(This is a sample cover image for this issue. The actual cover is not yet available at this time.)

Journal of Combinatorial Theory, Series A 119 (2012) 245–256

Contents lists available at SciVerse ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Cyclotomic constructions of skew Hadamard difference sets

Tao Feng, Qing Xiang [1]

Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

ARTICLE INFO

Article history:
Received 12 January 2011
Available online xxxx

Keywords:
Cyclotomy
Difference set
Gauss sum
Index 2 Gauss sum
Partial difference set
Skew Hadamard difference set

ABSTRACT

We revisit the old idea of constructing difference sets from cyclotomic classes. Two constructions of skew Hadamard difference sets are given in the additive groups of finite fields by using union of cyclotomic classes of $\mathbb{F}_q$ of order $N = 2p_1^m$, where p_1 is a prime and m a positive integer. Our main tools are index 2 Gauss sums, instead of cyclotomic numbers.

1. Introduction

We assume that the reader is familiar with the basic theory of difference sets as can be found in [18] and Chapter 6 of [5]. For a survey of recent progress in this area we refer the reader to [29].

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 primary example (and for many years, the only known example in abelian groups) of skew Hadamard difference sets is 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. Skew Hadamard difference sets are currently under intensive study, see [10,11,13,24,27,28]. There were two major conjectures in this area: (1) If an abelian group G contains a skew Hadamard difference set, then G is necessarily elementary abelian. (2) Up to equivalence the Paley difference sets mentioned above are the only skew Hadamard difference sets in abelian groups. The first conjecture is still open in general. We refer the reader to [6] for the known results on this conjecture. The second conjecture failed spectacularly: Ding and Yuan [10] constructed a family of skew Hadamard difference sets in $(\mathbb{F}_{3^m}, +)$, where $m \geqslant 3$ is odd, and showed that the 2nd and the 3rd examples in the family are inequivalent to the Paley difference sets. Very recently,

E-mail addresses: feng@math.udel.edu (T. Feng), xiang@math.udel.edu (Q. Xiang).

[1] Research supported in part by NSF Grant DMS 1001557, and by the Overseas Cooperation Fund (grant 10928101) of China.

0097-3165/$ – see front matter © 2011 Published by Elsevier Inc.
doi:10.1016/j.jcta.2011.08.007

Muzychuk [24] constructed exponentially many inequivalent skew Hadamard difference sets over an elementary abelian group of order q^3.

We give a short survey of the known constructions of skew Hadamard difference sets. Shortly after the appearance of the Ding–Yuan construction [10], by using certain permutation polynomials arising from the Ree–Tits slice symplectic spreads, Ding, Wang and Xiang [11] constructed a class of skew Hadamard difference sets in $(\mathbb{F}_{3^m}, +)$, where m is odd. Next the classical Paley construction was generalized from finite fields to commutative semifields in [28]. As a consequence, every finite commutative semifield of order congruent to 3 modulo 4 gives rise to a skew Hadamard difference set. The first author [13] then constructed a family of skew Hadamard difference sets in the nonabelian group of order p^3 and exponent p, where p is an odd prime. Prior to [13], only two nonabelian skew Hadamard difference sets were known [17]; both are in nonabelian groups of order 27. Motivated by [13], Muzychuk [24] has now given a prolific construction of skew Hadamard difference sets in elementary abelian groups of order q^3, where q is a prime power. We also mention that the construction in [13] was recently generalized in [7] and [8].

Let $q = p^f$, where p is a prime and f a positive integer. Let γ be a fixed primitive element of $\mathbb{F}_q$ and $N|(q-1)$ with $N > 1$. Let $C_0 = \langle \gamma^N \rangle$, and $C_i = \gamma^i C_0$ for $1 \leqslant i \leqslant N-1$. The C_i are called the *cyclotomic classes of order N* of $\mathbb{F}_q$. In this paper, we give two constructions of skew Hadamard difference sets in the additive groups of finite fields by using unions of cyclotomic classes.

The idea of constructing difference sets (and strongly regular Cayley graphs) from cyclotomic classes of course goes back to Paley [25]. In the mid-20th century, Baumert, Chowla, Hall, Lehmer, Storer, Whiteman, Yamamoto, etc. pursued this line of research vigorously. Storer's book [26] contains a summary of results in this direction up to 1967. See also Chapter 5 of [1] for a summary. This method for constructing difference sets, however, has had only very limited success. Let C_i be as above. It is known [5, pp. 123–124] that a single cyclotomic class can form a difference set in $(\mathbb{F}_q, +)$ if $N = 2, 4,$ or 8 and q satisfies certain conditions. (Note that in order to obtain difference sets this way, the conditions on q are quite restrictive when $N = 4$ or 8.) It is conjectured that the converse is also true. Namely, if C_0 is a difference set in $(\mathbb{F}_q, +)$, then N is necessarily 2, 4, or 8. This conjecture has been verified [12] up to $N = 20$. If one uses a union of cyclotomic classes, instead of just one single class, the only new family of difference sets found in this way is the Hall sextic difference sets in $(\mathbb{F}_q, +)$ formed by taking a union of three cyclotomic classes of order 6, where $q = 4x^2 + 27$ is a prime power congruent to 1 modulo 6. One of the reasons that very few difference sets have been discovered by using unions of cyclotomic classes is that the investigations often relied on the so-called cyclotomic numbers and these numbers are in general very difficult to compute if N is large.

In this paper, we construct skew Hadamard difference sets in $(\mathbb{F}_q, +)$ by using union of cyclotomic classes of order $N = 2p_1^m$ of $\mathbb{F}_q$, where p_1 is an odd prime, q is a power of a prime p, $\gcd(p, N) = 1$, $-1 \notin \langle p \rangle \subset (\mathbb{Z}/N\mathbb{Z})^*$, and the order of p modulo N is half of $\phi(N)$ (here ϕ is the Euler phi function). This last condition is the so-called index 2 condition in the theory of Gauss sums. The significance of our constructions is twofold. First, other than the classical Paley difference sets, previously known abelian skew Hadamard difference sets were constructed either in $(\mathbb{F}_q, +)$, where q is a power of 3, or in groups of order p^{3k}, where p is an odd prime. The constructions in this paper can produce skew Hadamard difference sets in elementary abelian groups where no previous constructions were known except for the classical Paley difference sets. Secondly, our constructions demonstrate that the old idea of constructing difference sets from cyclotomic classes is not a dead end, thus it should be further exploited.

The recent success in constructing strongly regular Cayley graphs by using union of cyclotomic classes in [14] lends further credence to our opinion on cyclotomic methods for constructing difference sets. Since the constructions in this paper are motivated by those in [14], we include here a brief discussion of the results in [14]. Let D be a subset of $\mathbb{F}_q$ such that $-D = D$ and $0 \notin D$. We define the *Cayley graph* $\mathrm{Cay}(\mathbb{F}_q, D)$ to be the graph with the elements of $\mathbb{F}_q$ as vertices; two vertices are adjacent if and only if their difference belongs to D. When D is a subgroup of the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ and $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular, then we speak of a *cyclotomic strongly regular graph*. In particular, if D is the subgroup of $\mathbb{F}_q^*$ consisting of the squares, where q is a prime power congruent to 1 modulo 4, then $\mathrm{Cay}(\mathbb{F}_q, D)$ is the well-known Paley graph. In [14], we were interested in examples due to De Lange [19] and Ikuta and Munemasa [15], in which one single cyclotomic class does

not give rise to a strongly regular Cayley graph while a union of several classes does. Generalizing these examples, we give two constructions of strongly regular Cayley graphs on finite fields $\mathbb{F}_q$ by using union of cyclotomic classes of $\mathbb{F}_q$ of order N, where $N = p_1^m$ or $p_1^m p_2$, p_1 and p_2 are distinct odd primes. The main tools used in the proofs are index 2 Gauss sums. In particular, we [14] obtain twelve infinite families of strongly regular Cayley graphs with new parameters.

2. Gauss sums

Let p be a prime, f a positive integer, and $q = p^f$. Let $\xi_p = e^{2\pi i/p}$ and let ψ be the additive character of $\mathbb{F}_q$ defined by

$$\psi : \mathbb{F}_q \to \mathbb{C}^*, \qquad \psi(x) = \xi_p^{\mathrm{Tr}(x)}, \tag{2.1}$$

where Tr is the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. Let $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ be a character of $\mathbb{F}_q^*$. We define the *Gauss sum* by

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

Usually we simply write $g(\chi)$ for $g_{\mathbb{F}_q}(\chi)$ if the finite field involved is clear from the context. Note that if χ_0 is the trivial multiplicative character of $\mathbb{F}_q$, then $g(\chi_0) = -1$. We are usually concerned with nontrivial Gauss sums $g(\chi)$, i.e., those with $\chi \neq \chi_0$. 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 $c \in \mathbb{F}_q^*$,

$$\psi(c) = \frac{1}{q-1} \sum_{\chi \in \widehat{\mathbb{F}}_q^*} g(\bar{\chi})\chi(c), \tag{2.2}$$

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

We first recall a few elementary properties of Gauss sums. For proofs of these properties, see [4, Theorem 1.1.4]. The first is

$$g(\chi)\overline{g(\chi)} = q, \quad \text{if } \chi \neq \chi_0. \tag{2.3}$$

The second is

$$g\big(\chi^p\big) = g(\chi), \tag{2.4}$$

and the third one is

$$g\big(\chi^{-1}\big) = \chi(-1)\overline{g(\chi)}. \tag{2.5}$$

While it is easy to determine the absolute value of nontrivial Gauss sums (see (2.3)), the explicit evaluation of Gauss sums is a difficult problem. However, there are a few cases where the Gauss sums $g(\chi)$ can be explicitly evaluated. The simplest case is the so-called *semi-primitive case*, where there exists an integer j such that $p^j \equiv -1 \pmod N$ (here N is the order of χ in $\widehat{\mathbb{F}}_q^*$). Some authors [3,4] also refer to this case as uniform cyclotomy, or pure Gauss sums. We refer the reader to [4, p. 364] for the precise evaluation of Gauss sums in this case.

The next interesting case is the index 2 case, where -1 is not in the subgroup $\langle p \rangle$, the cyclic group generated by p, and $\langle p \rangle$ has index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$ (again here N is the order of χ in $\widehat{\mathbb{F}}_q^*$). Many authors have studied this case, including Baumert and Mykkeltveit [2], McEliece [22], Langevin [20], Mbodj [21], Meijer and Van der Vlugt [23], and Yang and Xia [30]. In the index 2 case, it can be shown that N has at most two odd prime divisors. For the purpose of constructing difference sets by taking union of cyclotomic classes, we will need N to be even and $(q-1)/N$ to be odd (cf. [5, p. 357]). Below is the result on evaluation of Gauss sums that we will need in Section 3.

Theorem 2.1. *(See [30, Theorem 4.4, Case D].) Let $N = 2p_1^m$, where $p_1 > 3$ is a prime, $p_1 \equiv 3 \pmod 4$ and m is a positive integer. Assume that p is a prime, $\gcd(p, N) = 1$, $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle] = 2$. Let $f = \phi(N)/2$, $q = p^f$, and χ be a character of order N of $\mathbb{F}_q^*$. Then*

$$g(\chi) = \begin{cases} (-1)^{\frac{p-1}{2}m}\sqrt{p^*}\,p^{\frac{f-1}{2}}, & \text{if } p_1 \equiv 7 \pmod 8, \\ (-1)^{\frac{p-1}{2}(m+1)}\sqrt{p^*}\,p^{\frac{f-1}{2}-h}\left(\frac{b+c\sqrt{-p_1}}{2}\right)^2, & \text{if } p_1 \equiv 3 \pmod 8, \end{cases}$$

where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, $p^* = (-1)^{\frac{p-1}{2}}p$, and b, c are integers satisfying the following conditions

(i) $b, c \not\equiv 0 \pmod p$,
(ii) $b^2 + p_1c^2 = 4p^h$,
(iii) $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$.

Moreover, when $p \equiv 3 \pmod 4$, we have

(1) *for $0 \leqslant t \leqslant m-1$,*

$$g\left(\chi^{p_1^t}\right) = \begin{cases} (-1)^m\sqrt{-p}\,p^{(f-1)/2}, & \text{if } p_1 \equiv 7 \pmod 8, \\ (-1)^{m+1}\sqrt{-p}\,p^{(f-1)/2-hp_1^t}\left(\frac{b+c\sqrt{-p_1}}{2}\right)^{2p_1^t}, & \text{if } p_1 \equiv 3 \pmod 8; \end{cases}$$

(2) $g(\chi^{2p_1^t}) = p^{(f-p_1^th)/2}\left(\frac{b+c\sqrt{-p_1}}{2}\right)^{p_1^t}$;
(3) $g(\chi^{p_1^m}) = (-1)^{(f-1)/2}p^{(f-1)/2}\sqrt{-p}$.

We will also need the Stickelberger congruence for Gauss sums, which we state below. Let p be a prime, $q = p^f$, and 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

$$\omega_{\mathfrak{P}}(\alpha) \pmod{\mathfrak{P}} = \alpha, \tag{2.6}$$

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 $\mathcal{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q-1}, \xi_p]$ lying above $\mathfrak{P}$. For an integer a, let

$$s(a) = v_{\mathcal{P}}\left(g\left(\omega_{\mathfrak{P}}^{-a}\right)\right),$$

where $v_{\mathcal{P}}$ is the $\mathcal{P}$-adic valuation. Thus $\mathcal{P}^{s(a)} \parallel g(\omega_{\mathfrak{P}}^{-a})$. The following evaluation of $s(a)$ is due to Stickelberger (see [4, p. 344]).

Theorem 2.2. *Let p be a prime and $q = p^f$. For an integer a not divisible by $q-1$, let $a_0 + a_1p + a_2p^2 + \cdots + a_{f-1}p^{f-1}$, $0 \leqslant a_i \leqslant p-1$, be the p-adic expansion of the reduction of a modulo $q-1$. Then*

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

that is, $s(a)$ is the sum of the p-adic digits of the reduction of a modulo $q-1$. Furthermore, define

$$t(a) = a_0!a_1!\cdots a_{f-1}!, \qquad \pi = \xi_p - 1.$$

Then with $s(a)$ and $\omega_{\mathfrak{P}}$ as above we have the congruence

$$g\left(\omega_{\mathfrak{P}}^{-a}\right) \equiv -\frac{\pi^{s(a)}}{t(a)} \pmod{\mathcal{P}^{s(a)+1}}.$$

3. Cyclotomic constructions of difference sets

We first recall a well-known lemma in the theory of difference sets.

Lemma 3.1. *Let G be an abelian group of order v, D be a subset of G of size k, and let λ be a positive integer. Then D is a (v,k,λ) difference set in G if and only if*

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

for every nontrivial complex character χ of G. Here, $\chi(D)$ stands for $\sum_{d\in D}\chi(d)$. Moreover suppose that $D\cap D^{(-1)}=\emptyset$ and $1\notin D$. Then D is a skew Hadamard difference set in G if and only if

$$\chi(D) = \frac{-1\pm\sqrt{-v}}{2} \tag{3.1}$$

for every nontrivial complex character χ of G.

Paley type partial difference sets are counterparts of skew Hadamard difference sets. We give the definition of these sets here. Let G be a finite (multiplicative) group of order v. A k-element subset D of G is called a (v,k,λ,μ) *partial difference set* (PDS, in short) provided that the list of "differences" xy^{-1}, $x,y\in D$, $x\neq y$, contains each nonidentity element of D exactly λ times and each nonidentity element of $G\backslash D$ exactly μ times. Furthermore, assume that $v\equiv 1 \pmod 4$. A subset D of G, $1\notin D$, is called a *Paley type PDS* if D is a $(v,\frac{v-1}{2},\frac{v-5}{4},\frac{v-1}{4})$ PDS. The set of nonzero squares in $\mathbb{F}_q$, $q\equiv 1 \pmod 4$, is an example of Paley type PDS, which is usually called *the Paley PDS* in $\mathbb{F}_q$. The strongly regular Cayley graph constructed from the Paley PDS is the Paley graph.

All constructions in this section are done in the following specific index 2 case: $N=2p_1^m$, $p_1>3$ is a prime, and $p_1\equiv 3 \pmod 4$; p is a prime such that $\gcd(p,N)=1$, $-1\notin\langle p\rangle\subset(\mathbb{Z}/N\mathbb{Z})^*$, and $[(\mathbb{Z}/N\mathbb{Z})^*:\langle p\rangle]=2$ (that is, $f:=\mathrm{ord}_N(p)=\phi(N)/2$).

3.1. The $p_1\equiv 7 \pmod 8$ case

We first give a construction of skew Hadamard difference sets in the case where $p_1\equiv 7 \pmod 8$. Let p be a prime such that $\gcd(p,N)=1$. Write $f:=\mathrm{ord}_N(p)=\phi(N)/2$ (so $N|(p^f-1)$). Let $E=\mathbb{F}_{q^s}$ be an extension field of $\mathbb{F}_q$, where $q=p^f$. Let γ be a fixed primitive element of E, let $C_0=\langle\gamma^N\rangle$ and $C_i=\gamma^i C_0$ for $1\leqslant i\leqslant N-1$.

Theorem 3.2. *Assume that we are in the index 2 case as specified above, and $E=\mathbb{F}_{q^s}$ with s odd. Let I be any subset of $\mathbb{Z}/N\mathbb{Z}$ such that $\{i \pmod{p_1^m} \mid i\in I\}=\mathbb{Z}/p_1^m\mathbb{Z}$, and let $D=\bigcup_{i\in I}C_i$. Then D is a skew Hadamard difference set in $(E,+)$ if $p\equiv 3 \pmod 4$ and D is a Paley type PDS if $p\equiv 1 \pmod 4$.*

Proof. We shall only give the proof in the case where $p\equiv 3 \pmod 4$. The proof in the case where $p\equiv 1 \pmod 4$ is similar. First, we note that since $p\equiv 3 \pmod 4$ and s is odd, we have $-1\in C_{p_1^m}$. By the choice of I, we have $-D\cap D=\emptyset$. Secondly, observe that since $p_1\equiv 7 \pmod 8$, we have $f-1=\frac{p_1-1}{2}p_1^{m-1}-1\equiv(-1)^m-1 \pmod 4$. Therefore $(-1)^{(f-1)/2}=(-1)^m$. Thirdly, let η be any character of $\mathbb{F}_q^*$ of order N. By Theorem 2.1 and the second observation, we have that for every $0\leqslant t\leqslant m$, $g_{\mathbb{F}_q}(\eta^{p_1^t})=(-1)^m p^{(f-1)/2}\sqrt{-p}$; so by (2.5),

$$g_{\mathbb{F}_q}\left(\eta^{-p_1^t}\right)=\eta^{p_1^t}(-1)\overline{g_{\mathbb{F}_q}\left(\eta^{p_1^t}\right)}=(-1)^m p^{(f-1)/2}\sqrt{-p}.$$

Now by the index 2 assumption, any integer in the set $\{i\mid 1\leqslant i\leqslant N-1,\gcd(i,N)=1\}$ is congruent (modulo N) to an element in $\langle p\rangle$ or an element in $-\langle p\rangle$. Therefore all odd integers in the interval $[1,N-1]$ are congruent to $\pm p^r p_1^t$ modulo N. Using (2.4) and the third observation above, with η being any character of $\mathbb{F}_q^*$ of order N, we have

$$g_{\mathbb{F}_q}\left(\eta^{-j}\right)=(-1)^m p^{(f-1)/2}\sqrt{-p}$$

for all odd integers j, $1\leqslant j\leqslant N-1$.

Now let χ be an arbitrary character of E^* of order N. Since $N|(q-1)$, χ is the lift of some character η of $\mathbb{F}_q^*$ and $o(\eta) = N$ (see [4, Theorem 11.4.4]). Following the notation of [4], we write $\chi = \eta'$. It follows that $\chi^j = (\eta^j)'$ for all $1 \leqslant j \leqslant N-1$. Using the Davenport–Hasse theorem on lifted Gauss sums [4, p. 360], we have that for all odd integers j, $1 \leqslant j \leqslant N-1$,

$$g_E\left(\chi^{-j}\right) = (-1)^{s-1} g_{\mathbb{F}_q}\left(\eta^{-j}\right)^s = (-1)^m p^{\frac{s(f-1)}{2}} (\sqrt{-p})^s. \tag{3.2}$$

We will prove the result stated in the theorem by using the second part of Lemma 3.1. To this end, let a be an arbitrary integer such that $0 \leqslant a \leqslant N-1$ and let ψ be the additive character of E defined as in (2.1), with $\mathbb{F}_q$ replaced by E. We compute

$$\begin{aligned}\psi\left(\gamma^a D\right) &= \sum_{i\in I} \psi\left(\gamma^a C_i\right) \\ &= \frac{1}{N} \sum_{i\in I} \sum_{x\in E^*} \psi\left(\gamma^{a+i} x^N\right) \\ &= \frac{1}{N} T_a,\end{aligned}$$

where

$$T_a = \sum_{\theta\in C_0^\perp} g_E(\bar{\theta}) \sum_{i\in I} \theta\left(\gamma^{a+i}\right).$$

Here $C_0^\perp$ is the unique subgroup of order N of $\widehat{E}^*$. Note that in the last step of the above calculations we have used (2.2).

We now proceed to computing the sum T_a. If $\theta \in C_0^\perp$ and $o(\theta) = 1$, then $g_E(\bar{\theta}) = -1$, and $\sum_{i\in I} \theta(\gamma^{a+i}) = p_1^m$. If $\theta \in C_0^\perp$, $o(\theta) \neq 1$, and $o(\theta)$ is odd, then $\sum_{i\in I} \theta(\gamma^{a+i}) = \sum_{i=0}^{p_1^m-1} \theta(\gamma^{a+i}) = \theta(\gamma^a) \frac{\theta(\gamma)^{p_1^m}-1}{\theta(\gamma)-1} = 0$. Therefore, with χ a fixed generator of $C_0^\perp$, we have

$$T_a = -p_1^m + \sum_{j \text{ odd},\, 1\leqslant j\leqslant N-1} g_E\left(\chi^{-j}\right) \sum_{i\in I} \chi^j\left(\gamma^{a+i}\right).$$

Using (3.2) and writing ξ_N for $\chi(\gamma)$, a complex primitive Nth root of unity, we have

$$\begin{aligned}T_a &= -p_1^m + (-1)^m p^{s(f-1)/2} (\sqrt{-p})^s \sum_{u=0}^{p_1^m-1} \sum_{i\in I} \chi^{1+2u}\left(\gamma^{a+i}\right) \\ &= -p_1^m + (-1)^m p^{s(f-1)/2} (\sqrt{-p})^s \sum_{i\in I} \xi_N^{a+i} \left(\sum_{u=0}^{p_1^m-1} \xi_{p_1^m}^{u(a+i)} \right).\end{aligned}$$

For each a, $0 \leqslant a \leqslant N-1$, there is a unique $i_a \in I$ such that $p_1^m | (a + i_a)$. Write $a + i_a = p_1^m j_a$ for some integer j_a. Then

$$T_a = -p_1^m + (-1)^m p^{s(f-1)/2} (\sqrt{-p})^s (-1)^{j_a} p_1^m.$$

It follows that

$$\psi\left(\gamma^a D\right) = \frac{-1 + (-1)^{m+j_a} \sqrt{-p^{sf}}}{2}.$$

By Lemma 3.1, D is a skew Hadamard difference set in $(E, +)$. The proof is now complete. □

Example 3.3. Let $p_1 = 7$, $N = 14$, $p = 11$. Then it is routine to check that $\mathrm{ord}_N(p) = 3 = \phi(N)/2$. Let C_i, $0 \leqslant i \leqslant 13$, be the cyclotomic classes of order 14 of $\mathbb{F}_{11^3}$.

(1) Take $I = \{0, 1, \ldots, 6\}$. Then by Theorem 3.2, $D = C_0 \cup C_1 \cup \cdots \cup C_6$ is a skew Hadamard difference set in $(\mathbb{F}_{11^3}, +)$. Let $\mathrm{Dev}(D)$ denote the symmetric design developed from the difference set D. One can use a computer to find that $\mathrm{Aut}(\mathrm{Dev}(D))$ has size $5 \cdot 11^3 \cdot 19$.
(2) Take $I = \{0, 1, 3, 4, 5, 6, 9\}$. Then by Theorem 3.2, $D' = C_0 \cup C_1 \cup C_3 \cup C_4 \cup C_5 \cup C_6 \cup C_9$ is also a skew Hadamard difference set in $(\mathbb{F}_{11^3}, +)$. One finds by using a computer that $\mathrm{Aut}(\mathrm{Dev}(D'))$ has size $3 \cdot 5 \cdot 11^3 \cdot 19$.

The automorphism group of the Paley design has size $3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 19$. So the three difference sets D, D' and the Paley difference set in $(\mathbb{F}_{11^3}, +)$ are pairwise inequivalent. Also note that the sizes of the Sylow p-subgroups of $\mathrm{Aut}(\mathrm{Dev}(D))$ and $\mathrm{Aut}(\mathrm{Dev}(D'))$ are $q = 11^3$, while the size of the Sylow p-subgroups of the automorphism groups of the designs developed from the difference sets constructed by Muzychuk [24] is strictly greater than q, we conclude that both D and D' are inequivalent to the corresponding skew Hadamard difference sets in [24].

Remark 3.4.

(1) The automorphism group of the Paley design is determined in [16]. Our construction in Theorem 3.2 includes the Paley construction as a special case. It seems difficult to generalize the method in [16] to determine the automorphism groups of the designs developed from our difference sets. Based on some computational evidence, we conjecture that $\mathrm{Aut}(\mathrm{Dev}(D))$, with $D = \bigcup_{i \in I} C_i$ as given in the statement of the theorem, is generated by the following three types of elements: (i) translations by elements of E, (ii) multiplications by elements in C_0, and (iii) σ_p^i, $p^i I = I$, where σ_p is the Frobenius automorphism of the finite field $\mathbb{F}_{p^{sf}}$.
(2) Let $N = 2 \cdot 7^m$, where $m \geqslant 2$. One can use induction to prove that $\mathrm{ord}_N(11) = 3 \cdot 7^{m-1} = \phi(N)/2$. Therefore the conditions of Theorem 3.2 are satisfied. So the examples in Example 3.3 can be generalized into infinite families.

3.2. The $p_1 \equiv 3 \pmod 8$ case

We will again do the constructions in the index 2 case as specified at the beginning of this section. In addition, we will assume that

(1) $p_1 \equiv 3 \pmod 8$, $(p_1 \neq 3)$,
(2) $N = 2p_1$,
(3) $1 + p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$,
(4) $p \equiv 3 \pmod 4$.

Let $q = p^f$, $f = \mathrm{ord}_N(p) = \phi(N)/2$. As in Section 2, let ξ_{q-1} be a primitive complex $(q-1)$th root of unity, and $\mathfrak{P}$ be a prime ideal in $\mathbb{Z}[\xi_{q-1}]$ lying over p. Then $\mathbb{Z}[\xi_{q-1}]/\mathfrak{P}$ is a finite field of order q. We will use $\mathbb{Z}[\xi_{q-1}]/\mathfrak{P}$ as a model for $\mathbb{F}_q$. That is,

$$\mathbb{F}_q = \left\{\bar{0}, \bar{1}, \bar{\xi}_{q-1}, \bar{\xi}_{q-1}^2, \ldots, \bar{\xi}_{q-1}^{q-2}\right\}, \tag{3.3}$$

where $\bar{\xi}_{q-1} = \xi_{q-1} \pmod{\mathfrak{P}}$. Hence $\gamma := \bar{\xi}_{q-1}$ is a primitive element of $\mathbb{F}_q$. Let $\omega_{\mathfrak{P}}$ be the Teichmüller character of $\mathbb{F}_q$. Then

$$\omega_{\mathfrak{P}}(\gamma) = \xi_{q-1}.$$

Let $\chi = \omega_{\mathfrak{P}}^{(q-1)/N}$. Then χ is a character of $\mathbb{F}_q^*$ of order $N = 2p_1$ (and χ depends on the choice of $\mathfrak{P}$). To simplify notation, we write ξ_N for $\chi(\gamma) = \xi_{q-1}^{(q-1)/N}$ and ξ_{p_1} for $\chi^2(\gamma) = \xi_{q-1}^{\frac{q-1}{p_1}}$. Next let $n = (q-1)/p_1$. By the result in [20] (see also [4, p. 376]), we have

(1) $s(-n) = (p-1)b_0$, $s(n) = (p-1)b_1$ for some positive integers b_0, b_1, and $b_0 > b_1 = \frac{f-h}{2}$,

(2) $g(\chi^2) = p^{\frac{f-h}{2}} \frac{(b+c\sqrt{-p_1})}{2}$, where b, c are integers satisfying (i) $b, c \not\equiv 0 \pmod{p}$, (ii) $b^2 + p_1 c^2 = 4p^h$, (iii) $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$.

By the assumption that $1 + p_1 = 4p^h$, we must have $b, c \in \{1, -1\}$. The sign of b is determined by the congruence in (iii). The sign of c depends on the choice of $\mathfrak{P}$. We have the following:

Lemma 3.5. *With notation as above,* $bc \equiv -\sqrt{-p_1} \pmod{\mathfrak{P}}$.

Proof. Let $\mathcal{P}$ be the unique prime ideal of $\mathbb{Z}[\xi_{q-1}, \xi_p]$ lying above $\mathfrak{P}$. Applying the Stickelberger congruence to $g(\chi^2) = g(\omega_{\mathfrak{P}}^n)$, we have

$$g(\chi^2) = p^{\frac{f-h}{2}} \frac{(b + c\sqrt{-p_1})}{2} \equiv -\frac{\pi^{s(-n)}}{t(-n)} \quad \big(\mathrm{mod}\ \mathcal{P}^{s(-n)+1}\big).$$

Now using the fact that $p = \prod_{i=1}^{p-1}(1-\xi_p^i) \equiv \pi^{p-1} \prod_{i=1}^{p-1} i \equiv -\pi^{p-1} \pmod{\mathcal{P}^p}$, we can further simplify the above congruence to

$$b + c\sqrt{-p_1} \equiv 2(-1)^{1+\frac{f-h}{2}} \frac{\pi^{(p-1)(b_0-(f-h)/2)}}{t(-n)} \equiv 0 \pmod{\mathcal{P}},$$

where in the last step we have used the nontrivial fact that $b_0 > b_1 = \frac{f-h}{2}$. Therefore $bc \equiv -\sqrt{-p_1} \pmod{\mathcal{P}}$. Since $\sqrt{-p_1} \in \mathbb{Z}[\xi_{p_1}] \subset \mathbb{Z}[\xi_{q-1}]$, we have $bc + \sqrt{-p_1} \in \mathcal{P} \cap \mathbb{Z}[\xi_{q-1}] = \mathfrak{P}$. That is, $bc \equiv -\sqrt{-p_1} \pmod{\mathfrak{P}}$. The proof is complete. □

Since $1 + p_1 = 4p^h$, we have $(1 + \sqrt{-p_1})(1 - \sqrt{-p_1}) \in \mathfrak{P}$ for any prime ideal $\mathfrak{P}$ of $\mathbb{Z}[\xi_{q-1}]$ lying above p. It follows that either $1 + \sqrt{-p_1} \in \mathfrak{P}$ or $1 - \sqrt{-p_1} \in \mathfrak{P}$. We can choose a prime ideal $\mathfrak{P}$ (and then fix this choice) such that

$$1 + \sqrt{-p_1} \in \mathfrak{P}. \tag{3.4}$$

The corresponding b, c in the evaluation of $g(\chi^2)$ will then satisfy $bc = 1$ by Lemma 3.5. These discussions were essentially done in [31]. But there are a few minor problems in that paper. That is the reason why we gave the detailed account here.

By the index 2 assumption, we see that $\{i \pmod{p_1} \mid i \in \langle p \rangle\}$ is the set of nonzero squares of $\mathbb{Z}/p_1\mathbb{Z}$. Consequently, $\sum_{i\in\langle p\rangle} \xi_{p_1}^i = \frac{-1\pm\sqrt{-p_1}}{2}$. It follows that $1 + 2\sum_{i\in\langle p\rangle} \xi_{p_1}^i \equiv \pm\sqrt{-p_1} \equiv \mp 1 \pmod{\mathfrak{P}}$. Hence $1 + 2\sum_{i\in\langle p\rangle} \gamma^{in} = \mp 1$. Since $\sum_{i\in\langle p\rangle} \xi_{p_1}^i + \sum_{i\in\langle p\rangle} \xi_{p_1}^{-i} = -1$, we have

$$\left(1 + 2\sum_{i\in\langle p\rangle} \gamma^{in}\right) + \left(1 + 2\sum_{i\in\langle p\rangle} \gamma^{-in}\right) = 0.$$

Hence we can make a suitable choice of ξ_{q-1} (that is, if necessary replace the originally chosen ξ_{q-1} by ξ_{q-1}^{-1}) such that $1 + 2\sum_{i\in\langle p\rangle} \gamma^{in} = -1$.

We now give the construction of difference sets by using unions of cyclotomic classes. Let $\mathbb{F}_q$ be given as in (3.3) with $\mathfrak{P}$ chosen in such a way that (3.4) holds, and $\gamma = \bar{\xi}_{q-1}$ be the primitive element of $\mathbb{F}_q$ chosen above such that $1 + 2\sum_{i\in\langle p\rangle} \gamma^{in} = -1$. Let $N = 2p_1$ and let $C_0 = \langle \gamma^N \rangle$, and $C_i = \gamma^i C_0$ for $i = 1, 2, \ldots, N-1$, be the cyclotomic classes of $\mathbb{F}_q$ of order N. Choose $I = \langle p \rangle \cup 2\langle p \rangle \cup \{0\}$, and define

$$D := \bigcup_{i\in I} C_i.$$

Note that $|I| = p_1$, and since 2 is a quadratic nonresidue modulo p_1, we have $\{i \pmod{p_1} \mid i \in I\} = \mathbb{Z}/p_1\mathbb{Z}$.

Theorem 3.6. *With the above definition, D is a skew Hadamard difference set in $(\mathbb{F}_q, +)$.*

Proof. Since $-1 \in C_{p_1}$ and 2 is a quadratic nonresidue modulo p_1, we have $-D \cap D = \emptyset$. That is, D is skew.

We now proceed to proving the result by using the second part of Lemma 3.1. To this end, let a be an arbitrary integer such that $0 \leqslant a \leqslant N-1$ and let ψ be the additive character defined as in (2.1). Also let $\chi = \omega_{\mathfrak{P}}^{(q-1)/N}$, where $\mathfrak{P}$ is chosen such that (3.4) holds. We have

$$\begin{aligned}\psi\big(\gamma^a D\big) &= \sum_{i\in I} \psi\big(\gamma^a C_i\big)\\ &= \frac{1}{N}\sum_{i\in I}\sum_{x\in\mathbb{F}_q^*} \psi\big(\gamma^{a+i}x^N\big)\\ &= \frac{1}{N} T_a,\end{aligned}$$

where

$$T_a = \sum_{j=0}^{N-1} g\big(\chi^j\big)\sum_{i\in I}\chi^{-j}\big(\gamma^{a+i}\big).$$

When $j=0$, we have $g(\chi^0) = -1$, and $\sum_{i\in I}\chi^{-j}(\gamma^{(a+i)}) = p_1$. If $j \neq 0$ is even, then $\sum_{i\in I}\chi(\gamma^{-j(a+i)}) = \sum_{i=0}^{p_1-1}\chi(\gamma^{-j(a+i)}) = \chi(\gamma^{-ja})\frac{\chi(\gamma)^{-jp_1}-1}{\chi(\gamma^{-j})-1} = 0$. Now note that every odd integer in the interval $[1, N-1]$ is congruent (modulo N) to an element in $\langle p\rangle$, or an element in $-\langle p\rangle$, or p_1. Therefore, we have

$$T_a = -p_1 + \sum_{j\in\langle p\rangle} g\big(\chi^j\big)\sum_{i\in I}\bar{\chi}^j\big(\gamma^{a+i}\big) + \sum_{j\in-\langle p\rangle} g\big(\chi^j\big)\sum_{i\in I}\bar{\chi}^j\big(\gamma^{a+i}\big) + g\big(\chi^{p_1}\big)\sum_{i\in I}\bar{\chi}^{p_1}\big(\gamma^{a+i}\big).$$

Specializing Theorem 2.1 to the $m=1$ case and noting that $f - 1 \equiv 0 \pmod 4$ since $p_1 \equiv 3 \pmod 8$, we have

$$g(\chi) = p^{(f-1)/2-h}\sqrt{-p}\left(\frac{b+c\sqrt{-p_1}}{2}\right)^2, \qquad g\big(\chi^{p_1}\big) = p^{(f-1)/2}\sqrt{-p},$$

where b, c are the same as in the evaluation of $g(\chi^2)$ (cf. [30, p. 2531]), and $bc = 1$ by our choice of $\mathfrak{P}$. Also recall that by (2.4), we have $g(\chi^p) = g(\chi)$. We compute

$$\begin{aligned}T_a = -p_1 &+ p^{(f-1)/2-h}\sqrt{-p}\left(\frac{b+c\sqrt{-p_1}}{2}\right)^2 \sum_{j\in\langle p\rangle}\sum_{i\in I}\bar{\chi}^j\big(\gamma^{a+i}\big)\\ &+ p^{(f-1)/2-h}\sqrt{-p}\left(\frac{b-c\sqrt{-p_1}}{2}\right)^2 \sum_{j\in-\langle p\rangle}\sum_{i\in I}\bar{\chi}^j\big(\gamma^{a+i}\big)\\ &+ p^{(f-1)/2}\sqrt{-p}\sum_{i\in I}\bar{\chi}^{p_1}\big(\gamma^{a+i}\big).\end{aligned}$$

Since $\{i \pmod{p_1} \mid i \in I\} = \mathbb{Z}/p_1\mathbb{Z}$, for each a, $0 \leqslant a \leqslant N-1$, there is a unique i_a in I such that $p_1 | (a + i_a)$. Write $a + i_a = p_1 j_a$. We have

$$\sum_{j\in\langle p\rangle}\sum_{i\in I}\bar{\chi}^{j}\big(\gamma^{a+i}\big)+\sum_{j\in-\langle p\rangle}\sum_{i\in I}\bar{\chi}^{j}\big(\gamma^{a+i}\big)+\sum_{i\in I}\bar{\chi}^{p_1}\big(\gamma^{a+i}\big)$$
$$=\sum_{j\,\mathrm{odd}}\xi_N^{-j(a+i)}=\sum_{i\in I}\xi_{2p_1}^{-(a+i)}\sum_{u=0}^{p_1-1}\xi_{p_1}^{-u(a+i)}$$
$$=(-1)^{j_a}p_1.$$

In order to prove that D is a skew Hadamard difference set, we must show that

$$T_a=-p_1+p^{(f-1)/2}\sqrt{-p}p_1\epsilon_a \tag{3.5}$$

for some $\epsilon_a=\pm1$. Noting that $(\frac{b+c\sqrt{-p_1}}{2})^2=\frac{b^2-c^2p_1+2bc\sqrt{-p_1}}{4}=\frac{1-p_1+2\sqrt{-p_1}}{4}$, and

$$\sum_{j\in\langle p\rangle}\sum_{i\in I}\bar{\chi}^{j}\big(\gamma^{a+i}\big)+\sum_{j\in-\langle p\rangle}\sum_{i\in I}\bar{\chi}^{j}\big(\gamma^{a+i}\big)+\sum_{i\in I}\bar{\chi}^{p_1}\big(\gamma^{a+i}\big)=(-1)^{j_a}p_1,$$

one simplifies (3.5) to

$$\frac{1-p_1}{4p^h}p_1(-1)^{j_a}+\left(1-\frac{1-p_1}{4p^h}\right)(-1)^a+\frac{\sqrt{-p_1}}{2p^h}X_a=p_1\epsilon_a,$$

where $X_a=\sum_{j\in\langle p\rangle}\sum_{i\in I}\xi_N^{-j(a+i)}-\sum_{j\in-\langle p\rangle}\sum_{i\in I}\xi_N^{-j(a+i)}$. Using the assumption that $1+p_1=4p^h$, one further simplifies the last equation to

$$(1-p_1)(-1)^{j_a}+2(-1)^a-2\frac{X_a}{\sqrt{-p_1}}=(1+p_1)\epsilon_a. \tag{3.6}$$

Below we will prove that (3.6) always holds, thus proving that D is a skew Hadamard difference set. We recall some useful facts.

(1) $\{i \pmod{p_1} \mid i\in\langle p\rangle\}$ is the set of nonzero squares of $\mathbb{Z}/p_1\mathbb{Z}$.
(2) The odd integers $\frac{p_1-1}{2}$ and p_1-2 are congruent to elements in $\langle p\rangle$ modulo p_1 since both 2 and -1 are nonresidues modulo p_1.
(3) By our choice of ξ_{q-1} we have $\sum_{i\in\langle p\rangle}\xi_{p_1}^{i}=\frac{-1+\sqrt{-p_1}}{2}$.
(4) We have $\sum_{i\in\langle p\rangle}\xi_N^{-i}=\sum_{i\in\langle p\rangle}\xi_N^{(2\cdot(p_1-1)/2-p_1)i}=\sum_{i\in\langle p\rangle}\xi_{p_1}^{\frac{p_1-1}{2}i}(-1)^i=-\frac{-1+\sqrt{-p_1}}{2}=\frac{1-\sqrt{-p_1}}{2}$, since $\frac{p_1-1}{2}$ is a square in $\mathbb{Z}/p_1\mathbb{Z}$.

Now set $Y_a:=\sum_{j\in\langle p\rangle}\sum_{i\in I}\xi_N^{-j(a+i)}$. Then $X_a=Y_a-\overline{Y_a}$. We have

$$Y_a=\sum_{j\in\langle p\rangle}\xi_N^{-aj}\sum_{i\in I}\xi_N^{-ij}=\left(\sum_{j\in\langle p\rangle}\xi_N^{-aj}\right)\left(\sum_{i\in I}\xi_N^{-i}\right).$$

The last sum above, $\sum_{i\in I}\xi_N^{-i}$, can be evaluated as follows: $\sum_{i\in I}\xi_N^{-i}=\sum_{i\in\langle p\rangle}\xi_N^{-i}+\sum_{i\in 2\langle p\rangle}\xi_N^{-i}+1=\frac{1-\sqrt{-p_1}}{2}+\frac{-1-\sqrt{-p_1}}{2}+1=1-\sqrt{-p_1}$. Therefore

$$Y_a=\left(\sum_{j\in\langle p\rangle}\xi_N^{-aj}\right)(1-\sqrt{-p_1}).$$

We consider the following six cases.

Case 1. $a=0$. In this case, $i_a=0$, $j_a=0$. We have $\sum_{j\in\langle p\rangle}\xi_N^{-aj}=\frac{p_1-1}{2}$, $Y_a=\frac{p_1-1}{2}(1-\sqrt{-p_1})$, and $X_a=-(p_1-1)\sqrt{-p_1}$. Condition (3.6) is satisfied with $\epsilon_a=1$.

Case 2. $a \in \langle p\rangle$. In this case, $i_a = 2 \cdot \frac{p_1-1}{2} a \in 2\langle p\rangle$. $j_a = a \equiv 1 \pmod 2$. We have $\sum_{j\in\langle p\rangle} \xi_N^{-aj} = \sum_{j\in\langle p\rangle} \xi_N^{-j} = \frac{1-\sqrt{-p_1}}{2}$, $Y_a = \frac{1-\sqrt{-p_1}}{2} \cdot (1-\sqrt{-p_1}) = \frac{1-p_1}{2} - \sqrt{-p_1}$, and $X_a = -2\sqrt{-p_1}$. Condition (3.6) is satisfied with $\epsilon_a = 1$.

Case 3. $a \in -\langle p\rangle$. In this case, $i_a = -a \in \langle p\rangle$, $j_a = 0$. We have $\sum_{j\in\langle p\rangle} \xi_N^{-aj} = \sum_{j\in\langle p\rangle} \xi_N^{j} = \frac{1+\sqrt{-p_1}}{2}$, $Y_a = \frac{1+\sqrt{-p_1}}{2} \cdot (1-\sqrt{-p_1}) = \frac{p_1+1}{2}$, and $X_a = 0$. Condition (3.6) is satisfied with $\epsilon_a = -1$.

Case 4. $a \in 2\langle p\rangle$. In this case, write $a = 2u$ for some $u \in \langle p\rangle$. We have $i_a = (p_1-2)u \in \langle p\rangle$, $j_a = u \equiv 1 \pmod 2$, and $\sum_{j\in\langle p\rangle} \xi_N^{-aj} = \sum_{j\in\langle p\rangle} \xi_{p_1}^{-j} = \frac{-1-\sqrt{-p_1}}{2}$. It follows that $Y_a = \frac{-1-\sqrt{-p_1}}{2} \cdot (1-\sqrt{-p_1}) = -\frac{p_1+1}{2}$. Thus $X_a = 0$. Condition (3.6) is satisfied with $\epsilon_a = 1$.

Case 5. $a \in -2\langle p\rangle$. In this case, $i_a = -a \in 2\langle p\rangle$, $j_a = 0$. We have $\sum_{j\in\langle p\rangle} \xi_N^{-aj} = \sum_{j\in\langle p\rangle} \xi_{p_1}^{j} = \frac{-1+\sqrt{-p_1}}{2}$, $Y_a = \frac{-1+\sqrt{-p_1}}{2} \cdot (1-\sqrt{-p_1}) = \frac{-1+p_1}{2} + \sqrt{-p_1}$, and $X_a = 2\sqrt{-p_1}$. Condition (3.6) is satisfied with $\epsilon_a = -1$.

Case 6. $a = p_1$. In this case, $i_a = 0$, $j_a = 1$. We have $\sum_{j\in\langle p\rangle} \xi_N^{-aj} = -\frac{(p_1-1)}{2}$, $Y_a = -\frac{(p_1-1)}{2}(1-\sqrt{-p_1})$, and $X_a = (p_1-1)\sqrt{-p_1}$. Condition (3.6) is satisfied with $\epsilon_a = -1$.

The proof is now complete. □

Remark 3.7. It would be interesting to extend the construction in Theorem 3.6 to the general case where $N = 2p_1^m$, $p_1 \equiv 3 \pmod 8$ and $m \geqslant 2$ is arbitrary. If this can be done, then we will obtain infinite families of skew Hadamard difference sets in this way even though currently we only know finitely many pairs (p_1, p) such that $1 + p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$.

Example 3.8. Let $p = 3$, $N = 22$, $p_1 = 11$. It is routine to check that $\mathrm{ord}_{22}(3) = 5 = \phi(N)/2$. Let $f = 5$, $q = 3^5$ and $n = \frac{q-1}{p_1}$. The class number h of $\mathbb{Q}(\sqrt{-11})$ is 1 (cf. [9, p. 514]). Therefore the condition $1 + p_1 = 4p^h$ is indeed satisfied. Let $\mathbb{F}_{3^5}$ be the finite field as in (3.3) with $\mathfrak{P}$ chosen in such a way that (3.4) holds. Choose a primitive element γ of $\mathbb{F}_{3^5}$ such that γ such that $1 + 2\sum_{i\in\langle p\rangle} \gamma^{in} = -1$, and let C_i, $0 \leqslant i \leqslant 21$, be the cyclotomic classes with respect to this choice of γ. Define $I := \langle 3\rangle \cup 2\langle 3\rangle \cup \{0\} = \{0, 1, 2, 3, 5, 6, 8, 9, 10, 15, 18\}$. Then $D = \bigcup_{i\in I} C_i$ is a skew Hadamard difference set in $(\mathbb{F}_{3^5}, +)$. Using a computer one finds that $\mathrm{Aut}(\mathrm{Dev}(D))$ has size $3^5 \cdot 5 \cdot 11$, while the automorphism group of the corresponding Paley design has size $3^5 \cdot 5 \cdot 11^2$. We conclude that $\mathrm{Dev}(D)$ is not isomorphic to the Paley design.

References

[1] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Math., vol. 182, Springer-Verlag, 1971.
[2] L.D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, DSN Progr. Rep. 16 (1973) 128–131.
[3] L.D. Baumert, M.H. Mills, R.L. Ward, Uniform cyclotomy, J. Number Theory 14 (1982) 67–82.
[4] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, Wiley–Interscience, 1998.
[5] T. Beth, D. Jungnickel, H. Lenz, Design Theory, vol. I, second edition, Encyclopedia Math. Appl., vol. 78, Cambridge University Press, Cambridge, 1999.
[6] Y.Q. Chen, Q. Xiang, S. Sehgal, An exponent bound on skew Hadamard abelian difference sets, Des. Codes Cryptogr. 4 (1994) 313–317.
[7] Y.Q. Chen, J. Polhill, Paley type group schemes and planar Dembowski–Ostrom polynomials, Discrete Math. 311 (2011) 1349–1364.
[8] Y.Q. Chen, T. Feng, Abelian and non-abelian Paley type group schemes, preprint.
[9] H. Cohen, A Course in Computational Algebraic Number Theory, GTM, vol. 138, Springer, 1996.
[10] C. Ding, J. Yuan, A family of skew Hadamard difference sets, J. Combin. Theory Ser. A 113 (2006) 1526–1535.
[11] C. Ding, Z. Wang, Q. Xiang, Skew Hadamard difference sets from the Ree–Tits slice symplectic spreads in $PG(3, 3^{2h+1})$, J. Combin. Theory Ser. A 114 (2007) 867–887.
[12] R.J. Evans, Nonexistence of twentieth power residue difference sets, Acta Arith. 84 (1999) 397–402.

[13] T. Feng, Non-abelian skew Hadamard difference sets fixed by a prescribed automorphism, J. Combin. Theory Ser. A 118 (2011) 27–36.
[14] T. Feng, Q. Xiang, Strongly regular graphs from union of cyclotomic classes, arXiv:1010.4107v2.
[15] T. Ikuta, A. Munemasa, Pseudocyclic association schemes and strongly regular graphs, European J. Combin. 31 (2010) 1513–1519.
[16] W.M. Kantor, 2-Transitive symmetric designs, Trans. Amer. Math. Soc. 146 (1969) 1–28.
[17] R.E. Kibler, A summary of noncyclic difference sets, $k < 20$, J. Combin. Theory Ser. A 25 (1978) 62–67.
[18] E.S. Lander, Symmetric Designs: An Algebraic Approach, Cambridge University Press, 1983.
[19] C.L.M. de Lange, Some new cyclotomic strongly regular graphs, J. Algebraic Combin. 4 (1995) 329–330.
[20] P. Langevin, Calculs de certaines sommes de Gauss, J. Number Theory 63 (1997) 59–64.
[21] O.D. Mbodj, Quadratic Gauss sums, Finite Fields Appl. 4 (1998) 347–361.
[22] R.J. McEliece, Irreducible cyclic codes and Gauss sums, in: Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of Designs, Finite Geometry and Coding Theory, in: Math. Centre Tracts, vol. 55, Math. Centrum, Amsterdam, 1974, pp. 179–196.
[23] P. Meijer, M. van der Vlugt, The evaluation of Gauss sums for characters of 2-power order, J. Number Theory 100 (2003) 381–395.
[24] M.E. Muzychuk, On skew Hadamard difference sets, arXiv:1012.2089.
[25] R.E.A.C. Paley, On orthogonal matrices, J. Math. Phys. 12 (1933) 311–320.
[26] T. Storer, Cyclotomy and Difference Sets, Markham, Chicago, 1967.
[27] G.B. Weng, L. Hu, Some results on skew Hadamard difference sets, Des. Codes Cryptogr. 50 (2009) 93–105.
[28] G.B. Weng, W.S. Qiu, Z. Wang, Q. Xiang, Pseudo-Paley graphs and skew Hadamard difference sets from presemifields, Des. Codes Cryptogr. 44 (2007) 49–62.
[29] Q. Xiang, Recent progress in algebraic design theory, Finite Fields Appl. (Ten Year Anniversary Edition) 11 (2005) 622–653.
[30] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, Sci. China Ser. A 53 (2010) 2525–2542.
[31] J. Yang, L. Xia, A note on the sign (unit root) ambiguities of Gauss sums in index 2 and 4 case, arXiv:0912.1414v1.