Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Journal of Combinatorial Theory, Series A 114 (2007) 867–887
Journal of Combinatorial Theory
Series A
www.elsevier.com/locate/jcta

Skew Hadamard difference sets from the Ree–Tits slice symplectic spreads in PG(3, 3^{2h+1}) ☆

Cunsheng Ding [a], Zeying Wang [b], Qing Xiang [b]

[a] *Department of Computer Science, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong*

[b] *Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA*

Received 7 February 2006

Available online 13 November 2006

Abstract

Using a class of permutation polynomials of $\mathbb{F}_{3^{2h+1}}$ obtained from the Ree–Tits slice symplectic spreads in PG(3, 3^{2h+1}), we construct a family of skew Hadamard difference sets in the additive group of $\mathbb{F}_{3^{2h+1}}$. With the help of a computer, we show that these skew Hadamard difference sets are new when $h = 2$ and $h = 3$. We conjecture that they are always new when $h > 3$. Furthermore, we present a variation of the classical construction of the twin prime power difference sets, and show that inequivalent skew Hadamard difference sets lead to inequivalent difference sets with twin prime power parameters.

Keywords: Difference set; Gauss sum; Permutation polynomial; Ree–Tits slice spread; Skew Hadamard difference set; Symplectic spread; Twin prime power difference set

1. Introduction

Let G be a finite group of order v (written multiplicatively). A k-element subset D of G is called a (v, k, λ) *difference set* if the list of "differences" xy^{-1}, $x, y \in D$, $x \neq y$, represents each nonidentity element in G exactly λ times. As an example of difference sets, we mention the classical Paley difference set in $(\mathbb{F}_q, +)$ consisting of the nonzero squares of $\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field of order q, and q is a prime power congruent to 3 modulo 4. Difference sets are the subject of much study in the past 50 years. We assume that the reader is familiar with the

☆ Research supported in part by NSF Grant DMS 0400411.
E-mail addresses: cding@ust.hk (C. Ding), wangz@math.udel.edu (Z. Wang), xiang@math.udel.edu (Q. Xiang).

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2006.09.008

basic theory of difference sets as can be found in [2,15], and [4, Chapter 6]. For a recent survey, see [20].

A difference set D in a finite group G is called *skew Hadamard* if G is the disjoint union of D, $D^{(-1)}$, and $\{1\}$, where $D^{(-1)} = \{d^{-1} \mid d \in D\}$. The aforementioned Paley difference set in $(\mathbb{F}_q, +)$ is an example of skew Hadamard difference sets. Let D be a (v, k, λ) skew Hadamard difference set in an abelian group G. Then we have

$$1 \notin D, \quad k = \frac{v-1}{2} \quad \text{and} \quad \lambda = \frac{v-3}{4}.$$

If we employ group ring notation, then in $\mathbb{Z}[G]$, we have

$$DD^{(-1)} = \frac{v+1}{4} + \frac{v-3}{4}G,$$
$$D + D^{(-1)} = G - 1,$$

where $D^{(-1)} = \sum_{d \in D} d^{-1}$. Applying any nonprincipal (complex) character ϕ of G to the above two equations, one has

$$\phi(D) = \frac{-1 \pm \sqrt{-v}}{2}. \tag{1.1}$$

Therefore the complex character values of a (v, k, λ) skew Hadamard abelian difference set all lie in the quadratic extension $\mathbb{Q}(\sqrt{-v})$ of $\mathbb{Q}$. This property of abelian skew Hadamard difference sets places severe restrictions on these difference sets. Skew Hadamard difference sets were studied by Johnsen [11], Camion and Mann [5], Jungnickel [12], and Chen, Xiang and Sehgal [7]. The results in [5,7,11] can be summarized as follows:

Theorem 1.1. *Let D be a (v, k, λ) skew Hadamard difference set in an abelian group G. Then v is equal to a prime power $p^m \equiv 3 \pmod 4$, and the quadratic residues modulo v are multipliers of D. Moreover, if G has exponent p^s with $s \geqslant 2$, then $s \leqslant (m+1)/4$. In particular, if $v = p^3$ or p^5, then G must be elementary abelian.*

It was conjectured that if an abelian group G contains a skew Hadamard difference set, then G has to be elementary abelian. This conjecture is still open in general. Theorem 1.1 contains all known results on this conjecture. It was further conjectured some time ago that the Paley difference sets are the only examples of skew Hadamard difference sets in abelian groups. This latter conjecture was recently disproved by Ding and Yuan [8], who constructed new skew Hadamard difference sets in $(\mathbb{F}_{3^{2h+1}}, +)$ by using certain planar functions related to Dickson polynomials.

In this paper we construct new skew Hadamard difference sets by using certain permutation polynomials [1] from the Ree–Tits slice symplectic spreads in $\mathrm{PG}(3, 3^{2h+1})$. While the construction itself is quite simple (see Section 3), the proof that the candidate sets are indeed difference sets is not so easy: we had to resort to a lemma in [7] and use Gauss sums and Stickelberger's theorem on the prime ideal factorization of Gauss sums. To make the paper self-contained, we include a brief introduction to Gauss sums here.

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

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

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

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

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

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

Note that if χ_0 is the trivial multiplicative character of $\mathbb{F}_q$, then $g(\chi_0) = -1$. Gauss sums can be viewed as the Fourier coefficients in the Fourier expansion of $\psi|_{\mathbb{F}_q^*}$ in terms of the multiplicative characters of $\mathbb{F}_q$. That is, for every $c \in \mathbb{F}_q^*$,

$$\psi(c) = \frac{1}{q-1} \sum_{\chi \in X} g(\chi)\chi^{-1}(c), \tag{1.2}$$

where X denotes the character group of $\mathbb{F}_q^*$.

One of the elementary properties of Gauss sums is [3, Theorem 1.1.4]

$$g(\chi)\overline{g(\chi)} = q, \quad \text{if } \chi \neq \chi_0. \tag{1.3}$$

A deeper result on Gauss sums is Stickelberger's theorem (Theorem 1.2 below) on the prime ideal factorization of Gauss sums. We first introduce some notation. Let a be any integer not divisible by $q-1$. We use $L(a)$ to denote the least positive integer congruent to a modulo $q-1$. Write $L(a)$ to the base p so that

$$L(a) = a_0 + a_1 p + \cdots + a_{m-1} p^{m-1},$$

where $0 \leqslant a_i \leqslant p-1$ for all i, $0 \leqslant i \leqslant m-1$. We define the *digit sum* of $a \pmod{q-1}$ as

$$s(a) = a_0 + a_1 + \cdots + a_{m-1}.$$

For integers a divisible by $q-1$, we define $s(a) = 0$.

Next let ξ_{q-1} be a complex primitive $(q-1)$th root of unity. Fix any prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\xi_{q-1}]$ lying over p. Then $\mathbb{Z}[\xi_{q-1}]/\mathfrak{p}$ is a finite field of order q, which we identify with $\mathbb{F}_q$. Let $\omega_{\mathfrak{p}}$ be the Teichmüller character on $\mathbb{F}_q$, i.e., an isomorphism

$$\omega_{\mathfrak{p}} : \mathbb{F}_q^* \to \left\{1, \xi_{q-1}, \xi_{q-1}^2, \ldots, \xi_{q-1}^{q-2}\right\}$$

satisfying

$$\omega_{\mathfrak{p}}(\alpha) \pmod{\mathfrak{p}} = \alpha, \tag{1.4}$$

for all α in $\mathbb{F}_q^*$. The Teichmüller character $\omega_{\mathfrak{p}}$ has order $q-1$; hence it generates all multiplicative characters of $\mathbb{F}_q$.

Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q-1}, \xi_p]$ lying above $\mathfrak{p}$. For an integer a, let $\nu_{\mathfrak{P}}(g(\omega_{\mathfrak{p}}^{-a}))$ denote the $\mathfrak{P}$-adic valuation of $g(\omega_{\mathfrak{p}}^{-a})$. The following classical theorem is due to Stickelberger (see [16, p. 7], [3, p. 344]).

Theorem 1.2. *Let p be a prime, and $q = p^m$. Let a be any integer not divisible by $q-1$. Then*

$$\nu_{\mathfrak{P}}\left(g\left(\omega_{\mathfrak{p}}^{-a}\right)\right) = s(a).$$

The paper is organized as follows. In Section 2, we give a brief introduction to symplectic spreads in $\mathrm{PG}(3,q)$, and recall a theorem of Ball and Zieve [1] which shows that symplectic spreads in $\mathrm{PG}(3,q)$ give rise to permutation polynomials of $\mathbb{F}_q$ and vice versa. In particular, we recall a class of permutation polynomials $f_a(x)$ of $\mathbb{F}_{3^m}$, $a \in \mathbb{F}_{3^m}$, coming from the Ree–Tits slice symplectic spreads. In Section 3, we use the aforementioned permutation polynomials

$f_a(x)$ to construct skew Hadamard difference sets in $(\mathbb{F}_{3^m}, +)$. In Section 4, we address the inequivalence issues for skew Hadamard difference sets in $(\mathbb{F}_{3^m}, +)$. Finally in Section 5, we present a variation of the classical construction of the twin prime power difference sets. Also we show that inequivalent skew Hadamard difference sets can give rise to inequivalent difference sets with twin prime power parameters.

2. A class of permutation polynomials from the Ree–Tits slice symplectic spreads in PG(3, 3^{2h+1})

Let $\mathrm{PG}(3, q)$ denote the 3-dimensional projective space over $\mathbb{F}_q$, and let $V = \mathbb{F}_q^4$ be the underlying vector space of $\mathrm{PG}(3, q)$. A *spread* of $\mathrm{PG}(3, q)$ is a partition of the points of the space into lines. Now we equip V with a nondegenerate alternating form $B : V \times V \to \mathbb{F}_q$. A spread of $\mathrm{PG}(3, q)$ is called *symplectic* if every line of the spread is totally isotropic with respect to B. Since all nondegenerate alternating forms on V are equivalent, we may assume that B is defined as follows:

$$B\big((x_0, x_1, x_2, x_3), (y_0, y_1, y_2, y_3)\big) = x_0y_3 - x_3y_0 - x_1y_2 + y_1x_2. \tag{2.1}$$

Then a symplectic spread is a partition of the points of $\mathrm{PG}(3, q)$ into lines such that $B(P, Q) = 0$ for any points P, Q lying on the same line of the spread. For readers who are familiar with classical generalized quadrangles, a symplectic spread of $\mathrm{PG}(3, q)$ is nothing but a spread of the classical generalized quadrangle $W_3(q)$. By the Klein correspondence (see [9]), a spread of $W_3(q)$ corresponds to an ovoid of the classical generalized quadrangle $Q(4, q)$.

In [1], it was shown that every symplectic spread of $\mathrm{PG}(3, q)$ gives rise to a certain family of permutation polynomials of $\mathbb{F}_q$ and vice versa. Since the symplectic group $\mathrm{Sp}(V)$ leaving the alternating form in (2.1) invariant acts transitively on the set of totally isotropic lines, we may assume that the symplectic spread under consideration contains the line

$$\ell_\infty = \big\langle (0, 0, 0, 1), (0, 0, 1, 0) \big\rangle.$$

Theorem 2.1. [1] *The set of totally isotropic lines*

$$\ell_\infty \cup \big\{ \big\langle (0, 1, x, y), \big(1, 0, -y, g(x, y)\big) \big\rangle \,\big|\, x, y \in \mathbb{F}_q \big\} \tag{2.2}$$

is a symplectic spread of $\mathrm{PG}(3, q)$ *if and only if*

$$x \mapsto g(x, ax - b) + a^2x$$

is a permutation of $\mathbb{F}_q$ *for all* $a, b \in \mathbb{F}_q$.

Table 1 in [1] lists all known symplectic spreads of $\mathrm{PG}(3, q)$. For our purpose of constructing new skew Hadamard difference sets, we are interested in the Ree–Tits slice symplectic spread, which is a spread having the form (2.2), with

$$g(x, y) = -x^{2\alpha+3} - y^\alpha,$$

where $q = 3^{2h+1}$ and $\alpha = \sqrt{3q}$. This spread was discovered by Kantor [14] as an ovoid of $Q(4, q)$, which is a slice of the Ree–Tits ovoid of $Q(6, q)$.

By Theorem 2.1 the Ree–Tits example gives us a class of permutation polynomials, namely, the polynomials $f_a(x) = b^\alpha - (g(x, ax - b) + a^2x)$, $a \in \mathbb{F}_q$. Explicitly, we have

$$f_a(x) = x^{2\alpha+3} + (ax)^\alpha - a^2x. \tag{2.3}$$

As commented in [1], the polynomial f_a is remarkable in that it is a permutation polynomial of $\mathbb{F}_q$ whose degree is approximately $\sqrt{q}$. There are only a handful of known permutation polynomials with such a low degree. A direct proof that $f_a(x)$ is a permutation polynomial can be found in [1].

We comment that by going through Table 1 in [1], one can see that all other permutation polynomials arising from known symplectic spreads of PG$(3, q)$, q odd, are linearized permutation polynomials of $\mathbb{F}_q$, which will not lead to new skew Hadamard difference sets by the construction described below. That is the reason why we only choose to work with the polynomials $f_a(x)$ defined in (2.3).

3. A construction of skew Hadamard difference sets

Throughout this section, $q = 3^m$, where $m = 2h + 1$, $h \geqslant 0$. For any $a \in \mathbb{F}_q$, let $f_a(x)$ be the polynomial defined in (2.3). As seen in Section 2, $f_a(x)$ is a permutation polynomial of $\mathbb{F}_q$. For any nonzero $a \in \mathbb{F}_q$, let

$$D_a = \left\{ f_a\left(x^2\right) \mid x \in \mathbb{F}_q^* \right\}, \tag{3.1}$$

where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. We will show that D_a is a skew Hadamard difference set in $(\mathbb{F}_q, +)$. We start with the following

Lemma 3.1. *For any nonzero $a \in \mathbb{F}_q$, we have*

$$D_a \cap (-D_a) = \emptyset,$$

and

$$D_a \cup (-D_a) \cup \{0\} = \mathbb{F}_q.$$

Proof. Assume that $f_a(x^2) = -f_a(y^2)$ for some $x, y \in \mathbb{F}_q^*$. Then

$$f_a\left(x^2\right) = f_a\left(-y^2\right).$$

Since $f_a(x)$ is a permutation polynomial of $\mathbb{F}_q$, we have $x^2 = -y^2$, which implies that -1 is a square in $\mathbb{F}_q$. But -1 is not a square in $\mathbb{F}_q$, since $q = 3^m$ and m is odd. Therefore we reached a contradiction. Hence $D_a \cap (-D_a) = \emptyset$.

Next, clearly we have $f_a(0) = 0$. Since $f_a(x)$ is a permutation polynomial of $\mathbb{F}_q$, we see that $f_a(x^2) = 0$ if and only if $x = 0$. Therefore $0 \notin D_a$. The second assertion of the lemma now follows easily. This completes the proof. □

We will use the character sum approach (see, e.g., [4, p. 318]) to prove that D_a is a difference set. Using this approach, in order to show that D_a is a difference set, we must prove that for any nontrivial additive character ψ of $\mathbb{F}_q$,

$$\psi(D_a)\overline{\psi(D_a)} = \frac{q+1}{4}. \tag{3.2}$$

It seems difficult to prove directly that (3.2) holds for every nontrivial additive characters ψ of $\mathbb{F}_q$. We will use a lemma in [7] to bypass this difficulty.

Lemma 3.2. [7] *Let G be a (multiplicative) abelian p-group of order p^m, where p is a prime congruent to 3 modulo 4, and m is an odd integer. Let D be a subset of G such that in $\mathbb{Z}[G]$,*

$$D + D^{(-1)} = G - 1,$$

and $D^{(t)} = D$ for every nonzero quadratic residue t modulo p. If for every nontrivial character ϕ of G,

$$\phi(D) \equiv \frac{p^{(m-1)/2} - 1}{2} \pmod{p^{(m-1)/2}},$$

then D is a difference set in G.

The idea of Lemma 3.2 is that sometimes congruence properties of $\phi(D)$ can be used to determine the (complex) absolute value of $\phi(D)$. The proof of the lemma relies on Fourier inversions, and can be found in [7].

We now state the main theorem of this section.

Theorem 3.3. *Let $a \in \mathbb{F}_q^*$, and let D_a be defined as in* (3.1)*. Then D_a is a skew Hadamard difference set in $(\mathbb{F}_q, +)$.*

Proof. By Lemma 3.1, we know that D_a is skew. Since $1 \in \mathbb{Z}/3\mathbb{Z}$ is the only nonzero quadratic residue modulo 3, we certainly have $D_a^{(t)} = D_a$ for every nonzero quadratic residue t modulo 3. Therefore by Lemma 3.2, it suffices to show that for every nontrivial additive character $\psi_\beta : \mathbb{F}_q \to \mathbb{C}^*$,

$$\psi_\beta(D_a) \equiv \frac{3^{(m-1)/2} - 1}{2} \pmod{3^{(m-1)/2}}, \tag{3.3}$$

where $\psi_\beta(x) = \xi_3^{\mathrm{Tr}(\beta x)}$, $\xi_3 = e^{2\pi i/3}$, and Tr is the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_3$.

We now compute $\psi_\beta(D_a)$. Let χ be the (multiplicative) quadratic character of $\mathbb{F}_q$. Then

$$\begin{aligned}\psi_\beta(D_a) &= \sum_{x\in\mathbb{F}_q^*} \psi_\beta\big(f_a(x)\big)\frac{(\chi(x)+1)}{2} = \frac{1}{2}\Bigg(\sum_{x\in\mathbb{F}_q^*} \psi_\beta\big(f_a(x)\big)\chi(x) + \sum_{x\in\mathbb{F}_q^*} \psi_\beta\big(f_a(x)\big)\Bigg)\\ &= \frac{1}{2}\Bigg(\sum_{x\in\mathbb{F}_q^*} \psi_\beta\big(f_a(x)\big)\chi(x) - 1\Bigg),\end{aligned}$$

where in the last equality we used the facts that $f_a(x)$ is a permutation polynomial of $\mathbb{F}_q$ and $f_a(0) = 0$. From this last expression for $\psi_\beta(D_a)$, we see that (3.3) is equivalent to

$$\sum_{x\in\mathbb{F}_q^*} \psi_\beta\big(f_a(x)\big)\chi(x) \equiv 0 \pmod{3^h}. \tag{3.4}$$

Let $S_\beta = \sum_{x\in\mathbb{F}_q^*} \psi_\beta(f_a(x))\chi(x)$. We have

$$\begin{aligned}S_\beta &= \sum_{x\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(\beta x^{2\alpha+3} + (\beta a^\alpha - \beta^\alpha a^{2\alpha})x^\alpha)}\chi(x) = \sum_{y\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(\beta y^{\alpha+2} + (\beta a^\alpha - \beta^\alpha a^{2\alpha})y)}\chi(y)\\ &= \pm \sum_{y\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(y^{\alpha+2} + (\beta^{\alpha-1}a^\alpha - \beta^{2\alpha-2}a^{2\alpha})y)}\chi(y).\end{aligned}$$

Let $\gamma_a = \beta^{\alpha-1}a^\alpha - \beta^{2\alpha-2}a^{2\alpha}$. If $\gamma_a = 0$, then S_β is a quadratic Gauss sum, which can be evaluated exactly (see [17, p. 199]). Indeed, if $\gamma_a = 0$, then we have

$$S_\beta = \pm \sum_{y\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(y^{\alpha+2})}\chi(y) = \pm \sum_{z\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(z)}\chi(z) = \pm g(\chi) = \pm\sqrt{-q}$$
$$= \pm 3^h\sqrt{-3} \equiv 0 \pmod{3^h}.$$

Hence in this case, (3.4) is true. To finish the proof, it suffices to prove that when $\gamma_a \neq 0$,

$$\sum_{y\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(y^{\alpha+2}+\gamma_a y)}\chi(y) \equiv 0 \pmod{3^h}. \tag{3.5}$$

Now using Fourier inversion (e.g., see (1.2)), we have for any $y \in \mathbb{F}_q^*$,

$$\xi_3^{\mathrm{Tr}(y)} = \frac{1}{q-1}\sum_{b=0}^{q-2} g\big(\omega^{-b}\big)\omega^b(y),$$

where ω is the Teichmüller character on $\mathbb{F}_q$. Then

$$\sum_{y\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(y^{\alpha+2}+\gamma_a y)}\chi(y)$$
$$= \sum_{y\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(\gamma_a y)}\chi(y)\cdot\frac{1}{q-1}\sum_{b=0}^{q-2} g\big(\omega^{-b}\big)\omega^b\big(y^{\alpha+2}\big)$$
$$= \sum_{y\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(\gamma_a y)}\omega^{-\frac{q-1}{2}}(y)\cdot\frac{1}{q-1}\sum_{b=0}^{q-2} g\big(\omega^{-b}\big)\omega^{b(\alpha+2)}(y)$$
$$= \frac{1}{q-1}\sum_{b=0}^{q-2} g\big(\omega^{-b}\big)\sum_{y\in\mathbb{F}_q^*} \xi_3^{\mathrm{Tr}(\gamma_a y)}\omega^{-\frac{q-1}{2}+b(\alpha+2)}(y)$$
$$= \frac{1}{q-1}\sum_{b=0}^{q-2} g\big(\omega^{-b}\big)g\big(\omega^{-\frac{q-1}{2}+b(\alpha+2)}\big)\omega^{-\frac{q-1}{2}+b(\alpha+2)}\big(\gamma_a^{-1}\big).$$

Hence, we have

$$S_\beta = \pm\frac{1}{q-1}\sum_{b=0}^{q-2} g\big(\omega^{-b}\big)g\big(\omega^{-\frac{q-1}{2}+b(\alpha+2)}\big)\omega^{-\frac{q-1}{2}+b(\alpha+2)}\big(\gamma_a^{-1}\big). \tag{3.6}$$

Fix any prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\xi_{q-1}]$ lying over 3. Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q-1}, \xi_3]$ lying above $\mathfrak{p}$. Since $v_{\mathfrak{P}}(3) = 2$, we see that

$$S_\beta \equiv 0 \pmod{3^h} \quad\Leftrightarrow\quad v_{\mathfrak{P}}(S_\beta) \geqslant 2h.$$

Using the expression in (3.6) for S_β, we have

$$S_\beta \equiv 0 \pmod{3^h} \quad\Leftrightarrow\quad v_{\mathfrak{P}}\left(\sum_{b=0}^{q-2} g\big(\omega^{-b}\big)g\big(\omega^{-\frac{q-1}{2}+b(\alpha+2)}\big)\omega^{-\frac{q-1}{2}+b(\alpha+2)}\big(\gamma_a^{-1}\big)\right) \geqslant 2h. \tag{3.7}$$

By Theorem 1.2 and the fact that $g(\chi_0) = -1$, where χ_0 is the trivial multiplicative character of $\mathbb{F}_q$, we have for any b, $0 \leqslant b \leqslant q-2$,

$$v_{\mathfrak{P}}\big(g\big(\omega^{-b}\big)g\big(\omega^{-\frac{q-1}{2}+b(\alpha+2)}\big)\big) = s(b) + s\left(\frac{q-1}{2} - b(\alpha+2)\right).$$

Therefore if we can prove that for each b, $0 \leqslant b \leqslant q-2$,

$$s(b) + s\left(\frac{q-1}{2} - b(\alpha+2)\right) \geqslant 2h, \tag{3.8}$$

then (3.5) will follow. This is exactly what we will do. In fact, we prove a slightly stronger inequality in Theorem A.1. (Since the proof of Theorem A.1 is somewhat lengthy, we put it in Appendix A.) Now combine Theorem A.1 and Lemma 3.2, the proof of the theorem is complete. □

It is of interest to record the following corollary of Theorem 3.3.

Corollary 3.4. *Let $q = 3^m$, $m = 2h+1$, and $\alpha = 3^{h+1}$. For any $\beta \in \mathbb{F}_q^*$ and $a \in \mathbb{F}_q^*$, we have*

$$\sum_{x\in\mathbb{F}_q^*} \chi(x)\xi_3^{\mathrm{Tr}(x^{\alpha+2}+(\beta^{\alpha-1}a^{\alpha}-\beta^{2(\alpha-1)}a^{2\alpha})x)} = \pm\sqrt{-q}.$$

4. Inequivalence of skew Hadamard difference sets

Let D_1 and D_2 be two (v,k,λ) difference sets in an abelian group G. We say that D_1 and D_2 are *equivalent* if there exists an automorphism σ of G and an element $g \in G$ such that $\sigma(D_1) = D_2 g$. In this section, we discuss the inequivalence issues for skew Hadamard difference sets.

4.1. The known families of skew Hadamard difference sets

Let $a \in \mathbb{F}_q$ and let n be a positive integer. We define the *Dickson polynomial* $\mathcal{D}_n(x,a)$ over $\mathbb{F}_q$ by

$$\mathcal{D}_n(x,a) = \sum_{j=0}^{\lfloor n/2\rfloor} \frac{n}{n-j}\binom{n-j}{j}(-a)^j x^{n-2j},$$

where $\lfloor n/2\rfloor$ is the largest integer $\leqslant n/2$. It is well known that the Dickson polynomial $\mathcal{D}_n(x,a)$, $a \in \mathbb{F}_q^*$, is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(n, q^2-1) = 1$ (see [17, p. 356]). Let m be a positive odd integer. For any $u \in \mathbb{F}_{3^m}^*$, define

$$g_u(x) = \mathcal{D}_5\big(x^2, -u\big) = x^{10} - ux^6 - u^2x^2.$$

It was proved in [8] that when m is a positive odd integer and $u \in \mathbb{F}_{3^m}^*$, $\mathrm{Image}(g_u) \setminus \{0\}$ is a skew Hadamard difference set in $(\mathbb{F}_{3^m}, +)$. For convenience, we set

$$\mathrm{DY}(u) = \big\{x^{10} - ux^6 - u^2x^2 \;\big|\; x \in \mathbb{F}_{3^m}^*\big\},$$

and call these *the Ding–Yuan difference sets*. We have the following proposition.

Proposition 4.1. *All previously known skew Hadamard difference sets are equivalent to one of the following*:

(1) *The Paley difference set P in $\mathbb{F}_q$, where $q \equiv 3 \pmod 4$ is a prime power.*
(2) *The Ding–Yuan difference set* $\mathrm{DY}(1)$ *in $\mathbb{F}_{3^m}$, where m is odd.*
(3) *The Ding–Yuan difference set* $\mathrm{DY}(-1)$ *in $\mathbb{F}_{3^m}$, where m is odd.*

Proof. First of all, it can be checked directly that $\mathcal{D}_5(-x,u) = -\mathcal{D}_5(x,u)$ and

$$b^5\mathcal{D}_5(x,a) = \mathcal{D}_5\big(bx, b^2a\big), \quad \forall a,b \in \mathbb{F}_q. \tag{4.1}$$

Setting $a=-1$ in (4.1), we have

$$b^5\mathcal{D}_5\big(x^2,-1\big) = \mathcal{D}_5\big(bx^2,-b^2\big).$$

Thus, we have $\mathrm{DY}(b^2) = b^5\,\mathrm{DY}(1)$ if b is a nonzero square in $\mathbb{F}_{3^m}$; and $\mathrm{DY}(b^2) = -b^5\,\mathrm{DY}(1)$ if b is a nonsquare. Hence for any nonzero square $u \in \mathbb{F}_{3^m}$, $\mathrm{DY}(u)$ is equivalent to $\mathrm{DY}(1)$.

Similarly, we can prove that for any nonsquare $u \in \mathbb{F}_{3^m}$, $\mathrm{DY}(u)$ is equivalent to $\mathrm{DY}(-1)$.

Combining the above observation with the fact that the Paley family and the Ding–Yuan family were the only previously known skew Hadamard difference sets, we see that the proof of the proposition is complete. □

With the help of a computer, it was verified in [8] that the three skew Hadamard difference sets P, $\mathrm{DY}(1)$ and $\mathrm{DY}(-1)$ in $(\mathbb{F}_{3^m},+)$ are all equivalent when $m=3$, but they are indeed pairwise inequivalent when $m=5$ and 7. It is very likely that the three difference sets P, $\mathrm{DY}(1)$ and $\mathrm{DY}(-1)$ are pairwise inequivalent for all odd $m>7$, although this is not proved rigorously.

4.2. The inequivalence issues for the difference sets D_a

We now turn to the difference sets D_a constructed in Section 3. First we prove the following

Proposition 4.2. *Let $m=2h+1$ be a positive integer and let $a \in \mathbb{F}_{3^m}^*$. The skew Hadamard difference sets D_a in $(\mathbb{F}_{3^m},+)$ constructed in Section* 3 *are equivalent to one of the following*:

(1) *The difference set D_1 in $(\mathbb{F}_{3^m},+)$.*
(2) *The difference set D_{-1} in $(\mathbb{F}_{3^m},+)$.*

Proof. Using the definition of $f_a(x)$ in (2.3), it can be checked that

$$b^{2\alpha+3} f_a\left(\frac{x}{b}\right) = f_{ab^{\alpha+1}}(x), \quad \forall b \in \mathbb{F}_{3^m}^*.$$

Assume that a is a nonzero square in $\mathbb{F}_{3^m}$. Since $\gcd(\alpha+1, q-1) = 2$, one can find $\zeta \in \mathbb{F}_{3^m}^*$ such that

$$a\zeta^{\alpha+1} = 1.$$

Hence

$$\zeta^{2\alpha+3} f_a\left(\frac{x^2}{\zeta}\right) = f_1\big(x^2\big). \tag{4.2}$$

We note that if ζ is a square, then $\{f_a(\frac{x^2}{\zeta}) \mid x \in \mathbb{F}_{3^m}^*\} = \{f_a(x^2) \mid x \in \mathbb{F}_{3^m}^*\} = D_a$; and if ζ is a nonsquare, then $\{f_a(\frac{x^2}{\zeta}) \mid x \in \mathbb{F}_{3^m}^*\} = \{f_a(-x^2) \mid x \in \mathbb{F}_{3^m}^*\} = \{-f_a(x^2) \mid x \in \mathbb{F}_q^*\} = -D_a$. Therefore

$$\left\{ \zeta^{2\alpha+3} f_a\left(\frac{x^2}{\zeta}\right) \,\middle|\, x \in \mathbb{F}_{3^m}^* \right\} = \zeta^{2\alpha+3} D_a \quad \text{or} \quad -\zeta^{2\alpha+3} D_a. \tag{4.3}$$

Combining (4.3) with (4.2), we see that D_a is equivalent to D_1.

Similarly, we can show that D_a is equivalent to D_{-1} when a is a nonsquare in $\mathbb{F}_{3^m}$. □

Since equivalent difference sets give rise to isomorphic symmetric designs, which have the same p-rank and Smith normal form, we may use p-ranks and Smith normal forms to distinguish inequivalent difference sets. See [20] for a recent survey of results on this subject. Unfortunately, skew Hadamard difference sets with the same parameters have the same p-rank [13, pp. 297–299] and the same Smith normal form [18]. Thus in order to distinguish inequivalent skew Hadamard difference sets, we have to use some other techniques.

It seems not easy to settle completely the question whether the difference sets D_1 and D_{-1} are inequivalent to the previously known families stated in Proposition 4.1. With the aid of a computer, we will show that the skew Hadamard difference sets D_1 and D_{-1} in $(\mathbb{F}_{3^m}, +)$ are new when $m = 5$ and 7. (We mention that when $m = 3$, the difference sets D_1 and D_{-1} are equivalent to the Paley difference set in $\mathbb{F}_{3^3}$.)

Let D be a difference set in $(\mathbb{F}_q, +)$. For any 2-subset $\{a, b\} \subset \mathbb{F}_q^*$, we define

$$T\{a, b\} := \big|D \cap (D + a) \cap (D + b)\big|.$$

These numbers $T\{a, b\}$ are called the *triple intersection numbers*, which were used to distinguish inequivalent difference sets in 1971 by Baumert [2, p. 144].

We shall use the triple intersection numbers to distinguish the skew difference sets of this paper from the earlier ones in the cases where $m = 5$ and $m = 7$. We use P and RT(a) to denote the Paley difference set and the difference set D_a from Section 3, respectively.

With the help of Magma [6], the maximum and minimum triple intersection numbers of these difference sets in $\mathbb{F}_{3^7}$ are computed and listed below.

Difference set	Minimum (when $m = 7$)	Maximum (when $m = 7$)
P	261	284
DY(1)	246	300
DY(-1)	248	297
RT(1)	250	295
RT(-1)	249	296

Hence the five difference sets are pairwise inequivalent when $m = 7$. It then follows from Proposition 4.1 that the skew difference sets RT(1) and RT(-1) are new when $m = 7$.

When $m = 5$, the maximum and minimum triple intersection numbers of these difference sets in $\mathbb{F}_{3^m}$ are computed and listed below.

Difference set	Minimum (when $m = 5$)	Maximum (when $m = 5$)
P	26	33
DY(1)	23	36
DY(-1)	24	35
RT(1)	24	35
RT(-1)	24	35

In fact, in this case DY(−1), RT(1) and RT(−1) have the same set of triple intersection numbers, i.e., $\{i\colon\ 24 \leqslant i \leqslant 35\}$. We further compute the multiplicities of these triple intersection numbers for these three cases. We find the following data.

Difference set	Triple intersection numbers with multiplicities ($m = 5$)
DY(−1)	$24^{75}25^{435}26^{1155}27^{2385}\cdots 35^{120}$
RT(1)	$24^{75}25^{330}26^{1155}27^{2535}\cdots 35^{105}$
RT(−1)	$24^{90}25^{330}26^{1095}27^{2655}\cdots 35^{120}$

where the exponents denote multiplicities. Since the multiplicities of the (triple) intersection number 27 are pairwise distinct for the three cases, we conclude that DY(−1), RT(1) and RT(−1) are pairwise inequivalent when $m = 5$. Hence, the five difference sets P, DY(1), DY(−1), RT(1), and RT(−1) are pairwise inequivalent when $m = 5$. It then follows from Proposition 4.1 that the skew difference sets RT(1) and RT(−1) are new when $m = 5$.

Based on the above evidence, we make the following conjecture.

Conjecture 4.3. *The five difference sets P,* DY(1), DY(−1), RT(1) *and* RT(−1) *in* $(\mathbb{F}_{3^m}, +)$ *are pairwise inequivalent for all odd $m > 7$.*

5. Difference sets with twin prime power parameters

In this section we present a variation of the classical construction of the twin prime power difference sets. Using this variation we will show that inequivalent skew Hadamard difference sets can give rise to inequivalent difference sets with twin prime power parameters. We first recall the construction of the twin prime power difference sets. As usual, we denote the (multiplicative) quadratic character of a finite field by χ.

Theorem 5.1. (Stanton and Sprott [19]) *Let q and $q + 2$ be odd prime powers. Then the set*

$$D = \left\{(x, y) \;\middle|\; x \in \mathbb{F}_q^*,\ y \in \mathbb{F}_{q+2}^*,\ \chi(x) = \chi(y)\right\} \cup \left\{(x, 0) \;\middle|\; x \in \mathbb{F}_q\right\}$$

is a $(4n - 1, 2n - 1, n - 1)$ difference set in $(\mathbb{F}_q, +) \times (\mathbb{F}_{q+2}, +)$, where $n = \frac{(q+1)^2}{4}$.

For a proof of Theorem 5.1, we refer the reader to [19] or [4, p. 354]. For convenience, we will refer the parameters $(4n - 1, 2n - 1, n - 1)$, $n = \frac{(q+1)^2}{4}$, q an odd prime power, as the twin prime power parameters. We now give a variation of the above construction.

Theorem 5.2. *Let q and $q + 2$ be prime powers, and let $q \equiv 3 \pmod 4$. Let E be a skew Hadamard difference set in $(\mathbb{F}_q, +)$. Then the set*

$$D = \left\{(x, y) \;\middle|\; x \in E,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = 1\right\} \cup \left\{(x, y) \;\middle|\; x \in -E,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = -1\right\} \cup \left\{(x, 0) \;\middle|\; x \in \mathbb{F}_q\right\}$$

is a $(4n - 1, 2n - 1, n - 1)$ difference set in $(\mathbb{F}_q, +) \times (\mathbb{F}_{q+2}, +)$, where $n = \frac{(q+1)^2}{4}$.

Noting that the nontrivial character values of a skew Hadamard difference set are given by (1.1), one can easily give a character theoretic proof for Theorem 5.2. We leave this to the reader as an exercise.

Remark 5.3. (1) We remark that if q and $q+2$ are both prime powers, and $q \equiv 1 \pmod 4$, then we can similarly use a skew Hadamard difference set in $\mathbb{F}_{q+2}$ to construct a difference set in $(\mathbb{F}_q, +) \times (\mathbb{F}_{q+2}, +)$ with twin prime power parameters.

(2) One further generalization of Theorem 5.2 goes as follows. With the assumptions in Theorem 5.2, let Q be any $(q+2, \frac{q+1}{2}, \frac{q-3}{4}, \frac{q+1}{4})$ partial difference set in $(\mathbb{F}_{q+2}, +)$, $0 \notin Q$. (See [4, p. 230] for the definition of partial difference set.) Then the set

$$D' = \big\{(x,y) \bigm| x \in E,\ y \in Q\big\} \cup \big\{(x,y) \bigm| x \in -E,\ y \in \mathbb{F}_{q+2}^* \setminus Q\big\} \cup \big\{(x,0) \bigm| x \in \mathbb{F}_q\big\}$$

is a $(4n-1, 2n-1, n-1)$ difference set in $(\mathbb{F}_q, +) \times (\mathbb{F}_{q+2}, +)$, where $n = \frac{(q+1)^2}{4}$.

In view of the fact that there exist inequivalent skew Hadamard difference sets in $(\mathbb{F}_q, +)$, the following theorem is of interest.

Theorem 5.4. *Let q and $q+2$ be prime powers, and let $q \equiv 3 \pmod 4$. Let E and F be inequivalent skew Hadamard difference sets in $(\mathbb{F}_q, +)$. Then the two difference sets*

$$D = \big\{(x,y) \bigm| x \in E,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = 1\big\} \cup \big\{(x,y) \bigm| x \in -E,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = -1\big\} \cup \big\{(x,0) \bigm| x \in \mathbb{F}_q\big\}$$

and

$$D' = \big\{(x,y) \bigm| x \in F,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = 1\big\} \cup \big\{(x,y) \bigm| x \in -F,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = -1\big\} \cup \big\{(x,0) \bigm| x \in \mathbb{F}_q\big\}$$

are inequivalent.

Proof. Assume that D and D' are equivalent difference sets in $G = (\mathbb{F}_q, +) \times (\mathbb{F}_{q+2}, +)$. Then there exists an automorphism α of G and an element $(b_1, b_2) \in G$ such that

$$\alpha(D) = D' + (b_1, b_2). \tag{5.1}$$

We will show that E and F are equivalent.

For convenience, we define

$$A_1 = \big\{(x,y) \bigm| x \in E,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = 1\big\} \cup \big\{(x,y) \bigm| x \in -E,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = -1\big\},$$
$$A_2 = \big\{(x,y) \bigm| x \in F,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = 1\big\} \cup \big\{(x,y) \bigm| x \in -F,\ y \in \mathbb{F}_{q+2}^*,\ \chi(y) = -1\big\},$$

and

$$B = \big\{(x,0) \bigm| x \in \mathbb{F}_q\big\}.$$

So $D = A_1 \cup B$, $D' = A_2 \cup B$, and (5.1) can be written as

$$\alpha(A_1) \cup \alpha(B) = \big(A_2 + (b_1, b_2)\big) \cup \big(B + (b_1, b_2)\big). \tag{5.2}$$

Since $\gcd(q, q+2) = 1$, we have $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathbb{F}_q, +) \times \mathrm{Aut}(\mathbb{F}_{q+2}, +)$. Hence there exist $f \in \mathrm{Aut}(\mathbb{F}_q, +)$ and $g \in \mathrm{Aut}(\mathbb{F}_{q+2}, +)$ such that $\alpha(x,y) = (f(x), g(y))$ for all $(x,y) \in G$.

We claim that $b_2 = 0$. If not, then there exists a $y \in \mathbb{F}_{q+2}^*$ such that $g(y) = b_2$. Note that $B + (b_1, b_2) = \{(x, b_2) \mid x \in \mathbb{F}_q\}$. By (5.2), we must have

$$\big\{\big(f(x), g(y)\big) \bigm| x \in E\big\} = \big\{(x, b_2) \bigm| x \in \mathbb{F}_q\big\},$$

or

$$\big\{\big(f(x), g(y)\big) \,\big|\, x \in -E\big\} = \big\{(x, b_2) \,\big|\, x \in \mathbb{F}_q\big\},$$

according as $\chi(y) = 1$ or $\chi(y) = -1$. However both equalities are clearly impossible by comparing the cardinalities of the sets involved. This proves that $b_2 = 0$. It follows that $\alpha(B) = B + (b_1, 0)$ and

$$\alpha(A_1) = A_2 + (b_1, 0). \tag{5.3}$$

Let $y \in \mathbb{F}_{q+2}^*$ such that $g(y) = 1$. From (5.3), we see that

$$\big\{\big(f(x), g(y)\big) \,\big|\, x \in E\big\} = \big\{(x + b_1, 1) \,\big|\, x \in F\big\},$$

or

$$\big\{\big(f(x), g(y)\big) \,\big|\, x \in -E\big\} = \big\{(x + b_1, 1) \,\big|\, x \in F\big\},$$

according to $\chi(y) = 1$ or $\chi(y) = -1$. So $f(E) = F + b_1$ or $-f(E) = F + b_1$. This proves that E and F are equivalent difference sets in $(\mathbb{F}_q, +)$. □

Combining Theorem 5.4 with the results in Section 4, we see that whenever $3^{2h+1} \pm 2$ $(h > 1)$ is a prime power, there exist difference sets with twin prime power parameters that are inequivalent to the classical twin prime power difference sets. To indicate that there are $h > 1$ such that $3^{2h+1} \pm 2$ are prime powers, we mention the following specific examples: $3^5 - 2 = 241$ is a prime, $3^9 - 2 = 19\,681$ is a prime, and $3^{15} + 2 = 14\,348\,909$ is also a prime.

Acknowledgment

The authors thank an anonymous referee for his/her helpful comments.

Appendix A

In this appendix, we give the promised proof of (3.8). Throughout this section, $m = 2h + 1$ is a positive odd integer, $q = 3^m$, $r = \frac{m+1}{2} = h + 1$, and $\alpha = 3^{\frac{m+1}{2}} = 3^r$. Our goal is to prove

Theorem A.1. *For each a, $0 \leqslant a \leqslant q - 2$, we have*

$$s(a) + s\left(\frac{q-1}{2} - a(\alpha + 2)\right) \geqslant m, \tag{A.1}$$

where $s(a)$ is the digit sum of a defined in Section 1.

First of all, we observe that the only a, $0 \leqslant a \leqslant q - 2$, satisfying

$$\frac{q-1}{2} - a(\alpha + 2) \equiv 0 \pmod{q-1}$$

is $a = \frac{q-1}{2}$. For $a = \frac{q-1}{2}$, we have $s(a) = m$ and $s(\frac{q-1}{2} - a(\alpha + 2)) = 0$. So certainly (A.1) holds for $a = \frac{q-1}{2}$. Therefore in our discussion below, we will always assume that $a \neq \frac{q-1}{2}$ (and $\frac{q-1}{2} - a(\alpha + 2) \not\equiv 0 \pmod{q-1}$).

A sequence $\{u_i\}_{i\in\mathbb{Z}}$ is called periodic with period m if $u_i = u_j$ whenever $i \equiv j \pmod m$. All sequences in this section are periodic with period m. Let a be an integer satisfying $0 \leqslant a \leqslant q-2$ and $a \neq \frac{q-1}{2}$. Write

$$a = \sum_{i=0}^{m-1} a_i 3^i, \quad a_i \in \{0,1,2\},$$

and extend $a_0, a_1, \ldots, a_{m-1}$ to a periodic sequence with period m. We have

$$\begin{aligned}
\frac{q-1}{2} - \big(3^r+2\big)a &= \frac{q-1}{2} - 3^r a - 3a + a \\
&\equiv \sum_{i=0}^{m-1} (1 - a_{i-r} - a_{i-1} + a_i) 3^i \pmod{3^m-1} \\
&\equiv \sum_{i=0}^{m-1} \big(1 + (2-a_{i-r}) + (2-a_{i-1}) + a_i\big) 3^i \pmod{3^m-1} \\
&= \sum_{i=0}^{m-1} (5 + a_i - a_{i-1} - a_{i-r}) 3^i.
\end{aligned}$$

For each i, let

$$b_i = 5 + a_i - a_{i-1} - a_{i-r}.$$

It is easily seen that $b_i \in \{1,2,3,\ldots,7\}$. Write

$$\sum_{i=0}^{m-1} b_i 3^i \equiv \sum_{i=0}^{m-1} s_i 3^i \pmod{3^m-1}$$

with $s_i \in \{0,1,2\}$. By Theorem 13 of [10] (adapted to the ternary case), there exists a sequence $\{c_i\}$ such that

$$\forall i, \quad s_i = b_i - 3c_i + c_{i-1}, \tag{A.2}$$

where $c_i \in \{0,1,2,3\}$ is the carry from the ith digit to the $(i+1)$th digit in the modular summation of $\frac{q-1}{2}$, $-3^r a$, $-3a$ and a. Note that

$$\begin{aligned}
s(a) + s\left(\frac{q-1}{2} - \big(3^r+2\big)a\right) &= \sum_{i=0}^{m-1} a_i + \sum_{i=0}^{m-1} \big((5 + a_i - a_{i-1} - a_{i-r}) - 3c_i + c_{i-1}\big) \\
&= 5m - 2\sum_{i=0}^{m-1} c_i.
\end{aligned}$$

So in order to prove Theorem A.1, it suffices to prove

$$\sum_{i=0}^{m-1} c_i \leqslant 2m. \tag{A.3}$$

Since $\gcd(r,m) = \gcd(r, 2r-1) = 1$, for any fixed i, the sequence $c_i, c_{i-r}, c_{i-2r}, \ldots, c_{i-(m-1)r}$ is a rearrangement of $c_0, c_1, \ldots, c_{m-1}$. In the following, we will also frequently use the facts that $2r \equiv 1 \pmod m$, $c_{i-1} = c_{i-2r}$, $c_{i-2} = c_{i-4r}$, and so on.

Lemma A.2. *If $c_i = 3$, then $c_{i-1} = 2$ and $c_{i-r} \leqslant 2$, $a_i = 2$, $a_{i-1} = a_{i-r} = 0$.*

Proof. Note that $s_i = b_i - 3c_i + c_{i-1} \geqslant 0$, $1 \leqslant b_i \leqslant 7$, $0 \leqslant c_{i-1} \leqslant 3$. If $c_i = 3$, then

$$6 \leqslant b_i \leqslant 7, \qquad 2 \leqslant c_{i-1} \leqslant 3. \tag{A.4}$$

Assume to the contrary that $c_{i-1} = 3$. Since

$$s_{i-1} = b_{i-1} - 3c_{i-1} + c_{i-2} \geqslant 0,$$

we have

$$6 \leqslant b_{i-1} \leqslant 7, \qquad 2 \leqslant c_{i-2} \leqslant 3. \tag{A.5}$$

From the lower bounds on b_i and b_{i-1} in (A.4) and (A.5), we have

$$6 \leqslant b_i = 5 + a_i - a_{i-1} - a_{i-r}, \quad \text{and}$$
$$6 \leqslant b_{i-1} = 5 + a_{i-1} - a_{i-2} - a_{i-r-1}.$$

Adding up the two inequalities, we get

$$10 + a_i - a_{i-r} - a_{i-2} - a_{i-r-1} \geqslant 12,$$

which implies that

$$a_i = 2, \qquad a_{i-r} = a_{i-r-1} = a_{i-2} = 0.$$

We use the following table to summarize the above information:

$$\mathrm{A} := \begin{bmatrix} a_i & a_{i-r} & a_{i-1} & a_{i-r-1} & a_{i-2} \\ 2 & 0 & \geqslant 0 & 0 & 0 \end{bmatrix}.$$

Since

$$b_i = 5 + a_i - a_{i-1} - a_{i-r} \geqslant 6,$$

using the information in Table A, we have

$$a_{i-1} \leqslant 1.$$

Since

$$b_{i-1} = 5 + a_{i-1} - a_{i-2} - a_{i-r-1} \geqslant 6,$$

again using the information in Table A, we have

$$a_{i-1} \geqslant 1.$$

Hence $a_{i-1} = 1$. Therefore we can update the entries in Table A as follows:

$$\mathrm{A} = \begin{bmatrix} a_i & a_{i-r} & a_{i-1} & a_{i-r-1} & a_{i-2} \\ 2 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

It follows that $b_{i-1} = 5 + a_{i-1} - a_{i-2} - a_{i-r-1} = 6$. Since $s_{i-1} = b_{i-1} - 3c_{i-1} + c_{i-2} \geqslant 0$ and $c_{i-1} = 3$, we have $c_{i-2} = 3$. Combining this with $s_{i-2} = b_{i-2} - 3c_{i-2} + c_{i-3} \geqslant 0$, we obtain $b_{i-2} \geqslant 6$.

Since

$$b_{i-1} = 5 + a_{i-1} - a_{i-2} - a_{i-r-1} \geqslant 6,$$
$$b_{i-2} = 5 + a_{i-2} - a_{i-3} - a_{i-r-2} \geqslant 6,$$

adding up these two inequalities, we get

$$10 + a_{i-1} - a_{i-r-1} - a_{i-3} - a_{i-r-2} \geqslant 12,$$

which implies that

$$a_{i-1} = 2, \qquad a_{i-r-1} = a_{i-3} = a_{i-r-2} = 0.$$

But this is in contradiction with the previous conclusion that $a_{i-1} = 1$ as shown in Table A. Hence $c_{i-1} \neq 3$. By (A.4) we must have $c_{i-1} = 2$.

Combining the fact $c_{i-1} = 2$, $c_i = 3$ with $s_i = b_i - 3c_i + c_{i-1} \geqslant 0$, we have $b_i = 7$. Recall that

$$b_i = 5 + a_i - a_{i-1} - a_{i-r} \leqslant 7.$$

We obtain

$$a_i = 2, \qquad a_{i-1} = a_{i-r} = 0.$$

Now $b_{i-r} = 5 + a_{i-r} - a_{i-r-1} - a_{i-1} = 5 - a_{i-r-1} \leqslant 5$, $s_{i-r} = b_{i-r} - 3c_{i-r} + c_{i-r-1} \geqslant 0$, and $c_{i-r-1} \leqslant 3$, we conclude that $c_{i-r} \leqslant 2$. This completes the proof. □

Lemma A.3. *If $c_i = 3$, $c_{i-r} = c_{i-1} = 2$, then $c_{i-r-1} \leqslant 2$. That is,*

$$\begin{bmatrix} c_i & c_{i-r} & c_{i-1} \\ 3 & =2 & =2 \end{bmatrix} \Rightarrow \begin{bmatrix} c_i & c_{i-r} & c_{i-1} & c_{i-r-1} \\ 3 & =2 & =2 & \leqslant 2 \end{bmatrix}.$$

Proof. Assume to the contrary that $c_{i-r-1} = 3$. By Lemma A.2, we have $c_{i-r-2} = 2$, $c_{i-2} \leqslant 2$, $a_{i-r-1} = 2$, and $a_{i-r-2} = a_{i-2} = 0$. Since

$$s_{i-1} = b_{i-1} - 3c_{i-1} + c_{i-2} \geqslant 0,$$

and $c_{i-1} = 2$, $c_{i-2} \leqslant 2$, we have $b_{i-1} \geqslant 4$. By assumption $c_i = 3$. It follows from Lemma A.2 that $a_i = 2$, $a_{i-1} = a_{i-r} = 0$. We use the following table to summarize the above information:

$$\mathrm{A} := \begin{bmatrix} a_i & a_{i-r} & a_{i-1} & a_{i-r-1} & a_{i-2} & a_{i-r-2} \\ 2 & 0 & 0 & 2 & 0 & 0 \end{bmatrix}.$$

Recall that

$$b_{i-1} = 5 + a_{i-1} - a_{i-2} - a_{i-r-1}.$$

Using the information in Table A, we have $b_{i-1} = 5 + 0 - 0 - 2 = 3$, which contradicts the previous conclusion that $b_{i-1} \geqslant 4$. This completes the proof. □

Theorem A.4. *Let $t \geqslant 3$ be an integer. If $c_i = 3$, $c_{i-r} = c_{i-2r} = \cdots = c_{i-tr} = 2$, then $a_i = 2$, $a_{i-r} \leqslant 1$, $a_{i-2r} \leqslant 1$, …, $a_{i-(t-1)r} \leqslant 1$, $a_{i-(t-2)r} + a_{i-(t-1)r} \leqslant 1$, and $c_{i-tr-r} \leqslant 2$. Furthermore, if $c_i = 3$, $c_{i-r} = c_{i-2r} = \cdots = c_{i-tr} = 2$ and also $c_{i-tr-r} = 2$, then $a_{i-tr} \leqslant 1$ and $a_{i-(t-1)r} + a_{i-tr} \leqslant 1$.*

Proof. We will use induction on t. When $t = 3$, the assumptions are $c_i = 3$, and $c_{i-r} = c_{i-2r} = c_{i-3r} = 2$ (i.e., $c_{i-r} = c_{i-1} = c_{i-r-1} = 2$). We will show that $a_i = 2$, $a_{i-r} \leqslant 1$, $a_{i-2r} = a_{i-1} \leqslant 1$, $a_{i-r} + a_{i-1} \leqslant 1$, and $c_{i-3r-r} = c_{i-2} \leqslant 2$.

Since $c_i = 3$, by Lemma A.2, we have

$$a_i = 2, \qquad a_{i-r} = 0, \qquad a_{i-1} = 0. \tag{A.6}$$

It remains to show that $c_{i-2} \leqslant 2$. Assume to the contrary that $c_{i-2} = 3$, by Lemma A.2, we have $c_{i-3} = 2$ and $c_{i-2-r} \leqslant 2$, $a_{i-2} = 2$, $a_{i-3} = a_{i-2-r} = 0$. We summarize the information in the following table:

$$\mathrm{A} := \begin{bmatrix} a_i & a_{i-r} & a_{i-1} & a_{i-r-1} & a_{i-2} & a_{i-r-2} & a_{i-3} \\ 2 & 0 & 0 & \leqslant 2 & 2 & 0 & 0 \end{bmatrix}.$$

Since

$$\begin{aligned} &s_{i-r-1} = b_{i-r-1} - 3c_{i-r-1} + c_{i-r-2} \geqslant 0, \\ &s_{i-1} = b_{i-1} - 3c_{i-1} + c_{i-2} \geqslant 0, \\ &c_{i-r-1} = 2, \qquad c_{i-r-2} \leqslant 2, \qquad c_{i-1} = 2, \qquad c_{i-2} = 3, \end{aligned}$$

we see that $b_{i-r-1} \geqslant 4$ and $b_{i-1} \geqslant 3$. Using the information in Table A, we find that

$$b_{i-r-1} = 5 + a_{i-r-1} - a_{i-r-2} - a_{i-2} = 3 + a_{i-r-1}.$$

So $b_{i-r-1} \geqslant 4$ implies that $a_{i-r-1} \geqslant 1$. Again using the information in Table A, we find that

$$b_{i-1} = 5 + a_{i-1} - a_{i-2} - a_{i-r-1} = 3 - a_{i-r-1}.$$

So $b_{i-1} \geqslant 3$ implies that $a_{i-r-1} \leqslant 0$, which contradicts with the previous conclusion that $a_{i-r-1} \geqslant 1$. Therefore we must have $c_{i-2} \leqslant 2$.

Next we show that if $c_i = 3$ and $c_{i-r} = c_{i-2r} = c_{i-3r} = c_{i-4r} = 2$ (i.e., $c_{i-r} = c_{i-1} = c_{i-r-1} = c_{i-2} = 2$), then $a_{i-3r} = a_{i-r-1} \leqslant 1$, and $a_{i-1} + a_{i-r-1} \leqslant 1$. Note that (A.6) is still true. Since

$$\begin{aligned} &s_{i-r} = b_{i-r} - 3c_{i-r} + c_{i-r-1} \geqslant 0, \\ &s_{i-1} = b_{i-1} - 3c_{i-1} + c_{i-2} \geqslant 0, \\ &c_{i-r} = c_{i-1} = c_{i-r-1} = c_{i-2} = 2, \end{aligned}$$

we have

$$4 \leqslant b_{i-r} = 5 + a_{i-r} - a_{i-r-1} - a_{i-1}, \tag{A.7}$$

$$4 \leqslant b_{i-1} = 5 + a_{i-1} - a_{i-2} - a_{i-r-1}. \tag{A.8}$$

Adding up (A.7) and (A.8), we get

$$10 + a_{i-r} - 2a_{i-r-1} - a_{i-2} \geqslant 8.$$

As $a_{i-r} = 0$ (see (A.6)), the above inequality becomes

$$2a_{i-r-1} + a_{i-2} \leqslant 2.$$

Since $a_{i-2} \geqslant 0$, we have

$$a_{i-r-1} \leqslant 1.$$

Noting that $a_{i-1} = 0$ (see (A.6)), we have

$$a_{i-1} + a_{i-r-1} \leqslant 1.$$

This finishes the proof in the case where $t = 3$.

Assume that the theorem is proved for $t = k-1 \geqslant 3$. We will prove the theorem for $t = k$. So assume that $c_i = 3$, $c_{i-r} = c_{i-2r} = \cdots = c_{i-kr} = 2$. By induction hypothesis, we have

$$\begin{aligned} &a_i = 2, \qquad a_{i-r} \leqslant 1, \qquad a_{i-2r} \leqslant 1, \qquad \ldots, \qquad a_{i-(k-2)r} \leqslant 1, \\ &a_{i-(k-3)r} + a_{i-(k-2)r} \leqslant 1. \end{aligned} \tag{A.9}$$

Since it is also assumed that $c_{i-kr} = 2$, we have

$$a_{i-(k-1)r} \leqslant 1, \qquad a_{i-(k-2)r} + a_{i-(k-1)r} \leqslant 1. \tag{A.10}$$

Now we show that $c_{i-kr-r} \leqslant 2$. Assume to the contrary that $c_{i-kr-r} = 3$. Then by Lemma A.2, we have $c_{i-kr-r-1} = 2$, $c_{i-kr-1} \leqslant 2$, and $a_{i-kr-r} = 2$, $a_{i-kr-r-1} = a_{i-kr-1} = 0$. As before we summarize the information in the following table:

$$\mathrm{B} := \begin{bmatrix} a_{i-(k-2)r} & a_{i-(k-1)r} & a_{i-kr} & a_{i-kr-r} & a_{i-kr-1} & a_{i-kr-r-1} \\ \leqslant 1 & \leqslant 1 & \geqslant 0 & 2 & 0 & 0 \end{bmatrix}.$$

Since

$$\begin{aligned} &s_{i-(k-1)r} = b_{i-(k-1)r} - 3c_{i-(k-1)r} + c_{i-kr-r} \geqslant 0, \\ &s_{i-kr} = b_{i-kr} - 3c_{i-kr} + c_{i-kr-1} \geqslant 0, \\ &c_{i-(k-1)r} = c_{i-kr} = 2, \qquad c_{i-kr-r} = 3, \qquad c_{i-kr-1} \leqslant 2; \end{aligned}$$

we have

$$3 \leqslant b_{i-(k-1)r} = 5 + a_{i-(k-1)r} - a_{i-kr-r} - a_{i-kr}, \tag{A.11}$$

$$4 \leqslant b_{i-kr} = 5 + a_{i-kr} - a_{i-kr-1} - a_{i-kr-r}. \tag{A.12}$$

Adding up (A.11) and (A.12), we get

$$10 + a_{i-(k-1)r} - 2a_{i-kr-r} - a_{i-kr-1} \geqslant 7.$$

Since $a_{i-kr-r} = 2$, we have

$$a_{i-(k-1)r} - a_{i-kr-1} \geqslant 1,$$

which implies that $a_{i-(k-1)r} \geqslant 1$. Combining this with the information on $a_{i-(k-1)r}$ in Table B, we have

$$a_{i-(k-1)r} = 1. \tag{A.13}$$

Thus we can update the information in Table B as follows:

$$\mathrm{B} = \begin{bmatrix} a_{i-(k-2)r} & a_{i-(k-1)r} & a_{i-kr} & a_{i-kr-r} & a_{i-kr-1} & a_{i-kr-r-1} \\ \leqslant 1 & = 1 & \geqslant 0 & 2 & 0 & 0 \end{bmatrix}.$$

Using the updated Table B and (A.11) (respectively, (A.12)), we get $a_{i-kr} \leqslant 1$ (respectively, $a_{i-kr} \geqslant 1$). Hence

$$a_{i-kr} = 1. \tag{A.14}$$

Since

$$s_{i-(k-3)r} = b_{i-(k-3)r} - 3c_{i-(k-3)r} + c_{i-(k-1)r} \geqslant 0,$$
$$s_{i-(k-2)r} = b_{i-(k-2)r} - 3c_{i-(k-2)r} + c_{i-kr} \geqslant 0,$$
$$c_{i-(k-3)r} = c_{i-(k-2)r} = c_{i-(k-1)r} = c_{i-kr} = 2;$$

we have

$$4 \leqslant b_{i-(k-3)r} = 5 + a_{i-(k-3)r} - a_{i-(k-1)r} - a_{i-(k-2)r}, \tag{A.15}$$
$$4 \leqslant b_{i-(k-2)r} = 5 + a_{i-(k-2)r} - a_{i-kr} - a_{i-(k-1)r}. \tag{A.16}$$

Adding up (A.15) and (A.16), we get

$$10 + a_{i-(k-3)r} - 2a_{i-(k-1)r} - a_{i-kr} \geqslant 8. \tag{A.17}$$

Noting that $a_{i-(k-1)r} = a_{i-kr} = 1$, we obtain from (A.17) and (A.16) that

$$a_{i-(k-3)r} \geqslant 1, \qquad a_{i-(k-2)r} \geqslant 1, \tag{A.18}$$

which implies that

$$a_{i-(k-3)r} + a_{i-(k-2)r} \geqslant 2,$$

contradicting with $a_{i-(k-3)r} + a_{i-(k-2)r} \leqslant 1$ in (A.9). Therefore

$$c_{i-kr-r} \leqslant 2.$$

Finally, assume that $c_i = 3$, $c_{i-r} = c_{i-2r} = \cdots = c_{i-kr} = c_{i-kr-r} = 2$. From the conditions, we know that (A.9), (A.10), (A.15) and (A.16) still hold. Since

$$s_{i-(k-1)r} = b_{i-(k-1)r} - 3c_{i-(k-1)r} + c_{i-kr-r} \geqslant 0,$$
$$c_{i-(k-1)r} = c_{i-kr-r} = 2,$$

we have

$$4 \leqslant b_{i-(k-1)r} = 5 + a_{i-(k-1)r} - a_{i-(k+1)r} - a_{i-kr}. \tag{A.19}$$

Adding up (A.15) and (A.16), (A.16) and (A.19), respectively, we get

$$2a_{i-(k-1)r} + a_{i-kr} - a_{i-(k-3)r} \leqslant 2, \tag{A.20}$$
$$2a_{i-kr} + a_{i-(k+1)r} - a_{i-(k-2)r} \leqslant 2. \tag{A.21}$$

Adding up (A.20) and (A.21), we get

$$2a_{i-(k-1)r} + 3a_{i-kr} \leqslant 4 + (a_{i-(k-3)r} + a_{i-(k-2)r}) - a_{i-(k+1)r}.$$

Since $a_{i-(k-3)r} + a_{i-(k-2)r} \leqslant 1$, it follows that

$$2a_{i-(k-1)r} + 3a_{i-kr} \leqslant 5 - a_{i-(k+1)r} \leqslant 5. \tag{A.22}$$

Now we would like to show that $a_{i-(k-1)r} + a_{i-kr} \leqslant 1$. Assume to the contrary that $a_{i-(k-1)r} + a_{i-kr} > 1$. Since $a_{i-(k-1)r} \leqslant 1$, by (A.22), we have

$$a_{i-(k-1)r} = 1, \qquad a_{i-kr} = 1. \tag{A.23}$$

Combining (A.16) with (A.23), we get

$$a_{i-(k-2)r} \geqslant 1.$$

So $a_{i-(k-2)r} + a_{i-(k-1)r} \geqslant 2$, contradicting with $a_{i-(k-2)r} + a_{i-(k-1)r} \leqslant 1$ in (A.10). Hence

$$a_{i-(k-1)r} + a_{i-kr} \leqslant 1,$$

which in turn implies

$$a_{i-kr} \leqslant 1.$$

This completes the proof. □

Corollary A.5. *If $c_i = 3$, then $c_{i-r} \leqslant 2$. Let $t \geqslant 1$ be an integer. If $c_i = 3$, $c_{i-r} = c_{i-2r} = \cdots = c_{i-tr} = 2$, then $c_{i-tr-r} \leqslant 2$.*

Proof. The first assertion follows directly from Lemma A.2. For the second assertion, when $t = 1$ (respectively, $t = 2$), the corollary follows from Lemma A.2 (respectively, Lemma A.3). When $t \geqslant 3$, the corollary follows directly from Theorem A.4. □

Corollary A.6. *Let t be an integer satisfying $1 \leqslant t \leqslant m$. If $c_i = c_{i-tr} = 3$ and $c_{i-r} \leqslant 2$, $c_{i-2r} \leqslant 2, \ldots, c_{i-(t-1)r} \leqslant 2$, then there exists ℓ, $1 \leqslant \ell \leqslant t-1$, such that $c_{i-\ell r} < 2$.*

Proof. Using Corollary A.5, we see that the condition $c_i = c_{i-tr} = 3$ implies that $t \neq 1$. Assume to the contrary that for every $\ell \in \{1, 2, \ldots, t-1\}$, we have $c_{i-\ell r} = 2$. That is,

$$c_i = 3, \qquad c_{i-r} = c_{i-2r} = \cdots = c_{i-(t-1)r} = 2.$$

Then by Corollary A.5, we have $c_{i-tr} \leqslant 2$, contradicting with our assumption that $c_{i-tr} = 3$. This completes the proof. □

Proof of Theorem A.1. As stated before, it suffices to prove that

$$\sum_{i=0}^{m-1} c_i \leqslant 2m. \tag{A.24}$$

If $c_i \leqslant 2$, for all i, $0 \leqslant i \leqslant m-1$, then the inequality (A.24) of course holds. So we assume that there exists an h, $0 \leqslant h \leqslant m-1$, such that $c_h = 3$. Since $\gcd(m, r) = 1$, we see that the sequence $c_h, c_{h-r}, \ldots, c_{h-(m-1)r}$ is just a permutation of $c_0, c_1, \ldots, c_{m-1}$. We assume that $c_{h-i_1 r} = c_{h-i_2 r} = \cdots = c_{h-i_s r} = 3$, where $0 = i_1 < i_2 < \cdots i_s < m$, $s \geqslant 1$, and $c_{h-jr} \leqslant 2$ for each $j \in \{0, 1, \ldots, m-1\} \setminus \{i_1, i_2, \ldots, i_s\}$. By Corollary A.5, we have $i_2 \geqslant i_1 + 2$, $i_3 \geqslant i_2 + 2$, $\ldots$, $i_s \geqslant i_{s-1} + 2$, and $m \geqslant i_s + 2$. Using Corollary A.6, we can bound the sum of the entries in each segment as follows:

$$\begin{aligned}
&c_{h-i_1 r} + c_{h-(i_1+1)r} + \cdots + c_{h-(i_2-1)r} \leqslant 2(i_2 - i_1),\\
&c_{h-i_2 r} + c_{h-(i_2+1)r} + \cdots + c_{h-(i_3-1)r} \leqslant 2(i_3 - i_2),\\
&\quad\vdots\\
&c_{h-i_s r} + c_{h-(i_s+1)r} + \cdots + c_{h-(m-1)r} \leqslant 2(m - i_s).
\end{aligned}$$

Summing up the above inequalities, we obtain (A.24). The proof of the theorem is complete. □

References

[1] S. Ball, M. Zieve, Symplectic spreads and permutation polynomials, in: Finite Fields and Applications, in: Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, 2004, pp. 79–88.
[2] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Math., vol. 182, Springer, 1971.
[3] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, Wiley–Interscience, 1998.
[4] T. Beth, D. Jungnickel, H. Lenz, Design Theory, vol. I, second ed., Encyclopedia Math. Appl., vol. 78, Cambridge Univ. Press, Cambridge, 1999.
[5] P. Camion, H.B. Mann, Antisymmetric difference sets, J. Number Theory 4 (1972) 266–268.
[6] J. Cannon, C. Playoust, An Introduction to MAGMA, University of Sydney, Sydney, Australia, 1993.
[7] Y.Q. Chen, Q. Xiang, S. Sehgal, An exponent bound on skew Hadamard abelian difference sets, Des. Codes Cryptogr. 4 (1994) 313–317.
[8] C. Ding, J. Yuan, A family of skew Hadamard difference sets, J. Combin. Theory Ser. A 113 (7) (2006) 1526–1535.
[9] J.W.P. Hirschfeld, Finite Projective Spaces of Three Dimensions, Oxford Math. Monogr., Oxford Sci. Publ., Clarendon Press, Oxford Univ. Press, New York, 1985.
[10] H. Hollmann, Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences, Finite Fields Appl. 7 (2001) 253–286.
[11] E.C. Johnsen, Skew-Hadamard Abelian group difference sets, J. Algebra 4 (1966) 388–402.
[12] D. Jungnickel, On λ-ovals and difference sets, in: Contemporary Methods in Graph Theory, Bibliographisches Inst., Mannheim, 1990, pp. 429–448.
[13] D. Jungnickel, Difference sets, in: J. Dinitz, D.R. Stinson (Eds.), Contemporary Design Theory, A Collection of Surveys, in: Wiley–Intersci. Ser. Discrete Math. Optim., Wiley, New York, 1992, pp. 241–324.
[14] W.M. Kantor, Ovoids and translation planes, Canad. J. Math. 34 (1982) 1195–1207.
[15] E.S. Lander, Symmetric Designs: An Algebraic Approach, London Math. Soc. Lecture Note Ser., vol. 74, Cambridge Univ. Press, 1983.
[16] S. Lang, Cyclotomic Fields, Springer, New York, 1978.
[17] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.
[18] T.S. Michael, W.D. Wallis, Skew-Hadamard matrices and the Smith normal form, Des. Codes Cryptogr. 13 (1998) 173–176.
[19] R.G. Stanton, D.A. Sprott, A family of difference sets, Canad. J. Math. 10 (1958) 73–77.
[20] Q. Xiang, Recent progress in algebraic design theory, Finite Fields Appl. 11 (2005) 622–653.