

Inequivalence of skew Hadamard difference sets and triple intersection numbers modulo a prime

Koji Momihara*

Faculty of Education
Kumamoto University
2-40-1 Kurokami, Kumamoto 860-8555, Japan.

momihara@educ.kumamoto-u.ac.jp

Submitted: Sep 28, 2013; Accepted: Dec 10, 2013; Published: Dec 17, 2013

Mathematics Subject Classifications: 05B10, 05E30

Abstract

Recently, Feng and Xiang [10] found a new construction of skew Hadamard difference sets in elementary abelian groups. In this paper, we introduce a new invariant for equivalence of skew Hadamard difference sets, namely triple intersection numbers modulo a prime, and discuss inequivalence between Feng-Xiang skew Hadamard difference sets and the Paley difference sets. As a consequence, we show that their construction produces infinitely many skew Hadamard difference sets inequivalent to the Paley difference sets.

Keywords: skew Hadamard difference set, Feng-Xiang difference set, Paley difference set

1 Introduction

Let $(G, +)$ be an (additively written) finite group of order v . A k -subset $D \subseteq G$ is called a (v, k, λ) *difference set* if the list of differences $x - y$ with $x, y \in D$ and $x \neq y$ covers each nonzero element of G exactly λ times. We say that two difference sets D_1 and D_2 with the same parameters in an abelian group G are *equivalent* if there exists an automorphism $\sigma \in \text{Aut}(G)$ and an element $x \in G$ such that $\sigma(D_1) + x = D_2$. For general theory on difference sets, we refer the reader to [1].

*Supported by JSPS under Grant-in-Aid for Young Scientists (B) 25800093 and Scientific Research (C) 24540013.

A difference set D in a finite group G is called *skew Hadamard* if G is the disjoint union of D , $-D$, and $\{0\}$. 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. This situation changed dramatically in recent years. Skew Hadamard difference sets are currently under intensive study; see [3, 6, 7, 8, 9, 11, 10, 14, 15, 16, 17] for recent results and the introduction of [10] for a short survey of skew Hadamard difference sets and related problems.

There were two major conjectures in this area: (i) If an abelian group G contains a skew Hadamard difference set, then G is necessarily elementary abelian. (ii) Up to equivalence the Paley difference sets mentioned above are the only skew Hadamard difference sets in abelian groups. The former conjecture is still open in general. The latter conjecture turned out to be false: Ding and Yuan [7] constructed a family of skew Hadamard difference sets in $(\mathbb{F}_{3^m}, +)$, where $m \geq 3$ is odd, by using Dickson polynomials of order 5 and showed that two examples in the family are inequivalent to the Paley difference sets. Very recently, Ding, Pott, and Wang [6] found more skew Hadamard difference sets inequivalent to the Paley difference sets from Dickson polynomials of order 7. Muzychuk [15] gave a prolific construction of skew Hadamard difference sets in an elementary abelian group of order q^3 and showed that his skew Hadamard difference sets are inequivalent to the Paley difference sets. Although many other constructions have been known recently, as far as the author knows, there has been no theoretical result on the inequivalence problem of skew Hadamard difference sets except for [15]. Indeed, in most of recent papers, the inequivalence of skew Hadamard difference sets were checked by computer. Here, we should remark that some of known invariants for equivalence of ordinary difference sets (e.g., p -ranks of the symmetric designs developed from difference sets) do not contribute anything to the inequivalence problem of skew Hadamard difference sets D since they are determined from only the parameters of D [1, Chapter VI, Theorem 8.22]. On the other hand, some invariants (e.g., triple intersection numbers) are difficult to compute without computer.

A classical method for constructing difference sets in the additive groups of finite fields is to use cyclotomic classes of finite fields. Let p be a prime, f a positive integer, and let $q = p^f$. Let $k > 1$ be an integer such that $N|(q-1)$, and γ be a primitive element of \mathbb{F}_q . Then the cosets $C_i^{(N,q)} = \gamma^i \langle \gamma^N \rangle$, $0 \leq i \leq N-1$, are called the *cyclotomic classes of order N* of \mathbb{F}_q .

In this paper, we are particularly interested in the following construction of skew Hadamard difference sets given by Feng and Xiang [10].

Theorem 1. ([10, Theorem 3.2]) *Let $p_1 \equiv 7 \pmod{8}$ be a prime, $N = 2p_1^m$, and let $p \equiv 3 \pmod{4}$ be a prime such that $f := \text{ord}_N(p) = \phi(N)/2$. Let s be any odd integer, I any subset of $\mathbb{Z}/N\mathbb{Z}$ such that $\{i \pmod{p_1^m} \mid i \in I\} = \mathbb{Z}/p_1^m\mathbb{Z}$, and let $D = \bigcup_{i \in I} C_i^{(N,q)}$, where $q = p^{fs}$. Then, D is a skew Hadamard difference set.*

We call the difference set in Theorem 1 as the *Feng-Xiang skew Hadamard difference set* with index set I . Let t be an odd integer and γ be a primitive element of \mathbb{F}_{q^t} . Put

$\omega = \gamma^{(q^t-1)/(q-1)}$. If $D = \bigcup_{i \in I} C_i^{(N,q)} = \bigcup_{i \in I} \omega^i \langle \omega^N \rangle$ is a Feng-Xiang skew Hadamard difference set, then so does $D' = \bigcup_{i \in I} C_i^{(N,q^t)} = \bigcup_{i \in I} \gamma^i \langle \gamma^N \rangle$. We call D' the *lift* of D to \mathbb{F}_{q^t} . Furthermore, throughout this paper, we denote the set $\bigcup_{i \in I} \omega^{ti} \langle \omega^N \rangle$ by $D^{(t)}$. It is clear that $D^{(t)}$ is also a Feng-Xiang skew Hadamard difference set if $\gcd(t, N) = 1$.

In this paper, we introduce a new invariant for equivalence of skew Hadamard difference sets, namely triple intersection numbers modulo a prime, and show that infinitely many Feng-Xiang skew Hadamard difference sets are inequivalent to the Paley difference sets by using “recursive” techniques. Besides the existence of infinitely many skew Hadamard difference sets inequivalent to the Paley difference sets, our technique may contribute to inequivalence problems on combinatorial objects defined in finite fields not only on skew Hadamard difference sets.

This paper is organized as follows. In Section 2, we introduce some preliminaries on characters of finite fields, and present a proposition on divisibility of a character sum over a finite field by its characteristic. In Section 3, we introduce the concept of “triple intersection numbers modulo a prime” and we give two sufficient conditions for lifts of Feng-Xiang skew Hadamard difference sets being inequivalent to the Paley difference sets. As an example, we show that there are infinitely many integers t such that the lifts of a Feng-Xiang skew Hadamard difference set in \mathbb{F}_{11^3} to $\mathbb{F}_{11^{3t}}$ are inequivalent to the Paley difference sets. In Section 4, we conclude this paper with further examples of skew Hadamard difference sets inequivalent to the Paley difference sets, and some open problems.

2 Preliminaries on characters

Let p be a prime, f a positive integer, and $q = p^f$. The canonical additive character ψ of \mathbb{F}_q is defined by

$$\psi: \mathbb{F}_q \rightarrow \mathbb{C}^*, \quad \psi(x) = \zeta_p^{\text{Tr}_{q/p}(x)},$$

where $\zeta_p = \exp(\frac{2\pi i}{p})$ and $\text{Tr}_{q/p}$ is the trace from \mathbb{F}_q to \mathbb{F}_p . For a multiplicative character χ_N of order N of \mathbb{F}_q , we define the *Gauss sum*

$$G_q(\chi_N) = \sum_{x \in \mathbb{F}_q^*} \chi_N(x) \psi(x),$$

which belongs to the ring $\mathbb{Z}[\zeta_{pN}]$ of integers in the cyclotomic field $\mathbb{Q}(\zeta_{pN})$. Let $\sigma_{a,b}$ be the automorphism of $\mathbb{Q}(\zeta_{pN})$ determined by

$$\sigma_{a,b}(\zeta_N) = \zeta_N^a, \quad \sigma_{a,b}(\zeta_p) = \zeta_p^b$$

for $\gcd(a, N) = \gcd(b, p) = 1$. Below are several basic properties of Gauss sums [4]:

- (i) $G_q(\chi_N) \overline{G_q(\chi_N)} = q$ if χ is nontrivial;
- (ii) $G_q(\chi_N^p) = G_q(\chi_N)$, where p is the characteristic of \mathbb{F}_q ;

- (iii) $G_q(\chi_N^{-1}) = \chi_N(-1)\overline{G_q(\chi_N)}$;
- (iv) $G_q(\chi_N) = -1$ if χ_N is trivial;
- (v) $\sigma_{a,b}(G_q(\chi_N)) = \chi_N^{-a}(b)G_q(\chi_N^a)$.

In general, the explicit evaluation of Gauss sums is a very difficult problem. There are only a few cases where the Gauss sums have been evaluated. The most well known case is *quadratic* case, i.e., the case where $N = 2$. In this case, it holds that

$$G_f(\chi_N) = (-1)^{f-1} \left(\sqrt{(-1)^{\frac{p-1}{2}} p} \right)^f, \quad (1)$$

cf. [4, Theorem 11.5.4]. The next simple case is the so-called *semi-primitive case* (also referred to as *uniform cyclotomy* or *pure Gauss sum*), where there exists an integer j such that $p^j \equiv -1 \pmod{N}$, where N is the order of the multiplicative character involved. The explicit evaluation of Gauss sums in this case is given in [4]. The next interesting case is the *index 2* case, where the subgroup $\langle p \rangle$ generated by $p \in (\mathbb{Z}/N\mathbb{Z})^*$ is of index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$ and $-1 \notin \langle p \rangle$. A complete solution to the problem of evaluating index 2 Gauss sums was recently given in [18]. The following is the result on evaluation of index 2 Gauss sums, which was used to prove Theorem 1.

Theorem 2. ([18], Case D; Theorem 4.12) *Let $N = 2p_1^m$, where $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod{4}$ and m is a positive integer. Assume that p is a prime such that $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = 2$. Let $f = \phi(N)/2$, $q = p^f$, and χ be a multiplicative character of order N of \mathbb{F}_q . Then, for $0 \leq t \leq m - 1$, we have*

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

where $p^* = (-1)^{\frac{p-1}{2}} p$, h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, and b and c are integers determined by $4p^h = b^2 + p_1 c^2$ and $bp^{\frac{f-h}{2}} \equiv -2 \pmod{p_1}$.

The following theorem, called the *Davenport-Hasse lifting formula*, is useful for evaluating Gauss sums.

Theorem 3. ([12, Theorem 5.14]) *Let χ be a nontrivial multiplicative character of $\mathbb{F}_q = \mathbb{F}_{p^f}$ and let χ' be the lifted character of χ to the extension field $\mathbb{F}_{q'} = \mathbb{F}_{p^{fs}}$, i.e., $\chi'(\alpha) := \chi(\text{Norm}_{\mathbb{F}_{q'}/\mathbb{F}_q}(\alpha))$ for any $\alpha \in \mathbb{F}_{q'}^*$. It holds that*

$$G_{q'}(\chi') = (-1)^{s-1} (G_q(\chi))^s.$$

In relation to Gauss sums, we need to define the Jacobi sums. Let χ and χ' be multiplicative characters of \mathbb{F}_q . We define the sum

$$J(\chi, \chi') = \sum_{x \in \mathbb{F}_q, x \neq 0, 1} \chi(x)\chi'(1-x),$$

the so-called *Jacobi sum* of \mathbb{F}_q . It is known [12, Theorem 5.21] that if χ , χ' , and $\chi\chi'$ are nontrivial, it holds that

$$J(\chi, \chi') = \frac{G_q(\chi)G_q(\chi')}{G_q(\chi\chi')}. \quad (2)$$

We will use this formula later.

Now we are interested in computing the following character sum modulo the characteristic p :

$$\sum_{x \in \mathbb{F}_{p^f}} \chi(x^{i_1}(x+1)^{i_2}(x+a)^{i_3}) \pmod{p},$$

where χ is a multiplicative character of \mathbb{F}_{p^f} . The following theorem is well known as the *Weil theorem on multiplicative character sums*.

Theorem 4. ([12, Theorems 5.39 and 5.41]) *Let χ be a multiplicative character of \mathbb{F}_q of order $N > 1$ and $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that is not an N th power of a polynomial. Let d be the number of distinct roots of f in its splitting field over \mathbb{F}_q and suppose that $d \geq 2$. Then there exist complex numbers w_1, \dots, w_{d-1} , only depending on f and χ , such that for any positive integer t we have*

$$\sum_{x \in \mathbb{F}_{q^t}} \chi'(f(x)) = -w_1^t - \dots - w_{d-1}^t, \quad (3)$$

where χ' is the lift of χ to \mathbb{F}_{q^t} . In particular, it holds that

$$\left| \sum_{x \in \mathbb{F}_{q^t}} \chi'(f(x)) \right| \leq (d-1)\sqrt{q^t}. \quad (4)$$

With the notations above, we set $d = 3$. By Warning's formula [12, Theorem 1.76], $w_1^t + w_2^t$ can be expressed as follows:

$$w_1^t + w_2^t = \sum_{j=0}^{\lfloor t/2 \rfloor} (-1)^j \frac{t}{t-j} \binom{t-j}{j} (w_1 + w_2)^{t-2j} (w_1 w_2)^j, \quad (5)$$

where each coefficient of $(w_1 + w_2)^{t-2j} (w_1 w_2)^j$ takes an integral value. We assume that $f(x)$ can be decomposed as $f(x) = (x-a)^{i_1}(x-b)^{i_2}(x-c)^{i_3} \in \mathbb{F}_q[x]$ for distinct $a, b, c \in \mathbb{F}_q$ and $i_1, i_2, i_3 \not\equiv 0 \pmod{N}$. As found in the proof of Theorem 5.39 (also Eqs. (5.19) and (5.23)) in [12], we have

$$w_1 w_2 = \sum_{g \in \Phi_2} \lambda(g), \quad (6)$$

where Φ_2 is the set of all monic polynomials of degree 2 over \mathbb{F}_q and λ is defined by $\lambda(g) = \chi^{i_1}(g(a))\chi^{i_2}(g(b))\chi^{i_3}(g(c))$ for $g(x) \in \Phi_2$. Note that if t is an odd prime, by Eq. (5) we obviously have

$$w_1^t + w_2^t \equiv (w_1 + w_2)^t \pmod{t}$$

since $w_1 + w_2, w_1w_2 \in \mathbb{Z}[\zeta_N]$.

We will use the following proposition in the next section.

Proposition 5. *Let χ be a multiplicative character of \mathbb{F}_q of order $N > 1$ and $f(x) = x^{i_1}(x+1)^{i_2}(x+a)^{i_3} \in \mathbb{F}_q[x]$ for $a \in \mathbb{F}_q^* \setminus \{1\}$ and $i_1, i_2, i_3 \not\equiv 0 \pmod{N}$. Assume that p divides $J(\chi^{i_2}, \chi^{i_3})J(\chi^{i_1}, \chi^{i_2i_3})$ for i_2 and i_3 such that $\chi^{i_2i_3}$ is nontrivial. Then, for any odd integer t it holds that*

$$\sum_{x \in \mathbb{F}_{q^t}} \chi'(f(x)) \equiv \left(\sum_{x \in \mathbb{F}_q} \chi(f(x)) \right)^t \pmod{p},$$

where χ' is the lift of χ to \mathbb{F}_{q^t} .

Proof: By Eq. (3) of Theorem 4 and Eq. (5), it is enough to show that $w_1w_2 \equiv 0 \pmod{p}$. By Eq. (6), we need to compute the sum $\sum_{g \in \Phi_2} \lambda(g)$. By the definition of λ , we have

$$\begin{aligned} \sum_{g \in \Phi_2} \lambda(g) &= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \chi^{i_1}(y)\chi^{i_2}(1-x+y)\chi^{i_3}(a^2-ax+y) \\ &= \sum_{z \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \chi^{i_1}(y)\chi^{i_2}(z)\chi^{i_3}(a^2+y(1-a)-a+az) \\ &= \sum_{z \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q \setminus \{a\}} \chi^{i_1}(y)\chi^{i_2}(z)\chi^{i_3}(a^2+y(1-a)-a)\chi^{i_3}\left(1 + \frac{a}{a^2+y(1-a)-a}z\right) \\ &\quad + \sum_{z \in \mathbb{F}_q} \chi^{i_1}(a)\chi^{i_2}(z)\chi^{i_3}(az). \end{aligned} \tag{7a}$$

It is clear that

$$(7b) = \begin{cases} \chi^{i_1}(a)\chi^{-i_2}(a)(q-1) & \text{if } \chi^{i_2i_3} \text{ is trivial,} \\ 0 & \text{if } \chi^{i_2i_3} \text{ is nontrivial.} \end{cases}$$

Next, we compute the sum (7a). By the definition of Jacobi sums, we have

$$\begin{aligned} (7a) &= J(\chi^{i_2}, \chi^{i_3}) \sum_{y \in \mathbb{F}_q \setminus \{a\}} \chi^{i_1}(y)\chi^{-i_2}\left(\frac{-a}{a^2+y(1-a)-a}\right)\chi^{i_3}(a^2+y(1-a)-a) \\ &= J(\chi^{i_2}, \chi^{i_3})\chi^{-i_2}(-a) \sum_{y \in \mathbb{F}_q \setminus \{a\}} \chi^{i_1}(y)\chi^{i_2i_3}(a^2+y(1-a)-a) \\ &= J(\chi^{i_2}, \chi^{i_3})\chi^{-i_2}(-a)\chi^{i_2i_3}(a^2-a)\chi^{-i_1}\left(\frac{a-1}{a^2-a}\right) \sum_{w \in \mathbb{F}_q \setminus \{-1\}} \chi^{i_1}(-w)\chi^{i_2i_3}(1+w). \end{aligned} \tag{8}$$

If $\chi^{i_2}\chi^{i_3}$ is nontrivial, we have

$$(8) = \chi^{-i_2}(-a)\chi^{i_2i_3}(a^2 - a)\chi^{i_1}(a)J(\chi^{i_2}, \chi^{i_3})J(\chi^{i_1}, \chi^{i_2i_3}).$$

If $\chi^{i_2}\chi^{i_3}$ is trivial, by $J(\chi^{i_2}, \chi^{i_3}) = -\chi^{i_2}(-1)$, we have

$$\begin{aligned} (8) &= \chi^{-i_2}(-a)\chi^{i_1}(a)J(\chi^{i_2}, \chi^{i_3}) \sum_{w \in \mathbb{F}_q \setminus \{-1\}} \chi^{i_1}(-w) \\ &= -\chi^{-i_2}(-a)\chi^{i_1}(a)J(\chi^{i_2}, \chi^{i_3}) = \chi^{-i_2}(a)\chi^{i_1}(a). \end{aligned}$$

By the assumption that $p \mid J(\chi^{i_2}, \chi^{i_3})J(\chi^{i_1}, \chi^{i_2i_3})$ for i_2 and i_3 such that $\chi^{i_2i_3}$ is nontrivial, we finally obtain

$$\begin{aligned} \sum_{g \in \Phi_2} \lambda(g) &= \begin{cases} \chi^{i_1}(a)\chi^{-i_2}(a)q & \text{if } \chi^{i_2i_3} \text{ is trivial,} \\ \chi^{-i_2}(-a)\chi^{i_2i_3}(a^2 - a)\chi^{i_1}(a)J(\chi^{i_2}, \chi^{i_3})J(\chi^{i_1}, \chi^{i_2i_3}) & \text{if } \chi^{i_2i_3} \text{ is nontrivial,} \end{cases} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Then the proof is complete.

Remark 6. Let q and N be defined as in Theorem 1. Assume that i_1, i_2 , and i_3 are odd and $\chi^{i_2i_3}$ is nontrivial. Note that $\chi^{i_1i_2i_3}$ is nontrivial since i_1, i_2 , and i_3 are odd. Then, by Eq. (2), we have

$$J(\chi^{i_2}, \chi^{i_3})J(\chi^{i_1}, \chi^{i_2i_3}) = \frac{G(\chi^{i_2})G(\chi^{i_3})}{G(\chi^{i_2i_3})} \cdot \frac{G(\chi^{i_1})G(\chi^{i_2i_3})}{G(\chi^{i_1i_2i_3})} = \frac{G(\chi^{i_1})G(\chi^{i_2})G(\chi^{i_3})}{G(\chi^{i_1i_2i_3})}.$$

By Theorems 2 and 3, we have

$$J(\chi^{i_2}, \chi^{i_3})J(\chi^{i_1}, \chi^{i_2i_3}) = \left((-1)^{\frac{p-1}{2} \frac{f-1}{2}} p^{\frac{f-1}{2}} \sqrt{p^*} \right)^{2s} \equiv 0 \pmod{p},$$

i.e., the condition of Proposition 5 is satisfied.

3 Triple intersection numbers modulo a prime

Let $D \subseteq \mathbb{F}_q$ be a skew Hadamard difference set and ω a primitive element of \mathbb{F}_q . For $a \in \mathbb{F}_p^* \setminus \{1\}$, let

$$T_{\omega^\ell, a}(D) := |D \cap (D - \omega^\ell) \cap (D - a\omega^\ell)|.$$

The set $\{T_{\omega^\ell, a}(D) \mid 0 \leq \ell \leq q - 2\}$ is an invariant for equivalence of skew Hadamard difference sets. In fact, if D' is a skew Hadamard difference set equivalent to D , namely $\sigma(D) = D' + x$ for $\sigma \in \text{Aut}(\mathbb{F}_q, +)$ and $x \in \mathbb{F}_q$, we have

$$\begin{aligned} &\{T_{\omega^\ell, a}(D) \mid 0 \leq \ell \leq q - 2\} \\ &= \{|\sigma(D \cap (D - \omega^\ell) \cap (D - a\omega^\ell))| : 0 \leq \ell \leq q - 2\} \\ &= \{|\sigma(D) \cap (\sigma(D) - \sigma(\omega^\ell)) \cap (\sigma(D) - a\sigma(\omega^\ell))| : 0 \leq \ell \leq q - 2\} \\ &= \{|D' \cap (D' - \omega^\ell) \cap (D' - a\omega^\ell)| : 0 \leq \ell \leq q - 2\}. \end{aligned}$$

If D is the Paley difference set in \mathbb{F}_q , then $|\{T_{\omega^\ell, a}(D) \mid 0 \leq \ell \leq q - 2\}| \leq 2$ since $T_{1, a}(D) = T_{\omega^{2\ell}, a}(D)$ and $T_{\omega, a}(D) = T_{\omega^{2\ell+1}, a}(D)$ for all $0 \leq \ell \leq (q - 3)/2$. Hence, if a skew Hadamard difference set D' satisfies $|\{T_{\omega^\ell, a}(D') \mid 0 \leq \ell \leq q - 2\}| \geq 3$, then D' is inequivalent to the Paley difference set D .

Let $D = \bigcup_{i \in I} C_i^{(N, q)} \subseteq \mathbb{F}_{pfs} = \mathbb{F}_q$ be a Feng-Xiang skew Hadamard difference set. It is clear that

$$|\{T_{\omega^\ell, a}(D) \mid 0 \leq \ell \leq q - 2\}| = |\{T_{\omega^\ell, a}(D) \mid 0 \leq \ell \leq N - 1\}|.$$

In this section, we compute the size of the set $\{T_{\omega^\ell, a}(D) \pmod{t} \mid 0 \leq \ell \leq N - 1\}$ for a prime t . It is clear that this set is also an invariant for equivalence of skew Hadamard difference sets. Hence, if the set above contains at least three numbers, then D is inequivalent to the Paley difference set.

Let χ_N be the multiplicative character of order N of \mathbb{F}_q such that $\chi_N(\omega) = \zeta_N$ and let η_p be the quadratic character of \mathbb{F}_p . Note that $\chi_N|_{\mathbb{F}_p} = \eta_p$. Since the characteristic function of $D = \bigcup_{i \in I} C_i^{(N, q)}$ is given by

$$f(x) = \frac{1}{N} \sum_{h \in I} \sum_{i=0}^{N-1} \zeta_N^{-ih} \chi_N^i(x),$$

we have

$$\begin{aligned} & N^3 \cdot T_{\omega^\ell, a}(D) \\ &= \sum_{x \in \mathbb{F}_q \setminus \{0, -1, -a\}} \sum_{h_1, h_2, h_3 \in I} \left(\sum_{i_1=0}^{N-1} \zeta_N^{-i_1 h_1} \chi_N^{i_1}(x) \right) \left(\sum_{i_2=0}^{N-1} \zeta_N^{-i_2 h_2} \chi_N^{i_2}(x + \omega^\ell) \right) \left(\sum_{i_3=0}^{N-1} \zeta_N^{-i_3 h_3} \chi_N^{i_3}(x + a\omega^\ell) \right) \\ &= \sum_{x \in \mathbb{F}_q \setminus \{0, -1, -a\}} \sum_{h_1, h_2, h_3 \in I} \sum_{i_1, i_2, i_3=0}^{N-1} \zeta_N^{-i_1 h_1 - i_2 h_2 - i_3 h_3} \chi_N^{i_1}(x) \chi_N^{i_2}(x + \omega^\ell) \chi_N^{i_3}(x + a\omega^\ell). \end{aligned}$$

Write $M = N/2$. By noting that $\sum_{h \in I} \zeta_N^{2h} = 0$, the above is expanded as follows:

$$\begin{aligned} & M \sum_{h_2, h_3 \in I} \sum_{i_2, i_3=0}^{N-1} \zeta_N^{-i_2 h_2 - i_3 h_3 + \ell(i_2 + i_3)} \sum_{x \in \mathbb{F}_q \setminus \{-1, -a\}} \chi_N^{i_2}(x + 1) \chi_N^{i_3}(x + a) \\ & - M \sum_{h_2, h_3 \in I} \sum_{i_2, i_3 \in A} \zeta_N^{-i_2 h_2 - i_3 h_3 + \ell(i_2 + i_3)} \eta_p(a) \\ & + M \sum_{h_1, h_3 \in I} \sum_{i_1, i_3=0}^{N-1} \zeta_N^{-i_1 h_1 - i_3 h_3 + \ell(i_1 + i_3)} \sum_{x \in \mathbb{F}_q \setminus \{0, -a\}} \chi_N^{i_1}(x) \chi_N^{i_3}(x + a) \\ & - M \sum_{h_1, h_3 \in I} \sum_{i_1, i_3 \in A} \zeta_N^{-i_1 h_1 - i_3 h_3 + \ell(i_1 + i_3)} \eta_p(-a + 1) \\ & + M \sum_{h_1, h_2 \in I} \sum_{i_1, i_2=0}^{N-1} \zeta_N^{-i_1 h_1 - i_2 h_2 + \ell(i_1 + i_2)} \sum_{x \in \mathbb{F}_q \setminus \{0, -1\}} \chi_N^{i_1}(x) \chi_N^{i_2}(x + 1) \\ & - M \sum_{h_1, h_2 \in I} \sum_{i_1, i_2 \in A} \zeta_N^{-i_1 h_1 - i_2 h_2 + \ell(i_1 + i_2)} \eta_p(a^2 - a) \\ & - M^2 \sum_{h_1 \in I} \sum_{i_1=0}^{N-1} \zeta_N^{-i_1 h_1 + \ell i_1} \sum_{x \in \mathbb{F}_q \setminus \{0\}} \chi_N^{i_1}(x) + M^2 \sum_{h_1 \in I} \sum_{i_1 \in A} \zeta_N^{-i_1 h_1 + \ell i_1} \left(\eta_p(-1) + \eta_p(-a) \right) \end{aligned}$$

$$\begin{aligned}
& - M^2 \sum_{h_2 \in I} \sum_{i_2=0}^{N-1} \zeta_N^{-i_2 h_2 + \ell i_2} \sum_{x \in \mathbb{F}_q \setminus \{-1\}} \chi_N^{i_2}(x+1) + M^2 \sum_{h_2 \in I} \sum_{i_2 \in A} \zeta_N^{-i_2 h_2 + \ell i_2} (\eta_p(1) + \eta_p(-a+1)) \\
& - M^2 \sum_{h_3 \in I} \sum_{i_3=0}^{N-1} \zeta_N^{-i_3 h_3 + \ell i_3} \sum_{x \in \mathbb{F}_q \setminus \{-a\}} \chi_N^{i_3}(x+a) + M^2 \sum_{h_3 \in I} \sum_{i_3 \in A} \zeta_N^{-i_3 h_3 + \ell i_3} (\eta_p(a) + \eta_p(-1+a)) \\
& + \sum_{h_1, h_2, h_3 \in I} \sum_{i_1, i_2, i_3 \in A} \zeta_N^{-i_1 h_1 - i_2 h_2 - i_3 h_3 + \ell(i_1 + i_2 + i_3)} \sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) + (q-3)M^3,
\end{aligned}$$

where $A = \{2j+1 \mid 0 \leq j \leq (q-3)/2\}$. Then, by $\sum_{x \in \mathbb{F}_q^*} \chi_N(x) = 0$ and

$$|D \cap (D+a)| = \frac{1}{N^2} \sum_{h, h' \in I} \sum_{i, i'=0}^{N-1} \zeta_N^{-ih - i'h'} \sum_{x \in \mathbb{F}_q \setminus \{0, a\}} \chi_N^i(x) \chi_N^{i'}(x-a),$$

the above is also reformulated as

$$\begin{aligned}
& MN^2 (|(D - \omega^\ell) \cap (D - a\omega^\ell)| + |D \cap (D - a\omega^\ell)| + |D \cap (D - \omega^\ell)|) \\
& - M(\eta_p(a) + \eta_p(-a+1) + \eta_p(a^2 - a)) \left(\sum_{h \in I} \sum_{i \in A} \zeta_N^{i(\ell-h)} \right)^2 - 3M^3(q-1) \\
& - M^2 (\eta_p(-1) + \eta_p(-a) + \eta_p(1) + \eta_p(-a+1) + \eta_p(a) + \eta_p(-1+a)) \left(\sum_{h \in I} \sum_{i \in A} \zeta_N^{-ih + \ell i} \right) \\
& + \sum_{h_1, h_2, h_3 \in I} \sum_{i_1, i_2, i_3 \in A} \zeta_N^{-i_1 h_1 - i_2 h_2 - i_3 h_3 + \ell(i_1 + i_2 + i_3)} \sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) + (q-3)M^3.
\end{aligned} \tag{9}$$

Let

$$S_{i_1, i_2, i_3}(\omega^\ell, I) = \sum_{h_1, h_2, h_3 \in I} \zeta_N^{-i_1 h_1 - i_2 h_2 - i_3 h_3 + \ell(i_1 + i_2 + i_3)} \sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a).$$

Recall that D is a skew Hadamard difference set, i.e., $|D \cap (D+x)| = \frac{q-3}{4}$ for all $x \in \mathbb{F}_q^*$. Then, by $\eta_p(-1) = -1$, the sum (9) is reformulated as

$$\begin{aligned}
& \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}(\omega^\ell, I) + (q-3)M^3 + 3MN^2 \frac{q-3}{4} - 3M^3(q-1) \\
& - M(\eta_p(a) + \eta_p(-a+1) + \eta_p(a^2 - a)) \left(\sum_{h \in I} \sum_{i \in A} \zeta_N^{i(\ell-h)} \right)^2.
\end{aligned}$$

Since $I \pmod{p_1^m} = \mathbb{Z}/p_1^m\mathbb{Z}$, there is exactly one $h' \in I$ such that $\ell - h' \equiv 0 \pmod{p_1^m}$. Write $\ell - h' = \epsilon p_1^m$. Then, by noting that $A = \{2j+1 \mid 0 \leq j \leq p_1^m - 1\}$, we have

$$\left(\sum_{h \in I} \sum_{i \in A} \zeta_N^{i(\ell-h)} \right)^2 = \left(\sum_{h \in I} \zeta_N^{\ell-h} \sum_{j=0}^{p_1^m-1} \zeta_{p_1^m}^{j(\ell-h)} \right)^2 = \left(p_1^m \zeta_N^{\epsilon p_1^m} \right)^2 = p_1^{2m}.$$

Thus, we finally have

$$N^3 \cdot T_{\omega^\ell, a}(D) = \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}(\omega^\ell, I) + (q-3)M^3 + 3MN^2 \frac{q-3}{4} - 3M^3(q-1) - M(\eta_p(a) + \eta_p(-a+1) + \eta_p(a^2-a))p_1^{2m}. \quad (10)$$

3.1 Triple intersection numbers modulo a prime extension degree

The following theorem gives a sufficient condition for lifts of Feng-Xiang skew Hadamard difference sets being inequivalent to the Paley difference sets.

Theorem 7. *Let t be an odd prime with $\gcd(t, p_1) = 1$. Let $D = \bigcup_{i \in I} C_i^{(N, q)}$ be a Feng-Xiang skew Hadamard difference set and D' be the lift of D to \mathbb{F}_{q^t} . If the set $\{T_{\omega^\ell, a}(D^{(t^{-1})}) \pmod{t} \mid 0 \leq \ell \leq N-1\}$ contains u distinct numbers, then so does $\{T_{\gamma^\ell, a}(D') \pmod{t} \mid 0 \leq \ell \leq N-1\}$, where ω and γ are primitive elements of \mathbb{F}_q and \mathbb{F}_{q^t} , respectively.*

Proof: Without loss of generality, we can assume that $\omega = \gamma^{(q^t-1)/(q-1)}$. Let χ_N be a multiplicative character of order N of \mathbb{F}_q such that $\chi_N(\omega) = \zeta_N$ and χ'_N be the lift of χ_N to \mathbb{F}_{q^t} . Define

$$S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) = \sum_{h_1, h_2, h_3 \in I} \zeta_N^{-i_1 h_1 - i_2 h_2 - i_3 h_3 + \ell(i_1 + i_2 + i_3)} \sum_{x \in \mathbb{F}_{q^t}} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a).$$

Then, by Eq. (10), we have

$$N^3 \cdot T_{\gamma^\ell, a}(D') = \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) + (q^t-3)M^3 + 3MN^2 \frac{q^t-3}{4} - 3M^3(q^t-1) - M(\eta_p(a) + \eta_p(-a+1) + \eta_p(a^2-a))p_1^{2m}.$$

By Eq. (3) of Theorem 4, there are two complex numbers w_1, w_2 such that

$$\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) = -w_1 - w_2$$

and

$$\sum_{x \in \mathbb{F}_{q^t}} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) = -w_1^t - w_2^t.$$

Since t is an odd prime satisfying $\gcd(t, p_1) = 1$, we have

$$\begin{aligned}
 \sum_{x \in \mathbb{F}_{q^t}} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) &= -w_1^t - w_2^t \\
 &\equiv (-w_1 - w_2)^t \pmod{t} \\
 &\equiv \left(\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \right)^t \pmod{t} \\
 &\equiv \sum_{x \in \mathbb{F}_q} \chi_N^{ti_1}(x) \chi_N^{ti_2}(x+1) \chi_N^{ti_3}(x+a) \pmod{t}
 \end{aligned}$$

Therefore, we obtain

$$\begin{aligned}
 &S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) \\
 &\equiv \sum_{h_1, h_2, h_3 \in I} \zeta_N^{-ti_1(t^{-1}h_1) - ti_2(t^{-1}h_2) - ti_3(t^{-1}h_3) + (\ell \cdot t^{-1})(ti_1 + ti_2 + ti_3)} \\
 &\quad \cdot \sum_{x \in \mathbb{F}_q} \chi_N^{ti_1}(x) \chi_N^{ti_2}(x+1) \chi_N^{ti_3}(x+a) \pmod{t} \\
 &= S_{ti_1, ti_2, ti_3}(\omega^{t^{-1}\ell}, t^{-1}I).
 \end{aligned}$$

Hence, it holds that

$$\begin{aligned}
 &\left\{ \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) \mid 0 \leq \ell \leq N-1 \right\} \\
 &\equiv \left\{ \sum_{i_1, i_2, i_3 \in A} S_{ti_1, ti_2, ti_3}(\omega^{t^{-1}\ell}, t^{-1}I) \mid 0 \leq \ell \leq N-1 \right\} \pmod{t} \\
 &\equiv \left\{ \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}(\omega^\ell, t^{-1}I) \mid 0 \leq \ell \leq N-1 \right\} \pmod{t}. \tag{11}
 \end{aligned}$$

By the assumption that the set $\{T_{\omega^\ell, a}(D^{(t^{-1})}) \pmod{t} \mid 0 \leq \ell \leq N-1\}$ contains u distinct numbers, we have

$$\left| \left\{ \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}(\omega^\ell, t^{-1}I) \pmod{t} \mid 0 \leq \ell \leq N-1 \right\} \right| = u.$$

Then, by Eq. (11), we also have

$$\left| \left\{ \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) \pmod{t} \mid 0 \leq \ell \leq N-1 \right\} \right| = u,$$

i.e., the set $\{T_{\gamma^\ell, a}(D') \pmod{t} \mid 0 \leq \ell \leq N-1\}$ contains u distinct numbers.

Remark 8. (i) Let $D = \bigcup_{i \in I} C_i^{(N,q)}$ be defined as in Theorem 7. Assume that

$$\{T_{\omega^\ell, a}(D^{(t^{-1})}) \mid 0 \leq \ell \leq N-1\}$$

contains $u (\geq 3)$ distinct numbers, say, $a_1 < a_2 < \dots < a_u$. Put

$$v = \min\{a_{j+2} - a_j \mid 1 \leq j \leq u-2\}.$$

Let t be any odd prime satisfying $t > v$ and $\gcd(t, p_1) = 1$ and let D' be the lift of D to \mathbb{F}_{q^t} . Then, we have

$$\left| \{T_{\omega^\ell, a}(D^{(t^{-1})}) \pmod{t} \mid 0 \leq \ell \leq N-1\} \right| \geq 3.$$

Hence, by Theorem 7, we have $|\{T_{\gamma^\ell, a}(D') \pmod{t} \mid 0 \leq \ell \leq N-1\}| \geq 3$. (More roughly, one may take t so as $t > a_u - a_1$.)

(ii) If two Feng-Xiang skew Hadamard difference sets D_1 and D_2 in \mathbb{F}_q satisfy

$$\{T_{\omega^\ell, a}(D_1^{(t^{-1})}) \pmod{t} \mid 0 \leq \ell \leq N-1\} \neq \{T_{\omega^\ell, a}(D_2^{(t^{-1})}) \pmod{t} \mid 0 \leq \ell \leq N-1\},$$

then by the proof of Theorem 7 their lifts D'_1 and D'_2 to \mathbb{F}_{q^t} also satisfy

$$\{T_{\gamma^\ell, a}(D'_1) \pmod{t} \mid 0 \leq \ell \leq N-1\} \neq \{T_{\gamma^\ell, a}(D'_2) \pmod{t} \mid 0 \leq \ell \leq N-1\},$$

i.e., D'_1 and D'_2 are inequivalent.

Corollary 9. Let $D = \bigcup_{i \in I} C_i^{(N,q)}$ be a Feng-Xiang skew Hadamard difference set. Let t be any odd prime greater than $4N^3\sqrt{q}$ and D' be the lift of D to \mathbb{F}_{q^t} . If $\{T_{\omega^\ell, a}(D^{(t^{-1})}) \mid 0 \leq \ell \leq N-1\}$ contains u distinct numbers, then so does $\{T_{\gamma^\ell, a}(D') \pmod{t} \mid 0 \leq \ell \leq N-1\}$, where ω and γ are primitive elements of \mathbb{F}_q and \mathbb{F}_{q^t} , respectively.

Proof: Assume that $\{T_{\omega^\ell, a}(D^{(t^{-1})}) \mid 0 \leq \ell \leq N-1\}$ contains u distinct numbers. By Remark 8 (i), it is enough to show that $a_u - a_1 \leq 4N^3\sqrt{q}$. By Eq. (10), it is clear that

$$a_u - a_1 \leq \frac{2}{N^3} \max \left\{ \left| \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}(\omega^\ell, t^{-1}I) \right| : 0 \leq \ell \leq N-1 \right\}.$$

Now we estimate $|\sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}(\omega^\ell, t^{-1}I)|$. By Eq. (4) of Theorem 4, we have

$$\begin{aligned} & \left| \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}(\omega^\ell, t^{-1}I) \right| \\ & \leq \sum_{i_1, i_2, i_3 \in A} \sum_{h_1, h_2, h_3 \in t^{-1}I} \zeta_N^{-i_1 h_1 - i_2 h_2 - i_3 h_3 + \ell(i_1 + i_2 + i_3)} \left| \sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \right| \\ & \leq |A|^3 |I|^3 \sqrt{q} = 2N^6 \sqrt{q}. \end{aligned}$$

Thus, we obtain

$$a_u - a_1 \leq \frac{2}{N^3} \max \left\{ \left| \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}(\omega^\ell, t^{-1}I) \right| : 0 \leq \ell \leq N - 1 \right\} \leq 4N^3 \sqrt{q}.$$

This completes the proof of the corollary.

Corollary 9 implies that for any sufficiently large prime t the lift of a Feng-Xiang skew Hadamard difference set D in \mathbb{F}_q to \mathbb{F}_{q^t} is inequivalent to the Paley difference set if $|\{T_{\omega^\ell, a}(D^{(t^{-1})}) \mid 0 \leq \ell \leq N - 1\}| \geq 3$.

Example 10. Let $p = 11$, $N = 2p_1 = 14$, $f = 3$, and $I = \langle p \rangle \cup -2\langle p \rangle \cup \{0\} \pmod{N}$. Then, we have $I \pmod{p_1} = \mathbb{Z}/p_1\mathbb{Z}$ and the conditions of Theorem 1 are satisfied. Thus, $D = \bigcup_{i \in I} C_i^{(N, p^f)} = \bigcup_{i \in I} \omega^i \langle \omega^N \rangle$ is a Feng-Xiang skew Hadamard difference set, where ω is a primitive element of \mathbb{F}_{p^f} . Now, we consider the triple intersection numbers $T_{\omega^\ell, a}(D^{(t^{-1})})$, $0 \leq \ell \leq N - 1$, with $a = 3$. By Magma, the author checked that

$$\{T_{\omega^\ell, a}(D^{(t^{-1})}) \mid 0 \leq \ell \leq N - 1\} = \{147, 158, 164, 167, 173, 184\}$$

for any odd $1 \leq t < N$ with $\gcd(t, p_1) = 1$. This implies that $D^{(t^{-1})}$ is inequivalent to the Paley difference set.

It is clear that for any odd prime t with $\gcd(t, p_1) = 1$ it holds that

$$\left| \{T_{\omega^\ell, a}(D^{(t^{-1})}) \pmod{t} \mid 0 \leq \ell \leq N - 1\} \right| \geq 3.$$

Hence, by Theorem 7, the lift D' of D to $\mathbb{F}_{p^f t}$ for any odd prime t with $\gcd(p_1, t) = 1$ satisfies

$$\left| \{T_{\gamma^\ell, a}(D') \pmod{t} \mid 0 \leq \ell \leq N - 1\} \right| \geq 3,$$

where γ is a primitive element of $\mathbb{F}_{p^f t}$. Thus, D' is also inequivalent to the Paley difference set. Furthermore, by applying Theorem 7 recursively, the lift D'' of D to $\mathbb{F}_{p^f t^h}$ for any $h \geq 1$ is also inequivalent to the Paley difference set. The extension degrees t^h less than 50 covered by Theorem 7 in this case are listed below:

$$t^h = 3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 37, 41, 43, 47, 49.$$

3.2 Triple intersection numbers modulo the characteristic p

The extension degree t in Theorem 7 is limited to a prime. The following theorem allows us to take t as an arbitrary odd integer.

Theorem 11. Let t be any odd positive integer and consider the p -adic expansion $t = \sum_{h=0}^r x_h p^h$ with $0 \leq x_h \leq p - 1$. Write $e(t) = \sum_{h=0}^r x_h$ and then there is an odd integer t' such that $t' = e(e(\cdots e(t) \cdots))$ and $1 \leq t' \leq p - 2$. Let $D = \bigcup_{i \in I} C_i^{(N, q)}$ be a Feng-Xiang

skew Hadamard difference set and let D' and D'' be its lifts to \mathbb{F}_{q^t} and $\mathbb{F}_{q^{t'}}$, respectively. If the set $\{T_{\beta^\ell, a}(D'') \pmod{p} \mid 0 \leq \ell \leq N-1\}$ contains u distinct numbers, then so does $\{T_{\gamma^\ell, a}(D') \pmod{p} \mid 0 \leq \ell \leq N-1\}$, where β and γ are primitive elements of $\mathbb{F}_{q^{t'}}$ and \mathbb{F}_{q^t} , respectively.

Proof: Let ω be a primitive element of \mathbb{F}_q . Without loss of generality, we can assume that $\omega = \beta^{(q^{t'}-1)/(q-1)} = \gamma^{(q^t-1)/(q-1)}$. Let χ_N be a multiplicative character of order N of \mathbb{F}_q such that $\chi_N(\omega) = \zeta_N$ and let χ'_N and χ''_N be the lifts of χ_N to \mathbb{F}_{q^t} and $\mathbb{F}_{q^{t'}}$, respectively. Define

$$S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) = \sum_{h_1, h_2, h_3 \in I} \zeta_N^{-i_1 h_1 - i_2 h_2 - i_3 h_3 + \ell(i_1 + i_2 + i_3)} \sum_{x \in \mathbb{F}_{q^t}} \chi'^{i_1}_N(x) \chi'^{i_2}_N(x+1) \chi'^{i_3}_N(x+a).$$

Then, by Eq. (10), we have

$$\begin{aligned} N^3 \cdot T_{\gamma^\ell, a}(D') &= \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) + (q^t - 3)M^3 + 3MN^2 \frac{q^t - 3}{4} - 3M^3(q^t - 1) \\ &\quad - M(\eta_p(a) + \eta_p(-a+1) + \eta_p(a^2 - a))p_1^{2m}. \end{aligned}$$

By Eq. (3) of Theorem 4, there are two complex numbers w_1, w_2 such that

$$\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) = -w_1 - w_2,$$

$$\sum_{x \in \mathbb{F}_{q^t}} \chi'^{i_1}_N(x) \chi'^{i_2}_N(x+1) \chi'^{i_3}_N(x+a) = -w_1^t - w_2^t,$$

and

$$\sum_{x \in \mathbb{F}_{q^{t'}}} \chi''^{i_1}_N(x) \chi''^{i_2}_N(x+1) \chi''^{i_3}_N(x+a) = -w_1^{t'} - w_2^{t'}.$$

By Proposition 5, we have

$$\begin{aligned} \sum_{x \in \mathbb{F}_{q^t}} \chi'^{i_1}_N(x) \chi'^{i_2}_N(x+1) \chi'^{i_3}_N(x+a) &\equiv \left(\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \right)^t \pmod{p} \\ &= \prod_{h=0}^{r-1} \left(\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \right)^{x_h p^h} \\ &\equiv \prod_{h=0}^{r-1} \left(\sum_{x \in \mathbb{F}_q} \chi_N^{p^h i_1}(x) \chi_N^{p^h i_2}(x+1) \chi_N^{p^h i_3}(x+a) \right)^{x_h} \pmod{p} \\ &= \prod_{h=0}^{r-1} \left(\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x^{p^h}) \chi_N^{i_2}(x^{p^h} + 1) \chi_N^{i_3}(x^{p^h} + a) \right)^{x_h} \end{aligned}$$

$$\begin{aligned}
&= \prod_{h=0}^r \left(\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \right)^{x_h} \\
&= \left(\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \right)^{e(t)}.
\end{aligned}$$

By repeating this computation, we have

$$\begin{aligned}
\sum_{x \in \mathbb{F}_{q^t}} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) &\equiv \left(\sum_{x \in \mathbb{F}_q} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \right)^{t'} \pmod{p} \\
&\equiv \sum_{x \in \mathbb{F}_{q^{t'}}} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \pmod{p}.
\end{aligned}$$

Therefore, we obtain

$$\begin{aligned}
&S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) \\
&= \sum_{h_1, h_2, h_3 \in I} \zeta_N^{-i_1 h_1 - i_2 h_2 - i_3 h_3 + \ell(i_1 + i_2 + i_3)} \sum_{x \in \mathbb{F}_{q^t}} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \\
&\equiv \sum_{h_1, h_2, h_3 \in I} \zeta_N^{-i_1 h_1 - i_2 h_2 - i_3 h_3 + \ell(i_1 + i_2 + i_3)} \sum_{x \in \mathbb{F}_{q^{t'}}} \chi_N^{i_1}(x) \chi_N^{i_2}(x+1) \chi_N^{i_3}(x+a) \pmod{p} \\
&= S_{i_1, i_2, i_3}^{(t')}(\beta^\ell, I)
\end{aligned}$$

and

$$\begin{aligned}
&\left\{ \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) \mid 0 \leq \ell \leq N-1 \right\} \\
&\equiv \left\{ \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}^{(t')}(\beta^\ell, I) \mid 0 \leq \ell \leq N-1 \right\} \pmod{p}. \tag{12}
\end{aligned}$$

By the assumption that the set $\{T_{\beta^\ell, a}(D'') \pmod{p} \mid 0 \leq \ell \leq N-1\}$ contains u distinct numbers, we have

$$\left| \left\{ \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}^{(t')}(\beta^\ell, I) \pmod{p} \mid 0 \leq \ell \leq N-1 \right\} \right| = u.$$

Then, by Eq. (12), we also have

$$\left| \left\{ \sum_{i_1, i_2, i_3 \in A} S_{i_1, i_2, i_3}^{(t)}(\gamma^\ell, I) \pmod{p} \mid 0 \leq \ell \leq N-1 \right\} \right| = u,$$

i.e., the set $\{T_{\gamma^\ell, a}(D') \pmod{t} \mid 0 \leq \ell \leq N-1\}$ contains u distinct numbers.

Theorem 11 implies that for any odd integer t the lift D' of a Feng-Xiang skew Hadamard difference set D in \mathbb{F}_q to \mathbb{F}_{q^t} is inequivalent to the Paley difference set if the lift D'' of D to $\mathbb{F}_{q^{t'}}$ satisfies $|\{T_{\beta^\ell, a}(D'') \pmod{p} \mid 0 \leq \ell \leq N-1\}| \geq 3$ for every odd $1 \leq t' \leq p-2$.

Example 12. Let p, N, f, a , and I be defined as in Example 10. Then $D = \bigcup_{i \in I} C_i^{(N, q)}$ satisfies

$$\{T_{\omega^\ell, a}(D) \mid 0 \leq \ell \leq N-1\} = \{147, 158, 164, 167, 173, 184\}.$$

It is clear that

$$\left| \{T_{\omega^\ell, a}(D) \pmod{p} \mid 0 \leq \ell \leq N-1\} \right| \geq 3.$$

Hence, by Theorem 11, the lift D' of D to $\mathbb{F}_{p^{ft}}$ for any odd t with $e(e(\cdots e(t)\cdots)) = 1$ satisfies

$$\left| \{T_{\gamma^\ell, a}(D') \pmod{p} \mid 0 \leq \ell \leq N-1\} \right| \geq 3,$$

where γ is a primitive element of $\mathbb{F}_{p^{ft}}$. Thus, D' is inequivalent to the Paley difference set. The extension degrees $t > 1$ less than 50 covered by Theorem 11 in this case are $t = 11, 21, 31$, and 41. Note that $t = 21$ is not covered by Theorem 7.

4 Concluding remarks

In this paper, we obtained two theorems which give sufficient conditions for lifts of Feng-Xiang skew Hadamard difference sets being inequivalent to the Paley difference sets. As an example, we showed that there are infinitely many integers t such that the lifts of the Feng-Xiang difference set $D = \bigcup_{i \in \langle 11 \rangle \cup -2\langle 11 \rangle \cup \{0\}} C_i^{(14, 11^3)}$ to $\mathbb{F}_{11^{3t}}$ are inequivalent to the Paley difference sets. Further small examples are listed in Table 1. (In the table, let ω be a primitive element of \mathbb{F}_{p^f} , $n_t := |\{T_{\omega^\ell, 3}(D^{(t-1)}) \pmod{t} \mid 0 \leq \ell \leq N-1\}|$, and t be prime to N .) In these examples, we fixed parameters as $N = 14$ and $f = 3$ due to the memory-capacity of computer. For each $p \in \{11, 23, 67, 79, 107\}$, the Feng-Xiang skew Hadamard difference sets $D = \bigcup_{i \in I} C_i^{(N, p^f)}$ for I listed in the table and their lifts to $\mathbb{F}_{p^{ft}}$ for sufficiently large odd primes t are inequivalent to the Paley difference sets. Moreover, the lifts are mutually inequivalent by Remark 8 (ii).

Our main theorems works well for Feng-Xiang skew Hadamard difference sets since the difference sets have the nice property that their lifts are again skew Hadamard difference sets. Here, we have the following natural question: are there skew Hadamard difference sets with the “lifting” property other than Paley difference sets and Feng-Xiang skew Hadamard difference sets? Below, we give an immediate generalization of Feng-Xiang skew Hadamard difference sets.

Theorem 13. Let p_1 be a prime, $N = 2p_1^m$, and let $p \equiv 3 \pmod{4}$ be a prime such that $2 \in \langle p \rangle \pmod{p_1^m}$, $\gcd(p_1, p-1) = 1$, and $f := \text{ord}_N(p)$ is odd. Let s be any odd integer, I any subset of $\mathbb{Z}/N\mathbb{Z}$ such that $\{i \pmod{p_1^m} \mid i \in I\} = \mathbb{Z}/p_1^m\mathbb{Z}$, and let $D = \bigcup_{i \in I} C_i^{(N, q)}$, where $q = p^{fs}$. Then, D is a skew Hadamard difference set.

Table 1: Examples of Feng-Xiang skew Hadamard difference sets and their triple intersection numbers

(p, f, N)	index set I	$\{T_{\omega^\ell, 3}(D^{(t^{-1})}) \mid 0 \leq \ell \leq N-1\}$	n_t for odd primes t
(11, 3, 14)	$\{0, 1, 2, 3, 4, 5, 6\}$	$\{159, 162, 164, 167, 169, 172\}$	$n_5 = 2$ and $n_t \geq 3$ for any other t
	$\{0, 1, 2, 3, 4, 6, 12\}$	$\{157, 160, 165, 166, 171, 174\}$	$n_3 = 2$ and $n_t \geq 3$ for any other t
	$\{0, 1, 6, 9, 10, 11, 12\}$	$\{147, 158, 164, 167, 173, 184\}$	$n_t \geq 3$ for any t
	$\{0, 1, 2, 4, 6, 10, 12\}$	$\{163, 164, 167, 168\}$	$n_t \geq 3$ for any $t \geq 3$
(11, 3, 2)	$\{0\}$ (Paley)	$\{157, 174\}$	$n_{17} = 1$ and $n_t = 2$ for any other t
(23, 3, 14)	$\{0, 1, 2, 3, 4, 5, 6\}$	$\{1497, 1498, 1503, 1515, 1525, 1537, 1542, 1543\}$	$n_3 = 2$ and $n_t \geq 3$ for any other t
	$\{0, 1, 2, 3, 4, 6, 12\}$	$\{1498, 1503, 1508, 1514, 1526, 1532, 1537, 1542\}$	$n_t \geq 3$ for any t
	$\{0, 1, 6, 9, 10, 11, 12\}$	$\{1481, 1509, 1514, 1526, 1531, 1559\}$	$n_5 = 2$ and $n_t \geq 3$ for any other t
	$\{0, 1, 2, 4, 6, 10, 12\}$	$\{1508, 1514, 1526, 1532\}$	$n_3 = 1$ and $n_t \geq 3$ for any t
(23, 3, 2)	$\{0\}$ (Paley)	$\{1520\}$	$n_t = 1$ for any t
(67, 3, 14)	$\{0, 1, 2, 3, 4, 5, 6\}$	$\{37457, 37519, 37525, 37587, 37602, 37664, 37670, 37732\}$	$n_t \geq 3$ for any t
	$\{0, 1, 2, 3, 4, 6, 12\}$	$\{37453, 37523, 37587, 37591, 37598, 37602, 37666, 37736\}$	$n_t \geq 3$ for any t
	$\{0, 1, 6, 9, 10, 11, 12\}$	$\{37526, 37587, 37594, 37595, 37602, 37663\}$	$n_t \geq 3$ for any t
	$\{0, 1, 2, 4, 6, 10, 12\}$	$\{37543, 37559, 37630, 37646\}$	$n_3, n_{29} = 2$ and $n_t \geq 3$ for any other t
(67, 3, 2)	$\{0\}$ (Paley)	$\{37502, 37687\}$	$n_t = 2$ for any t
(79, 3, 14)	$\{0, 1, 2, 3, 4, 5, 6\}$	$\{61470, 61575, 61607, 61623, 61636, 61652, 61684, 61789\}$	$n_t \geq 3$ for any t
	$\{0, 1, 2, 3, 4, 6, 12\}$	$\{61398, 61535, 61549, 61552, 61707, 61710, 61724, 61861\}$	$n_t \geq 3$ for any t
	$\{0, 1, 6, 9, 10, 11, 12\}$	$\{61513, 61533, 61546, 61713, 61726, 61746\}$	$n_3, n_5 = 2$ and $n_t \geq 3$ for any other t
	$\{0, 1, 2, 4, 6, 10, 12\}$	$\{61434, 61511, 61748, 61825\}$	$n_7, n_{11}, n_{157} = 2$ $n_t \geq 3$ for any other t
(79, 3, 2)	$\{0\}$ (Paley)	$\{61519, 61740\}$	$n_t = 2$ for any t
(107, 3, 14)	$\{0, 1, 2, 3, 4, 5, 6\}$	$\{152751, 152895, 152976, 153021, 153238, 153283, 153364, 153508\}$	$n_3 = 2$ and $n_t \geq 3$ for any other t
	$\{0, 1, 2, 3, 4, 6, 12\}$	$\{152969, 153065, 153092, 153167, 153194, 153290\}$	$n_3 = 1$ and $n_t \geq 3$ for any other t
	$\{0, 1, 6, 9, 10, 11, 12\}$	$\{152643, 153040, 153102, 153157, 153219, 153616\}$	$n_3 = 2$ and $n_t \geq 3$ for any other t
	$\{0, 1, 2, 4, 6, 10, 12\}$	$\{153028, 153103, 153156, 153231\}$	$n_3, n_5 = 2$ and $n_t \geq 3$ for any other t
(107, 3, 2)	$\{0\}$ (Paley)	$\{152977, 153282\}$	$n_t = 2$ for any t

The above theorem follows immediately from [4, Theorem 11.3.5] and the proof of [10, Theorem 3.2]. This can be seen as follows. By Theorem 11.3.5 (the Davenport-Hasse product formula on Gauss sums) in [4] and the assumption that $2 \in \langle p \rangle \pmod{p_1^m}$, we have

$$G_f(\chi_N) = \frac{G_f(\chi_{p_1^m})G_f(\chi_2)}{\chi_{p_1^m}(2)G_f(\chi_{p_1^{2^{-1}}})} = G_f(\chi_2)\chi_{p_1^m}^{-1}(2).$$

By $\gcd(p_1, p-1) = 1$, the restriction of $\chi_{p_1^m}$ to \mathbb{F}_p is trivial. Hence, we have $G_f(\chi_N) = G_f(\chi_2)$. The remaining proof is same with that of Theorem 3.2 in [10]. For example, the case where $(p, p_1, f) = (47, 127, 21)$ is covered by Theorem 13 but not covered by Theorem 1.

Interesting problems which are worth looking into as future works are listed below.

- (1) We showed that there are infinitely many skew Hadamard difference sets inequivalent

to the Paley difference sets by using “recursive” techniques not saying anything about the inequivalence of “starting” skew Hadamard difference sets theoretically. Determine whether the “starting” skew Hadamard difference sets are inequivalent to the Paley difference sets without using computer.

- (2) Find skew Hadamard difference sets with the lifting property, i.e., their lifts are again skew Hadamard difference sets, other than the Paley difference sets and the difference sets of Theorem 13.
- (3) Recently, several new constructions of skew Hadamard difference sets have been known other than Feng-Xiang skew Hadamard difference sets [2, 6, 7, 8, 13, 16]. Determine whether such skew Hadamard difference sets are inequivalent to the Paley difference sets.

Acknowledgements

The author would like to thank the referees and the editor for their helpful comments.

References

- [1] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Chapter VI, Cambridge University Press, 1999.
- [2] Y. Q. Chen and T. Feng, Paley type group schemes from cyclotomic classes and Arasu-Dillon-Player difference sets, arXiv:1210.2801.
- [3] Y. Q. Chen and J. Polhill, Paley type group schemes and planar Dembowski-Ostrom polynomials, *Discrete Math.*, 311:1349–1364, 2011.
- [4] B. Berndt, R. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.
- [5] P. Ó. Catháin, Inequivalence of difference sets: On a remark of Baumert, *Elec. J. Combinatorics*, 20:#P38, 2013.
- [6] C. Ding, A. Pott and Q. Wang, Skew Hadamard difference sets from Dickson polynomials of order 7, arXiv:1305.1831.
- [7] C. Ding and J. Yuan, A family of skew Hadamard difference sets, *J. Combinatorial Theory, Ser. A*, 113:1526–1535, 2006.
- [8] C. Ding, Z. Wang and Q. Xiang, Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in $\text{PG}(3, 3^{2h+1})$, *J. Combinatorial Theory, Ser. A*, 114:867–887, 2007.
- [9] T. Feng, Non-abelian skew Hadamard difference sets fixed by a prescribed automorphism, *J. Combinatorial Theory, Ser. A*, 118:27–36, 2011.
- [10] T. Feng and Q. Xiang, Cyclotomic constructions of skew Hadamard difference sets, *J. Combinatorial Theory, Ser. A*, 119:245–256, 2012.

- [11] T. Feng, K. Momihara and Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, arXiv:1201.0701.
- [12] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.
- [13] K. Momihara, Cyclotomic strongly regular graphs, skew Hadamard difference sets, and rationality of relative Gauss sums, *Europ. J. Combinatorics.*, 34:706–723 2013.
- [14] K. Momihara, Skew Hadamard difference sets from cyclotomic strongly regular graphs, *SIAM Journal on Discrete Mathematics*, 27:1112–1122, 2013.
- [15] M. E. Muzychuk, On skew Hadamard difference sets, arXiv:1012.2089.
- [16] G. B. Weng and L. Hu, Some results on skew Hadamard difference sets, *Des. Codes Cryptogr.*, 50:93–105, 2009.
- [17] G. B. Weng, W. S. Qiu, Z. Wang and Q. Xiang, Pseudo-Paley graphs and skew Hadamard difference sets from presemifields, *Des. Codes Cryptogr.*, 44:49–62, 2007.
- [18] J. Yang and L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Ser. A*, 53:2525–2542, 2010.