = 2k + 1$ follows Theorem 2.9. Hence, $D \cup H_1$ is a Hadamard difference set, and D and $D \cup H_2 \cup H_1$ are divisible difference sets relative to H_1. □

Remark: 1. Twin prime power difference sets (we refer the reader to [2, Theorem 5.27, p. 131]) and [8, Theorems 5.1 and 5.2] are two special cases of the Hadamard difference sets in Theorem 3.4.

2. In Theorem 3.4, since $gcd(|H_1|, |H_2|) = 1$, we have $Aut(G) = Aut(H_1) \times Aut(H_2)$. Hence, if D_1 and D_1' are two SHDS in H_1 and D_2 and D_2' are two regular partial difference sets with same parameters, then D and D' are equivalent if and only if D_1 and D_2 are respectively equivalent to D_1' and D_2', or to D_1' and $H_2 - D_2' - e$.

Some examples from Theorems 3.3 and 3.4 are listed below.

1. Let D_1 be a Paley difference set in a group H_1 of order 27. Then $D = D_1 \times D_1 \cup (H_1 - D_1 - e) \times (H_1 - D_1)$ is a (729, 27, 351, 162, 169) divisible difference set in $H_1 \times H_1$ relative to $H_1 \times e$.

2. Let $D_1 = P$, $DY(\pm 1)$, $RT(\pm 1)$, or $DY(\pm 1)^*$ be a SHDS in $(\mathbf{F}_{243}, +)$ (we will define and discuss these seven sets in Sect. 4), and D_2 be the (241, 120, 59, 60) regular partial difference set in H_2 formed by all quadratic residues modulo 241. Then

$$D_1 \times D_2 \cup (H_1 - D_1 - e) \times (H_2 - D_2 - e) \cup H_2$$

are 7 pairwise inequivalent Hadamard difference sets in $H_1 \times H_2$.

3. Let D_1 be the Paley difference set in $H_1 = (\mathbf{F}_{83}, +)$, and D_2 be the Paley partial difference set, or biquadratic residues partial difference set P^* (not the dual set here) [18], or the Dickson partial difference set [20] in $H_2 = (\mathbf{F}_{81}, +)$. Then

$$D_1 \times D_2 \cup (H_1 - D_1 - e) \times (H_2 - D_2 - e) \cup H_2$$

are 3 pairwise inequivalent Hadamard difference sets in $H_1 \times H_2$.

4. Let D_1 be the Paley difference set in $H_1 = (\mathbf{F}_{83}, +)$, D_2 be a $(81, 40, 19, 20)$ partial difference set in $H_2 = \mathbf{Z}_9 \times \mathbf{Z}_9$ (We refer readers to Leifman and Muzychuk [13] and Leung and Ma [14].) Then

$$D_1 \times D_2 \cup (H_1 - D_1 - e) \times (H_2 - D_2 - e) \cup H_2$$

is Hadamard difference set in $\mathbf{Z}_{747} \times \mathbf{Z}_9$.

5. Let D_1 be the Paley difference sets in $H_1 = (\mathbf{F}_{83}, +)$, D_2 be a $(243, 22, 1, 2)$ partial difference set in $H_2 = (\mathbf{F}_{243}, +)$. Then

$$D_1 \times D_2 \cup (H_1 - D_1 - e) \times (H_2 - D_2 - e)$$

is $(83, 243, 9922, 8241, 4840)$ divisible difference set in $H_1 \times H_2$ relative to H_2.

It should be noted that Theorems 3.2, 3.3, and 3.4 can be proved in the group ring notion where the condition that H_1 and H_2 are abelian is not necessarily assumed. The reader can do this by calculating $DD^{(-1)}$. For instance, we state the construction of Hadamard difference sets as the following corollary.

Corollary 3.5 *Let D_1 be a SHDS in a group H_1 of order v_1, and let D_2 be a $(v_2, \frac{v_2-1}{2}, \frac{v_2-5}{4}, \frac{v_2-1}{4})$ regular partial difference set in a group H_2. Define D as a subset in the group $G = H_1 \times H_2$ by*

$$D = D_1 \times D_2 \cup (H_1 - D_1 - e) \times (H_2 - D_2 - e).$$

(1) *When $v_1 = v_2 + 2$, then $D \cup H_2$ is a Hadamard difference set in G.*
(2) *When $v_1 = v_2 - 2$, then $D \cup H_1$ is a Hadamard difference set in G.*

In [12], all difference sets with $k < 20$ are listed. There are two Hadamard difference sets D_1 and D_2 in a nonabelian group G of order 27, and moreover, D_1 is a SHDS, where

$$G = \langle a, b \mid a^3 = b^9 = e, a^{-1}ba = b^4 \rangle,$$
$$D_1 = b + b^5 + b^6 + b^7 + a(e + b + b^2 + b^3 + b^4 + b^6) + a^2(b + b^5 + b^7),$$
$$D_2 = e + b + b^3 + b^4 + b^5 + b^7 + a(e + b + b^2 + b^6) + a^2(e + b^2 + b^3).$$

Thus, we can get new Hadamard difference sets in nonabelian group $G \times \mathbf{Z}_{29}$ and $G \times \mathbf{Z}_5^2$ by Corollary 3.5, and can also get $(27, 27, 351, 162, 169)$ divisible difference sets in $G \times G$ and $G \times \mathbf{Z}_3^3$.

4 Skew Hadamard difference sets in elementary abelian groups

A classical example of SHDS is the Paley difference sets in the additive groups of finite fields $\mathbf{F}_q$ formed by the nonzero squares of $\mathbf{F}_q$, where $q \equiv 3 (\bmod 4)$. Recently, Ding and Yuan give a new construction for SHDS in [7], and another construction for SHDS is given by Ding et al. [8]. We conclude these as the following theorem.

Theorem 4.1 *Let $\mathbf{F}_q$ be the finite field of order q. Then the subsets*

$$P = \{x^2 \mid x \in \mathbf{F}_q, x \neq 0\},$$
$$DY(\pm 1) = \{x^{10} \pm x^6 - x^2 \mid x \in \mathbf{F}_q = \mathbf{F}_{3^h}, x \neq 0\},$$
$$RT(\pm 1) = \{x^{4\alpha+6} \pm x^{2\alpha} - x^2 \mid x \in \mathbf{F}_q = \mathbf{F}_{3^h}, x \neq 0\},$$

are SHDS in the additive groups of $\mathbf{F}_q$, where h is odd and $\alpha = 3^{\frac{h+1}{2}}$. Furthermore, they are pairwise inequivalent when $q = 3^5$ and 3^7.

Let D be a SHDS in an abelian group G with $|G| = v = 4n - 1$. Then

$$DD^{(-1)} = ne + (n-1)G, \quad D^{(-1)} = G - D - e,$$

and

$$D^2 = nG - ne - D, (D^{(-1)})^2 = (n-1)G - (n-1)e + D.$$

Thus, the subalgebra of $\mathbf{C}[G]$ spanned by e, D, and $D^{(-1)}$ is of dimension 3. It follows that for any integers s and t,

$$D^s(D^{(-1)})^t = n_1 e + n_2 D + n_3 D^{(-1)},$$

holds for some integers n_1, n_2, and n_3.

Lemma 4.2 *Let D be a SHDS in an abelian group G with $|G| > 3$, $g \in G$ and $\sigma \in Aut(G)$. Then $g\sigma(D)$ is again a SHDS if and only if $g = e$.*

Proof Obviously, D is SHDS if and only if $\sigma(D)$ is SHDS, so we assume without loss of generality that σ is the identity automorphism. When both D and gD are SHDS, we have $D^2 = nG - ne - D$ and $(gD)^2 = nG - ne - (gD)$, where $n = \frac{v+1}{4} > 1$. Thus $g = e$ follows that $nG - ng^2 - g^2 D = nG - ne - (gD)$. □

This lemma implies that there exists an automorphism σ such that $D = \sigma(E)$ if D and E are two equivalent SHDS. Lemma 4.2 still holds when G is replaced by the nonabelian group of order 27 mentioned in Sect. 3.

Lemma 4.3 *Let D be a SHDS in an elementary abelian group G. Then $\prod_{g \in D} g = e$ if $|G| > 3$.*

Proof Set $d = \prod_{g \in D} g$. For any quadratic residue t modulo p, we have $D^{(t)} = D$. Hence, $d^t = \prod_{g \in D} g^t = \prod_{h \in D^{(t)}} h = d$. When $p > 3$, there exist a quadratic residue t such that $(t-1, p) = 1$, and hence, $d = e$. When G is elementary abelian and of order $3^h > 3$, we can give a proof which follows by Lemma 4.4 and Corollary 4.5. □

Lemma 4.4 *Let D be a SHDS in an abelian group G, and e be the identity of G. Denote by $P_{st}(a)$ the number of the solutions to the equation*

$$x_1 x_2 \ldots x_s y_1 y_2 \ldots y_t = a, \quad x_i \in D, \;\; y_j \in D^{(-1)}.$$

Then

$$P_{st}(a) = \begin{cases} n_1, & \text{if } a = e, \\ n_2, & \text{if } a \in D, \\ n_3, & \text{if } a \in D^{(-1)}, \end{cases}$$

where n_1, n_2, and n_3 are defined by $D^s(D^{(-1)})^t = n_1 e + n_2 D + n_3 D^{(-1)}$.

Corollary 4.5 *Let D be a SHDS in an elementary abelian group G of order 3^h. Denote by $Q_{st}(a)$ the number of solutions to following equation*

$$x_1 x_2 \ldots x_s y_1 y_2 \ldots y_t = a,$$

where $x_i \in D$, $y_j \in D^{(-1)}$, and the $\langle x_i \rangle$ and the $\langle y_j \rangle$ are pairwise distinct subgroups. Here the notation $\langle g \rangle$ denotes the subgroup of G generated by element g. Then

$$Q_{st}(a) = \begin{cases} m_1, & \text{if } a = e, \\ m_2, & \text{if } a \in D, \\ m_3, & \text{if } a \in D^{(-1)}, \end{cases}$$

where m_1, m_2, m_3 are some integers depended on s and t. In particular, if $h > 1$, then $\prod_{g \in D} g = e$.

Proof We prove the first statement by induction on $s + t$. The case that $s + t = 1$ is trivial, and let us assume the statement is true for any $s + t < n$.

For given s, t with $s + t = n$, we consider the solution $(g_1, g_2, \ldots, g_n)$ to the equation

$$x_1 x_2 \ldots x_s y_1 y_2 \ldots y_t = a, \quad x_i \in D, y_j \in D^{(-1)},$$

where $s + t = n$, $x_i = g_i$ and $y_j = g_{s+j}$. Let $A = \{A_1, A_2, \ldots, A_m\}$ be a partition of $\bigcup_{i=1}^{m} A_i = \{1, 2, \ldots, n\}$, $A_i \neq \emptyset$ and $A_i \cap A_j = \emptyset$ if $i \neq j$. We call the solution $(g_1, g_2, \ldots, g_n)$ is *type* A, if $\langle g_i \rangle = \langle g_j \rangle$ holds if and only if there exists k such that $i, j \in A_k$. We also denoted by $N(A, a)$ the number of the type A solutions.

Since G is an elementary abelian group of order 3^h, $\langle g \rangle = \{e, g, g^{-1}\}$. Note that $|\langle g \rangle \cap D| = 1$, then we have

$$f_1^{a_1 - b_1} f_2^{a_2 - b_2} \ldots f_m^{a_m - b_m} = a,$$

where $f_i = D \cap \langle g_j \rangle$ with $j \in A_i$, $a_i = |A_i \cap \{1, 2, \ldots, s\}|$ and $b_i = |A_i| - a_i$. Without loss of generality, we assume:

$$\begin{aligned} a_i - b_i &\equiv 1 (\text{mod } 3), \quad i = 1, 2, \ldots, s_1, \\ a_i - b_i &\equiv 2 (\text{mod } 3), \quad i = s_1 + 1, s_1 + 2, \ldots, s_1 + t_1, \\ a_i - b_i &\equiv 0 (\text{mod } 3), \quad i = s_1 + t_1 + 1, s_1 + t_1 + 2, \ldots, m. \end{aligned}$$

Let $z_1, z_2, \ldots, z_{s_1+t_1}$ be $s_1 + t_1$ different elements in D such that $z_1 z_2 \ldots z_{s_1} z_{s_1+1}^{-1} z_{s_1+2}^{-1} \ldots z_{s_1+t_1}^{-1} = a$. Then for any $m - s_1 - t_1$ different elements in $D \setminus \{z_1, z_2, \ldots, z_{s_1+t_1}\}$, $z_{s_1+t_1+1}$, $z_{s_1+t_1+2}, \ldots, z_m$, we have a solution $(g_1, g_2, \ldots, g_n)$ of type A:

$$g_i = \begin{cases} z_j, & \text{if } i \leq s \quad \text{and } i \in A_j, \\ z_j^{-1}, & \text{if } i > s \quad \text{and } i \in A_j. \end{cases}$$

Thus $N(A, a) = \frac{(v - s_1 - t_1)!}{(v - m)!} Q_{s_1 t_1}(a)$, where $|D| = v$.
If $m < n$, then $s_1 + t_1 < n$. By the induction assumption, we have

$$N(A, a) = \begin{cases} N_1, & \text{if } a = e, \\ N_2, & \text{if } a \in D, \\ N_3, & \text{if } a \in D^{(-1)}. \end{cases}$$

If $m = n$, then $N(A, a) = Q_{st}(a)$. As

$$P_{st}(a) = \sum_A N(A, a),$$

we complete the proof of first statement by Lemma 4.4.

In particular, when $|G| = 3^h > 3$, setting $s = \frac{3^h-1}{2}$ and $t = 0$, $d = \prod_{g\in D} g$. We have

$$Q_{st}(a) = \begin{cases} s!, & \text{if } a = d, \\ 0, & \text{if } a \neq d. \end{cases}$$

Thus we have $d = e$. □

By Lemmas 4.2 and 4.3, we can easily check whether a given Hadamard difference set in the elementary abelian group is equivalent to some SHDS or not.

Theorem 4.6 *Let D be a Hadamard difference set in an elementary abelian group G, and $d = \prod_{g\in D} g$. Then D is equivalent to some SHDS if and only if $d^2 D$ is a SHDS.*

Proof By Lemma 4.2, if D is equivalent to a SHDS, then there exists an element $h \in G$ such that hD is a SHDS. By Lemma 4.3, we have $e = \prod_{g\in hD} g = h^{|D|} \prod_{g\in D} g$. Thus $h = d^2$. □

Corollary 4.7 *Any Hall difference set, which is the union of three cosets of the sextic residues are inequivalent to any SHDS. (We refer the reader to Baumert [2] and Storer [19] for the details of Hall difference sets.)*

For the dual sets of SHDS, we have

Theorem 4.8 *Let D and E be two SHDS in an abelian group G. Then D and E are equivalent if and only if D^* and E^* are equivalent in $\widehat{G}$.*

Proof Let σ be an automorphism of G. Note the map

$$\widehat{\sigma} : \chi \mapsto \chi \circ \sigma$$

is an automorphism of $\widehat{G}$, where $\widehat{\sigma}(\chi)(g) = \chi(\sigma(g)), \forall g \in G$. Thus if $D = \sigma(E)$, then $\chi(D) = \chi(\sigma(E)) = \widehat{\sigma}(\chi)(E)$, that is $D^* = \widehat{\sigma}(E^*)$. Another direction of the assertion holds from $D^{**} = D^{(-1)}$. □

P, $DY(\pm 1)$, $RT(\pm 1)$, and their dual sets are all known SHDS up to date, below we discuss the inequivalence among these ten families of SHDS.

Note that any character χ_a of $(\mathbf{F}_q, +)$ can be written as

$$\chi_a(x) = \xi^{\mathrm{Tr}(ax)}, \quad \forall a \in \mathbf{F}_q,$$

where $\xi = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a pth primitive root of unity in $\mathbf{C}$, p is the characteristic of $\mathbf{F}_q$, $q = p^m$, and Tr is the trace map from $\mathbf{F}_q$ to $\mathbf{F}_p$ defined by

$$\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{p^i}.$$

Let η be the quadric character of the multiplicative group of $\mathbf{F}_q$, that is, η maps all squares of $\mathbf{F}_q$ to 1 and maps all non-squares to -1, and convention that $\eta(0) = 0$. From

$$\begin{aligned} \chi_a(P) &= \sum_{x\in P} \xi^{\mathrm{Tr}(ax)} \\ &= \frac{1}{2}\left(\sum_{x\in \mathbf{F}_q} \eta(x)\xi^{\mathrm{Tr}(ax)} - 1 \right) \\ &= \frac{1}{2}\left(\eta(a) \sum_{x\in \mathbf{F}_q} \eta(x)\xi^{\mathrm{Tr}(x)} - 1 \right), \end{aligned}$$

we have $\chi_a(P)$ depends on only $\eta(a)$. Hence, the dual set of P is equivalent to P. For other known SHDS, we generally have not an effective method to discuss their equivalence yet. With the help of a computer, we classify them in the cases of small parameters.

When $q = 3^5$ or 3^7, we checked the equivalence of the known SHDS by running through all automorphisms with computer programming. It turns out that $RT(1)^*$ is equivalent to $RT(-1)$, and P, $RT(\pm 1)$, $DY(\pm 1)$, and $DY(\pm 1)^*$ are all pairwise inequivalent. Furthermore, we confirmed the following formula by computer for $q = 3^h$ with $h = 1, 3, 5, 7, 9, 11$:

$$\sum_{x \in \mathbf{F}_q} \eta(x) \xi^{\mathrm{Tr}(a(x^{2\alpha+3}+x^{\alpha}-x))} = \begin{cases} (-1)^{\frac{h+1}{2}} \sqrt{-q}, & \text{if } a \in RT(-1), \\ (-1)^{\frac{h-1}{2}} \sqrt{-q}, & \text{if } a \notin RT(-1). \end{cases}$$

Thus, $RT(1)^*$ is equivalent to the dual set of $RT(-1)$ when $q = 3^h$ and $h = 1, 3, 5, 7, 9, 11$. We conjecture the above formula holds for any odd h, but we have no proof by now yet.

To search the (in) equivalence in the larger case of q, we introduce here an invariant called rank. For a SHDS $D \subset \mathbf{F}_q$, set B_D as a $q \times q$ matrix over $\mathbf{F}_q$, whose rows and columns are indexed by elements of $\mathbf{F}_q$, and its entry at row x and column y is $B_D(x, y) = f(x - y)$, where

$$f(x) = \begin{cases} 0, & x = 0, \\ 1, & x \in D, \\ -1, & x \in D^{(-1)}. \end{cases}$$

If D and E are two equivalent SHDS in an elementary abelian group G, that is, there exists an automorphism σ, $D = \sigma(E)$, and $D^{(-1)} = \sigma(E^{(-1)})$, then we have

$$B_D = P_\sigma B_E P'_\sigma,$$

where P_σ is a permutation matrix with entries $P_\sigma(x, y) = 1$ if and only if $y = \sigma(x)$. Hence matrices B_D and B_E have the same rank. When D is a Paley difference set and $f(x) = x^{\frac{q-1}{2}}$ with $q = p^h$, $rank(B_D) = (\frac{p+1}{2})^h$ (We refer the reader to Brouwer and van Eijl [3] for this rank calculation.). When $D = DY(\pm 1)$, then

$$f(x) = D_{\frac{1}{5}}(x, \pm 1)^{\frac{q-1}{2}},$$

where $D_{\frac{1}{5}}(x, a) = D_{\frac{3q^2-2}{5}}(x, a)$ is the Dickson polynomial of the first kind. It seems not easy to get the ranks by an algebraic way.

In Table 1, we list the ranks of the matrices B_D for all known SHDS for $q = 3^5, 3^7$, and 3^9.

Table 1 Ranks of known SHDS for $q = 3^5, 3^7$, and 3^9

	$q = 3^5$	$q = 3^7$	$q = 3^9$
P	32	128	512
$DY(1)$	42	226	1232
$DY(-1)$	42	226	1232
$RT(1)$	42	226	1178
$RT(-1)$	42	226	1178
$DY(1)^*$	42	226	1214
$DY(-1)^*$	42	226	1214

From Table 1, there are at least four pairwisely inequivalent SHDS when $q = 3^9$. We conjectured that P, $DY(\pm 1)$, $DY(\pm 1)^*$, $RT(\pm 1)$ are pairwisely inequivalent SHDS when $q \geq 3^5$.

Acknowledgments The authors would like to thank Prof. Q. Xiang and C. Ding for their helpful comments. The first author would like to thank Prof. W. Qiu for his guidance and encouragement.

References

1. Arasu K.T., Jungnickel D., Ma S.L., Pott A.: Strongly regular Cayley graphs with $\lambda - \mu = -1$. J. Combin. Theory (A) **67**, 116–125 (1994).
2. Baumert L.D.: Cyclic Difference Sets. Springer Lecture Notes, vol. 182. Springer, Berlin (1971).
3. Brouwer A.E., van Eijl C.A.: On the p-rank of the adjacency matrices of strongly regular graphs. J. Algebraic Combin. **1**, 329–346 (1992).
4. Camion P., Mann H.B.: Antisymmetric difference sets. J. Number Theory **4**, 266–268 (1972).
5. Chen Y.Q., Xiang Q., Sehgal S.: An exponent bound on skew Hadamard abelian difference sets. Des. Codes Cryptogr. **4**, 313–317 (1994).
6. Delsarte P.: An algebraic approach to the association schemes of coding theory. Philips Research Report. Suppl. No. 10 (1973).
7. Ding C., Yuan J.: A family of skew Hadamard difference sets. J. Combin. Theory (A) **113**, 1526–1535 (2006).
8. Ding C., Wang Z., Xiang Q.: Skew Hadamard difference sets from Ree-Tits slice symplectic spreads in $PG(3, 3^{2h+1})$. J. Combin. Theory Ser. A **114**, 867–887 (2007).
9. Hughes D.R., van Lint J.H., Wilson R.M.: Announcement at the Seventh British Combinatorial Conference, Cambridge (1979), Unpublished.
10. Johnsen E.C.: Skew-Hadamard abelian group difference sets. J. Algebra **4**, 388–402 (1966).
11. Jungnickel D.: On λ-ovals and difference sets. In: Contemporary Methods in Graph Theory, pp. 429–448. Bibliographisches Inst., Mannheim (1990).
12. Kibler R.E.: A summary of noncyclic difference sets, $k < 20$. J. Combin. Theory Ser. A **25**, 62–67 (1978).
13. Leifman Y.I., Muzychuk M.E.: Strongly regular Cayley graphs over the group $\mathbf{Z}_{p^n} \oplus \mathbf{Z}_{p^n}$. Discrete Math. **305**, 219–239 (2005).
14. Leung K.H., Ma S.L.: Partial difference sets with Paley parameters. Bull. London Math. Soc. **27**, 553–564 (1995).
15. Ma S.L.: Partial difference sets. Discrete Math. **52**, 75–89 (1984).
16. Ma S.L.: Polynomial addition sets and symmetric difference sets. In: Ray-Chaudhuri D. (ed.) Coding Theory and Design Theory, part 2, pp. 273–279. Springer, New York (1990).
17. Menon P.K.: On difference sets whose parameters satisfy a certain relation. Proc. Amer. Math. Soc. **13**, 739–745 (1962).
18. Peisert W.: All self-complementary symmetric graphs. J. Algebra **240**, 209–229 (2001).
19. Storer T.: Cyclotomy and Difference Sets. Markham Publishing Comp., Chicago (1967).
20. Weng G., Qiu W., Wang Z., Xiang Q.: Pseudo-Paley graphs and skew Hadamard difference sets from commutative semifields. Des. Codes Cryptogr. **44**, 49–62 (2007).
21. Xiang Q.: Note on Paley partial difference sets. In: Group, Difference Sets, and the Monster (Columbus, OH 1993), pp. 239–244. Ohio State Univ. Math. Res. Inst. Publ., 4, de Gruyter, Berlin (1996).