A recursive construction for skew Hadamard difference sets

Koji Momihara*

Division of Natural Science
Faculty of Advanced Science and Technology
Kumamoto University
Kumamoto, Japan

momihara@educ.kumamoto-u.ac.jp

Submitted: Oct 14, 2019; Accepted: Aug 6, 2020; Published: Aug 21, 2020

Abstract

A major conjecture on the existence of abelian skew Hadamard difference sets is: if an abelian group G contains a skew Hadamard difference set, then G must be elementary abelian. This conjecture remains open in general.

In this paper, we give a recursive construction for skew Hadamard difference sets in abelian (not necessarily elementary abelian) groups. The new construction can be considered as a result on the aforementioned conjecture: if there exists a counterexample to the conjecture, then there exist infinitely many counterexamples to it.

Mathematics Subject Classifications: 05B10, 05E30, 11T22

1 Introduction

Let G be an additively written group, let $G^* = G \setminus \{0_G\}$, and let D be a subset of G. We say that D is a *difference set* if the list of differences "$x - y, x, y \in D, x \neq y$" represents every element of G^* exactly λ times. In this paper, we are concerned with difference sets in abelian groups. We say that a difference set is *skew Hadamard* if D is a skew-symmetric $(|G|-1)/2$-subset of G, i.e., $D \cup -D = G^*$ and $D \cap -D = \emptyset$, where $-D = \{-x : x \in D\}$. Two difference sets D_1 and D_2 in an abelian group G are said to be *equivalent* if there is a group automorphism σ of G and an element $b \in G$ such that $\sigma(D_1) = D_2 + b$.

Let D be a skew Hadamard difference set in G, and let $D + x = \{y + x : y \in D\}$ for $x \in G$. It is known that the collection $\mathrm{Dev}(D) = \{D + x : x \in G\}$ forms a symmetric 2-design, called a *Hadamard design*, which gives rise to a skew Hadamard matrix of order $|G|+1$. Thus, the problems on the existence and classification of skew Hadamard difference sets are well-rooted in design theory.

We will use the following well-known property of skew Hadamard difference sets later.

*Supported by JSPS under Grant-in-Aid for Scientific Research (C) 20K03719.

Lemma 1. *Let G be an abelian group of order v. A subset D of G is a skew Hadamard difference set if and only if $\psi(D) \in \{\frac{-1+\sqrt{-v}}{2}, \frac{-1-\sqrt{-v}}{2}\}$ for any nontrivial character ψ of G.*

For a skew Hadamard difference set D, we call $-D$ the *inverse* of D, which is also a skew Hadamard difference set in G. It is clear that $\psi(D) = \frac{-1\pm\sqrt{-v}}{2}$ if and only if $\psi(-D) = \frac{-1\mp\sqrt{-v}}{2}$.

The primary example of skew Hadamard difference sets is the classical *Paley difference set* in the additive group of the finite field $\mathbb{F}_q$ ($q \equiv 3 \pmod 4$), which consists of all nonzero squares of $\mathbb{F}_q$. The automorphism group of the design developed from the Paley difference set was determined by Carlitz [1] and Kantor [10]. The Paley difference set was the only known example in abelian groups for many years. Therefore, many researchers had believed that up to equivalence the Paley difference sets are the only skew Hadamard difference sets in elementary abelian groups. In 2006, Ding and Yuan [5] disproved this conjecture by giving counterexamples of skew Hadamard difference sets in $(\mathbb{F}_{3^5}, +)$ inequivalent to the Paley difference set. This discovery re-energized the research on skew Hadamard difference sets. On the other hand, the following conjecture is also known.

Conjecture 2. If an abelian group contains a skew Hadamard difference set, then the group is necessarily elementary abelian.

This conjecture is still open in general while an exponent bound on groups containing skew Hadamard difference sets was studied in [4]. In this paper, we make some progress on this conjecture.

Many constructions for skew Hadamard difference sets in $(\mathbb{F}_q, +)$ have been known in the past two decades as listed in Table 1. They are classified into three types: (1) Constructions as images of polynomials over $\mathbb{F}_3$; (2) product constructions in $\mathbb{F}_q^3$; (3) constructions based on cyclotomy. In particular, the construction by Muzychuk [14] and its generalization by Chen-Feng [2] are very powerful; indeed their constructions yield many inequivalent skew Hadamard difference sets but the group is limited to $(\mathbb{F}_q^n, +)$ with $n = 3$. For large $n > 3$, Feng-Xiang's skew Hadamard difference sets [8, 13] are the only known class containing infinitely many examples inequivalent to the Paley difference sets. Thus, the problem on whether there exists a skew Hadamard difference set inequivalent to the Paley difference set in $(\mathbb{F}_q, +)$ for every odd prime power $q \equiv 3 \pmod 4$ is still unsolved.

The purpose of this paper is to give a recursive construction for skew Hadamard difference sets in abelian groups. As far as the author knows, no recursive construction was known while "recursive-like" product constructions were known. The construction given by Muzychuk [14] and its generalization by Chen-Feng [2] needs one skew Hadamard difference set in $\mathbb{F}_q$ and one "vertically balanced" Paley type partial difference set in $\mathbb{F}_q^2$ to construct a skew Hadamard difference set in $(\mathbb{F}_q^3, +)$. On the other hand, Chen-Feng's construction [3] needs an "Arasu-Dillon-Player" difference set in $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ to construct a skew Hadamard difference set in $(\mathbb{F}_{q^n}, +)$.

Our construction needs *many* (not necessarily distinct) abelian skew Hadamard difference sets as input, where the exact number of skew Hadamard difference sets needed represents the "flexibility" of the construction. For example, we assume the existence of 25 skew Hadamard difference sets in abelian groups of order q to construct a skew Hadamard difference set in an abelian group of order q^5. Thus, our construction seems to be very flexible. In fact, the construction can give rise to some inequivalent skew

Table 1: Known constructions for skew Hadamard difference sets except for the classical Paley difference sets

Groups	Construction – Tools	Ref
$(\mathbb{F}_3^n,+)$	Polynomial construction	
	– Dickson polynomial of degree 5	[5]
	– Dickson polynomial of degree 7	[7]
	– the Ree-Tits slice symplectic spread	[6]
	– Squares in presemifields	[16]
$(\mathbb{F}_q^3,+)$	Product construction	
	– A skew Hadamard difference set in $(\mathbb{F}_q,+)$ and and a Paley type partial difference set in $(\mathbb{F}_q^2,+)$	[14, 2]
$(\mathbb{F}_q^n,+)$	Cyclotomic construction	
	– Arasu-Dillon-Player difference sets	[3]
	– Cyclotomic strongly regular graphs	[12]
	– Cyclotomy associated with index 2 Gauss sums (There are some restrictions for the group order.)	[8]

Hadamard difference sets when the group order is small. For example, Chen-Feng [3, Table 2] found by computer two inequivalent skew Hadamard difference sets D in $(\mathbb{F}_7^3,+)$ with $\#\mathsf{Aut}(\mathrm{Dev}(D)) = 3^4\cdot 7^3$, where $\mathsf{Aut}(\mathrm{Dev}(D))$ stands for the full automorphism group of the design $\mathrm{Dev}(D)$. On the other hand, no general construction covering these examples have been known. Our construction covers these examples as explained below.

Example 3. Let $H_{i,0}$, $1 \leqslant i \leqslant 6$, be six skew Hadamard difference sets in $(\mathbb{F}_q,+)$, and $H_{i,1}$, $1 \leqslant i \leqslant 6$, be the inverses of $H_{i,0}$, $1 \leqslant i \leqslant 6$, respectively. Furthermore, let D be the union of the following subsets of $\mathbb{F}_q^3$:

$$H_{1,0}\times H_{2,0}\times H_{3,0},\quad H_{1,0}\times H_{2,1}\times H_{3,1},\quad H_{1,1}\times H_{2,1}\times H_{3,0},\quad H_{1,1}\times H_{2,0}\times H_{3,1},$$
$$\{0\}\times\mathbb{F}_q\times H_{4,0},\quad H_{5,0}\times\{0\}\times\mathbb{F}_q,\quad \mathbb{F}_q\times H_{6,0}\times\{0\}.$$

Then, our main theorem implies that D is a skew Hadamard difference set in $(\mathbb{F}_q^3,+)$. In particular, in the case where $q = 7$, the sets D with $H_{1,0} = H_{2,0} = \cdots = H_{6,0} = \{x : x \text{ is a nonzero square in } \mathbb{F}_q\}$ and $H_{1,0} = H_{2,0} = \cdots = H_{6,0} = \{x : x \text{ is a nonsquare in } \mathbb{F}_q\}$ give rise to two inequivalent difference sets in $(\mathbb{F}_q^3,+)$ with $\#\mathsf{Aut}(\mathrm{Dev}(D)) = 3^4\cdot 7^3$. Thus, this construction covers the aforementioned two inequivalent skew Hadamard difference sets in $(\mathbb{F}_7^3,+)$.

In this paper, we give a recursive construction for skew Hadamard difference sets, which is a generalization of the construction in Example 3. We briefly explain the construction. Let $n > 1$ be an odd integer and G_i, $i = 0,1,\ldots,n-1$, be abelian (not necessarily elementary abelian) groups of order q. We assume that each G_i contains some (not necessarily distinct) skew Hadamard difference sets H_i. We construct a skew Hadamard difference set D in $G = G_0\times G_1\times\cdots\times G_{n-1}$ so that D is a union of direct products of either $\{0_{G_i}\}$, G_i, H_i or $-H_i$ for $0 \leqslant i \leqslant n-1$ as in Example 3. We will study how to choose such direct products in relation to an identity for coefficients of the Lucas polynomial and binomial coefficients. The main point of our recursive construction is that the assumed abelian groups containing skew Hadamard difference sets are not necessarily elementary abelian. Hence, if one finds a skew Hadamard difference set in a nonelementary abelian group, by plugging it into the construction, we obtain skew Hadamard difference sets in other nonelementary abelian groups. Therefore, we claim that if there exists a counterexample for Conjecture 2, then there exist infinitely many counterexamples for it.

The paper is organized as follows. In Section 2, we give an identity for coefficients of the Lucas polynomial and binomial coefficients, which is behind our construction. In particular, we need a constructive proof for the identity. In Section 3, we give our main construction for skew Hadamard difference sets based on the identity, and prove that the construction works well. In the final section, we apply our construction for small q's and discuss about the inequivalence of resulting skew Hadamard difference sets.

2 An identity for coefficients of Lucas polynomials and binomial coefficients

In this section, we study a relationship between coefficients of the Lucas polynomial and the binomial coefficients, which will be used to construct skew Hadamard difference sets.

The *Lucas polynomial* $L_n(x) \in \mathbb{Z}[x]$ of degree n is defined by the following recurrence relation:

$$L_n(x) = \begin{cases} 2, & \text{if } n = 0, \\ x, & \text{if } n = 1, \\ L_{n-1}(x)x + L_{n-2}(x), & \text{if } n \geqslant 2. \end{cases}$$

Remark 4. The following facts on Lucas polynomials are classically well-known. See, e.g., [11].

(1) $L_n(x)$ can be explicitly written as

$$L_n(x) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-k} \binom{n-k}{k} x^{n-2k}.$$

(2) Let $b_{n,h}$, $0 \leqslant h \leqslant n$, denote the coefficient of x^h in $L_n(x)$. Then, $b_{n,n-2k}$ is the number of k-subsets without consecutive points of a set of n points on a circle.

The key part of this paper is to give a "constructive" proof for the following identity.

Proposition 5. *For positive integers n and $0 \leqslant k \leqslant n$, it holds that*

$$\binom{n}{k} = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i}{i} b_{n,n-2(k-i)}. \tag{1}$$

Proof. Let $V = \{0, 1, \ldots, n-1\}$ be a set of n points on a circle in the ordering $0 \to 1 \to \ldots \to n-1 \to 0$. Define $\mathcal{S}_{n,k}$ to be the set of k-subsets without neighbors of V. Then, by Remark 4 (2), $|\mathcal{S}_{n,k}| = b_{n,n-2k}$. For any $S \in \mathcal{S}_{n,k}$, let $S^+ = \{x + 1 \,(\mathrm{mod}\ n) : x \in S\}$. Note that $|S \cup T| = k + \ell$ for any $T \in \binom{S^+}{\ell}$ with $0 \leqslant \ell \leqslant k$ since $S \cap S^+ = \varnothing$. Define

$$\mathcal{T}_{n,\ell}(S) = \left\{ S \cup T \,:\, T \in \binom{S^+}{\ell} \right\}, \ 0 \leqslant \ell \leqslant k, \ S \in \mathcal{S}_{n,k}.$$

We now consider the following process to make a k-subset of V: choose $0 \leqslant i \leqslant k$, $S \in \mathcal{S}_{n,k-i}$ and $T \in \binom{S^+}{i}$. Then, we have $(X :=) S \cup T \in \binom{V}{k}$.

Conversely, let X be any k-subset of V, and let $S = S^+ = \varnothing$. For all $A = \{a, a+1, \ldots, a+d\} \subseteq X$ such that $d \geqslant 0$ and $a-1, a+d+1 \notin X$, we add $a, a+2, a+4, \ldots \in A$ into S and add their neighbors $a+1, a+3, a+5, \ldots$ into S^+. In this way, we can determine unique $1 \leqslant i \leqslant k$, $S \in \mathcal{S}_{n,k-i}$ and $T \in \binom{S^+}{i}$ such that $X = S \cup T \in \mathcal{T}_{n,i}(S)$. It is not difficult to see that this is the reverse process of the above. This implies that

$$\binom{V}{k} = \bigcup_{i=0}^{\lfloor \frac{k}{2} \rfloor} \bigcup_{S \in \mathcal{S}_{n,k-i}} \mathcal{T}_{n,i}(S). \tag{2}$$

Then,

$$\begin{aligned}\binom{n}{k} = \left|\binom{V}{k}\right| &= \Big|\bigcup_{i=0}^{\lfloor \frac{k}{2} \rfloor} \bigcup_{S \in \mathcal{S}_{n,k-i}} \mathcal{T}_{n,i}(S)\Big| \\ &= \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \sum_{S \in \mathcal{S}_{n,k-i}} |\mathcal{T}_{n,i}(S)| = \sum_{i=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k-i}{i} b_{n,n-2(k-i)},\end{aligned}$$

which proves the proposition. □

Remark 6. We should mention that the identity in Proposition 5 is a special case of the following more general formula:

$$\binom{tn+r+s}{n} = \sum_k \binom{tk+r}{k}\binom{tn-tk+s}{n-k}\frac{t}{tk+r}, \tag{3}$$

which is given in [9, Eq. (5.62)]. In fact, we obtain (1) by putting n, k, r, s, t in (3) as $k, k-i, n, k, -1$, respectively. This was pointed out by one of the reviewers. However, we could not find our constructive proof in the literature, and we particularly need the structural identity (2) in our construction for skew Hadamard difference sets.

3 Construction of skew Hadamard difference sets

In this section, we use the following notation:

- n: an odd positive integer;
- $G_0, G_1, \ldots, G_{n-1}$: not necessarily distinct abelian groups of order $q \equiv 3 \pmod 4$;
- $G := G_0 \times G_1 \times \cdots \times G_{n-1}$;
- $V := \{0, 1, \ldots, n-1\}$ with the ordering $0 \to 1 \to \cdots \to n-1 \to 0$;
- $R_S := V \setminus (S \cup S^+)$ for $S \in \mathcal{S}_{n,k}$;
- For each $S \in \mathcal{S}_{n,k}$, let $H_{S,i_j,0} \subseteq G_{i_j}$, $1 \leqslant j \leqslant |R_S|$, be skew Hadamard difference sets, where the subscripts i_j are labeled by the elements in R_S.
- $H_{S,i_j,1} \subseteq G_{i_j}$, $1 \leqslant j \leqslant |R_S|$: the inverses of $H_{S,i_j,0}$, $1 \leqslant j \leqslant |R_S|$, respectively;

- For each $S \in \mathcal{S}_{n,k}$, define D_S as a union of all subsets $A_0 \times A_1 \times \cdots \times A_{n-1} \subseteq G$ such that

  1. $A_i = \{0_{G_i}\}$ for all $i \in S$;
  2. $A_i = G_i$ for all $i \in S^+$;
  3. $A_i \in \{H_{S,i,0}, H_{S,i,1}\}$ for $i \in R_S$ so that the number of $i \in R_S$ such that $A_i = H_{S,i,1}$ is even.

Example 7. If $S = \{0, 2\} \in \mathcal{S}_{5,2}$, we have $D_S = \{0_{G_0}\} \times G_1 \times \{0_{G_2}\} \times G_3 \times H_{S,4,0}$. If $S = \{0\} \in \mathcal{S}_{5,1}$, D_S is the union of $\{0_{G_0}\} \times G_1 \times H_{S,2,0} \times H_{S,3,0} \times H_{S,4,0}$, $\{0_{G_0}\} \times G_1 \times H_{S,2,1} \times H_{S,3,1} \times H_{S,4,0}$, $\{0_{G_0}\} \times G_1 \times H_{S,2,0} \times H_{S,3,1} \times H_{S,4,1}$ and $\{0_{G_0}\} \times G_1 \times H_{S,2,1} \times H_{S,3,0} \times H_{S,4,1}$.

The following is our main theorem.

Theorem 8. *Define*

$$D = \bigcup_{k=0}^{\frac{n-1}{2}} \bigcup_{S \in \mathcal{S}_{n,k}} D_S. \tag{4}$$

Then, D forms a skew Hadamard difference set in G.

Remark 9. We need $\sum_{k=0}^{\frac{n-1}{2}} |\mathcal{S}_{n,k}|(n-2k)$ skew Hadamard difference sets in abelian groups of order q to define the set D. Note that by Remark 4 we have

$$\sum_{k=0}^{\frac{n-1}{2}} |\mathcal{S}_{n,k}|(n-2k) = \sum_{k=0}^{\frac{n-1}{2}} \frac{n(n-2k)}{n-k} \binom{n-k}{k}. \tag{5}$$

This number represents the "flexibility" of this construction of skew Hadamard difference sets.

Example 10. In the case where $n = 5$, the set D is the union of the sets in Table 2. We need $\sum_{k=0}^{2} \frac{5(5-2k)}{5-k}\binom{5-k}{k} = 25$ skew Hadamard difference sets.

3.1 Collection of auxiliary lemmas

We now collect some auxiliary and elementary lemmas for proving Theorem 8.

Lemma 11. *Let $m = 2h+1$ be an odd positive integer, and let*

$$f(x, y) = \sum_{i=0}^{h} \binom{m}{2i} (x+y)^{m-2i}(x-y)^{2i} \in \mathbb{Z}[x, y].$$

Then, $f(x, y) = 2^{m-1}(x^m + y^m)$.

Proof. Since $f(x, -y) = \sum_{i=0}^{h} \binom{m}{2i} (x-y)^{m-2i}(x+y)^{2i}$, we have

$$f(x, y) + f(x, -y) = (2x)^m. \tag{6}$$

Since the coefficient of $x^{m-2j}y^{2j}$ in $f(x, y)$ is equal to that in $f(x, -y)$ for each $1 \leqslant j \leqslant h$, (6) implies that it is equal to 0. On the other hand, by $f(x, y) = f(y, x)$, we conclude that the coefficient of $y^{m-2j}x^{2j}$, $1 \leqslant j \leqslant h$, in $f(x, y)$ is also equal to 0. This completes the proof. □

Table 2: $S \in \mathcal{S}_{5,k}$ and its corresponding D_S

k	$S \in \mathcal{S}_{5,k}$	D_S
0	$S = \varnothing$	$H_{S,0,0} \times H_{S,1,0} \times H_{S,2,0} \times H_{S,3,0} \times H_{S,4,0}$, $H_{S,0,0} \times H_{S,1,0} \times H_{S,2,0} \times H_{S,3,1} \times H_{S,4,1}$ $H_{S,0,0} \times H_{S,1,0} \times H_{S,2,1} \times H_{S,3,0} \times H_{S,4,1}$, $H_{S,0,0} \times H_{S,1,1} \times H_{S,2,0} \times H_{S,3,0} \times H_{S,4,1}$ $H_{S,0,1} \times H_{S,1,0} \times H_{S,2,0} \times H_{S,3,0} \times H_{S,4,1}$, $H_{S,0,0} \times H_{S,1,0} \times H_{S,2,1} \times H_{S,3,1} \times H_{S,4,0}$ $H_{S,0,0} \times H_{S,1,1} \times H_{S,2,0} \times H_{S,3,1} \times H_{S,4,0}$, $H_{S,0,1} \times H_{S,1,0} \times H_{S,2,0} \times H_{S,3,1} \times H_{S,4,0}$ $H_{S,0,0} \times H_{S,1,1} \times H_{S,2,1} \times H_{S,3,0} \times H_{S,4,0}$, $H_{S,0,1} \times H_{S,1,0} \times H_{S,2,1} \times H_{S,3,0} \times H_{S,4,0}$ $H_{S,0,1} \times H_{S,1,1} \times H_{S,2,0} \times H_{S,3,0} \times H_{S,4,0}$, $H_{S,0,0} \times H_{S,1,1} \times H_{S,2,1} \times H_{S,3,1} \times H_{S,4,1}$ $H_{S,0,1} \times H_{S,1,0} \times H_{S,2,1} \times H_{S,3,1} \times H_{S,4,1}$, $H_{S,0,1} \times H_{S,1,1} \times H_{S,2,0} \times H_{S,3,1} \times H_{S,4,1}$ $H_{S,0,1} \times H_{S,1,1} \times H_{S,2,1} \times H_{S,3,0} \times H_{S,4,1}$, $H_{S,0,1} \times H_{S,1,1} \times H_{S,2,1} \times H_{S,3,1} \times H_{S,4,0}$
1	$S = \{0\}$	$\{0_{G_0}\} \times G_1 \times H_{S,2,0} \times H_{S,3,0} \times H_{S,4,0}$, $\{0_{G_0}\} \times G_1 \times H_{S,2,0} \times H_{S,3,1} \times H_{S,4,1}$ $\{0_{G_0}\} \times G_1 \times H_{S,2,1} \times H_{S,3,0} \times H_{S,4,1}$, $\{0_{G_0}\} \times G_1 \times H_{S,2,1} \times H_{S,3,1} \times H_{S,4,0}$
1	$S = \{1\}$	$H_{S,0,0} \times \{0_{G_1}\} \times G_2 \times H_{S,3,0} \times H_{S,4,0}$, $H_{S,0,0} \times \{0_{G_1}\} \times G_2 \times H_{S,3,1} \times H_{S,4,1}$ $H_{S,0,1} \times \{0_{G_1}\} \times G_2 \times H_{S,3,0} \times H_{S,4,1}$, $H_{S,0,1} \times \{0_{G_1}\} \times G_2 \times H_{S,3,1} \times H_{S,4,0}$
1	$S = \{2\}$	$H_{S,0,0} \times H_{S,1,0} \times \{0_{G_2}\} \times G_3 \times H_{S,4,0}$, $H_{S,0,0} \times H_{S,1,1} \times \{0_{G_2}\} \times G_3 \times H_{S,4,1}$ $H_{S,0,1} \times H_{S,1,0} \times \{0_{G_2}\} \times G_3 \times H_{S,4,1}$, $H_{S,0,1} \times H_{S,1,1} \times \{0_{G_2}\} \times G_3 \times H_{S,4,0}$
1	$S = \{3\}$	$H_{S,0,0} \times H_{S,1,0} \times H_{S,2,0} \times \{0_{G_3}\} \times G_4$, $H_{S,0,0} \times H_{S,1,1} \times H_{S,2,1} \times \{0_{G_3}\} \times G_4$ $H_{S,0,1} \times H_{S,1,0} \times H_{S,2,1} \times \{0_{G_3}\} \times G_4$, $H_{S,0,1} \times H_{S,1,1} \times H_{S,2,0} \times \{0_{G_3}\} \times G_4$
1	$S = \{4\}$	$G_0 \times H_{S,1,0} \times H_{S,2,0} \times H_{S,3,0} \times \{0_{G_4}\}$, $G_0 \times H_{S,1,0} \times H_{S,2,1} \times H_{S,3,1} \times \{0_{G_4}\}$ $G_0 \times H_{S,1,1} \times H_{S,2,0} \times H_{S,3,1} \times \{0_{G_4}\}$, $G_0 \times H_{S,1,1} \times H_{S,2,1} \times H_{S,3,0} \times \{0_{G_4}\}$
2	$S = \{0, 2\}$	$\{0_{G_0}\} \times G_1 \times \{0_{G_2}\} \times G_3 \times H_{S,4,0}$
2	$S = \{1, 3\}$	$H_{S,0,0} \times \{0_{G_1}\} \times G_2 \times \{0_{G_3}\} \times G_4$
2	$S = \{2, 4\}$	$G_0 \times H_{S,1,0} \times \{0_{G_2}\} \times G_3 \times \{0_{G_4}\}$
2	$S = \{3, 0\}$	$\{0_{G_0}\} \times G_1 \times H_{S,2,0} \times \{0_{G_3}\} \times G_4$
2	$S = \{4, 1\}$	$G_0 \times \{0_{G_1}\} \times G_2 \times H_{S,3,0} \times \{0_{G_4}\}$

Lemma 12. ([15]) *For any monic polynomial $f(x)$ of degree k of $\mathbb{Z}[x]$ and any integer m, it holds that*

$$\sum_{h=0}^{k} (-1)^h \binom{k}{h} f(m + k - h) = k!. \tag{7}$$

Lemma 13. *For any positive integer ℓ, let*

$$P_{\ell,1}(x) = \sum_{h=0}^{\lfloor \frac{\ell}{2} \rfloor} x^h (-x + 1)^{\ell - 2h} \binom{\ell - h}{h} \in \mathbb{Z}[x].$$

Then, $P_{\ell,1}(x) = 1 - x + x^2 - \cdots + (-1)^\ell x^\ell$.

Proof. It is clear that

$$\begin{aligned} P_{\ell,1}(x) &= \sum_{h=0}^{\lfloor \frac{\ell}{2} \rfloor} \sum_{i=0}^{\ell - 2h} (-1)^i x^{i+h} \binom{\ell - 2h}{i} \binom{\ell - h}{h} \\ &= \sum_{k=0}^{\ell} (-1)^k x^k \sum_{h=0}^{k} (-1)^h \binom{\ell - 2h}{k - h} \binom{\ell - h}{h}. \end{aligned} \tag{8}$$

Since $\binom{\ell-2h}{k-h}\binom{\ell-h}{h} = \binom{k}{h}\binom{\ell-h}{k}$, continuing from (8), we have

$$P_{\ell,1}(x) = \sum_{k=0}^{\ell} (-1)^k x^k \sum_{h=0}^{k} (-1)^h \binom{k}{h} \binom{\ell - h}{k}. \tag{9}$$

By applying (7) in Lemma 12 as $f(x) = x(x-1)\cdots(x-k+1)$ and $m = \ell - k$, we have

$$\sum_{h=0}^{k} (-1)^h \binom{k}{h} \binom{\ell-h}{k} = 1.$$

Hence, continuing from (9), it follows that $P_{\ell,1}(x) = \sum_{k=0}^{\ell} (-1)^k x^k$. □

Lemma 14. *For any positive integer ℓ, let*

$$P_{\ell,2}(x) = \sum_{h=1}^{\lceil \frac{\ell}{2} \rceil} x^{h-1}(-x+1)^{\ell-2h+1} \binom{\ell-h}{h-1}.$$

Then, $P_{\ell,2}(x) = 1 - x + x^2 - \cdots + (-1)^{\ell-1} x^{\ell-1}$.

One can prove this lemma similarly to Lemma 13. Hence, we omit the proof.

3.2 Proof of Theorem 8

In this subsection, we prove Theorem 8 by a series of lemmas.

Lemma 15. *The set D defined in* (4) *satisfies that $D \cap -D = \varnothing$ and $D \cup -D = G^*$.*

Proof. Recall that $G = G_0 \times G_1 \times \cdots \times G_{n-1}$. We first see that for any $x \in G^*$, the set D contains either x or $-x$. Let $I_x \subseteq V$ be the set of zero-coordinates of x. By (2) in the proof of Proposition 5, we have $\binom{V}{k} = \bigcup_{i=0}^{\lfloor \frac{k}{2} \rfloor} \bigcup_{S \in \mathcal{S}_{n,k-i}} \mathcal{T}_{n,i}(S)$. This implies that there exists a unique $S \in \mathcal{S}_{n,|I_x|-i}$ such that $I_x \in \mathcal{T}_{n,i}(S)$. For this S, D_S contains either x or $-x$.

We next see that $|D| = \frac{q^n-1}{2}$. Noting that $|D_S| = q^{|S|}(q-1)^{n-2|S|}/2$ and $|\mathcal{S}_{n,k}| = b_{n,n-2k} = \frac{n}{n-k}\binom{n-k}{k} = 2\binom{n-1-k}{k-1} + \binom{n-1-k}{k}$, by applying Lemmas 13 and 14, we have

$$|D| = \frac{1}{2} \sum_{k=0}^{\frac{n-1}{2}} b_{n,n-2k} q^k (q-1)^{n-2k} = \frac{q-1}{2} P_{n-1,1}(q) - q P_{n-1,2}(q) = \frac{q^n-1}{2}.$$

This completes the proof of the lemma. □

We next evaluate the character values of D. To do so, we first fix some notation:

- $G_i^\perp$, $0 \leqslant i \leqslant n-1$: the character group of G_i, $0 \leqslant i \leqslant n-1$, respectively;
- $G^\perp := G_0^\perp \times G_1^\perp \times \cdots \times G_{n-1}^\perp$;
- For fixed $\psi = (\psi_0, \psi_1, \ldots, \psi_{n-1}) \in G^\perp$, let $I_\psi \subseteq V$ be the set of indices i such that ψ_i is trivial, and let $J_\psi = V \setminus I_\psi$.
- For a subset $X = X_0 \times X_1 \times \cdots \times X_{n-1}$ of G and for $A = \{i_j : 1 \leqslant j \leqslant s\} \subseteq V$ with $i_1 < i_2 < \cdots < i_s$, let $\prod_{i \in A} X_i := X_{i_1} \times X_{i_2} \times \cdots \times X_{i_s}$.
- For $E \subseteq G$ and $A \subseteq V$, let $E_{|A}$ denote the multi-subset of $\prod_{i \in A} G_i$ obtained from E by restricting its coordinates to A. For example, if $n = 3$, $E = E_0 \times E_1 \times E_2$ and $A = \{2\}$, the multiset $E_{|A}$ contains each element of E_2 exactly $|E_0| \cdot |E_1|$ times.

- For $A \subseteq V$, let $\psi_{|A}$ denote the character of $\prod_{i\in A} G_i$ obtained from $\psi \in G^\perp$ by restricting its coordinates to A.

We first evaluate the character values of D_S, $S \in \mathcal{S}_{n,k}$.

Lemma 16. *Let $\psi = (\psi_0, \psi_1, \dots, \psi_{n-1}) \in G^\perp$ be nontrivial, and let $S \in \mathcal{S}_{n,k}$. If $S^+ \cap J_\psi \neq \varnothing$, then*

$$\sum_{x\in D_S} \psi(x) = 0.$$

Proof. If $S^+ \cap J_\psi \neq \varnothing$, there is $i \in S^+$ such that ψ_i is nontrivial. On the other hand, by the definition of D_S, there exists $A \subseteq G_0 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_{n-1}$ such that $D_S = \{(a_0, \dots, a_{i-1}, b, a_{i+1}, \dots, a_{n-1}) : (a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_{n-1}) \in A, b \in G_i\}$. Then, since $\sum_{b\in G_i} \psi_i(b) = 0$, we obtain

$$\sum_{x\in D_S} \psi(x) = \Big(\sum_{(a_1,\dots,a_{i-1},a_{i+1},\dots,a_{n-1})\in A} \prod_{j\neq i} \psi_j(a_j) \Big) \Big(\sum_{b\in G_i} \psi_i(b) \Big) = 0.$$

This completes the proof of the lemma. □

Next, we treat the case where $S^+ \cap J_\psi = \varnothing$. Define

$$E_S = \bigcup_{\sum_{i\in R_S} j_i \equiv 0 \,(\mathrm{mod}\ 2)} \Big(\prod_{i\in R_S} H_{S,i,j_i} \Big) \subseteq \prod_{i\in R_S} G_i. \tag{10}$$

Since $S^+ \cap J_\psi = \varnothing$, we have

$$\sum_{x\in D_S} \psi(x) = \Big(\prod_{i\in S^+} \sum_{x\in G_i} \psi_i(x) \Big) \Big(\prod_{i\in S} \psi_i(0_{G_i}) \Big) \Big(\sum_{y\in E_S} \psi_{|R_S}(y) \Big) = q^{|S|} \sum_{y\in E_S} \psi_{|R_S}(y). \tag{11}$$

Lemma 17. *Let $\psi = (\psi_0, \psi_1, \dots, \psi_{n-1}) \in G^\perp$ be nontrivial, and let $S \in \mathcal{S}_{n,k}$. If $S^+ \cap J_\psi = \varnothing$ and ψ_i is nontrivial for any $i \in R_S$, it holds that*

$$\psi(D_S) = \frac{-q^{|S|} \pm \sqrt{-q^n}}{2}.$$

Proof. By (11), we need to show that $\sum_{y\in E_S} \psi_{|R_S}(y) = \frac{-1\pm\sqrt{-q^{|R_S|}}}{2}$. By the definition of E_S and Lemma 1,

$$\sum_{y\in E_S} \psi_{|R_S}(y) = \sum_{i=0}^{\frac{|R_S|-1}{2}} \binom{|R_S|}{2i} \left(\frac{-1+\sqrt{-q}}{2} \right)^{|R_S|-2i} \left(\frac{-1-\sqrt{-q}}{2} \right)^{2i}$$
$$\text{or} \quad \sum_{i=0}^{\frac{|R_S|-1}{2}} \binom{|R_S|}{2i} \left(\frac{-1-\sqrt{-q}}{2} \right)^{|R_S|-2i} \left(\frac{-1+\sqrt{-q}}{2} \right)^{2i}.$$

Then, by Lemma 11, we have

$$\sum_{y\in E_S} \psi_{|R_S}(y) = \frac{-1+\sqrt{-q^{|R_S|}}}{2} \text{ or } \frac{-1-\sqrt{-q^{|R_S|}}}{2}.$$

This completes the proof of the lemma. □

Lemma 18. *Let $\psi = (\psi_0, \psi_1, \ldots, \psi_{n-1}) \in G^\perp$ be nontrivial, and let $S \in \mathcal{S}_{n,k}$. If $S^+ \cap J_\psi = \varnothing$ and ψ_i is trivial for some $i \in R_S$, it holds that*

$$\psi(D_S) = -q^{|S|}\frac{(-q+1)^{n-2|S|-t}}{2},$$

where t is the number of $i \in R_S$ such that ψ_i is nontrivial, i.e., $t = |R_S \cap J_\psi|$.

Proof. By (11), we need to show that $\sum_{y\in E_S} \psi_{|R_S}(y) = -(-q+1)^{|R_S|-t}/2$. We consider $E_{S|R_S\cap J_\psi}$, which is the multi-subset of $\prod_{i\in R_S\cap J_\psi} G_i$ obtained from E_S by restricting its coordinates to $R_S \cap J_\psi$. The multiset $E_{S|R_S\cap J_\psi}$ contains every element of $\prod_{i\in R_S\cap J_\psi} G_i^*$ exactly $(q-1)^{|R_S|-t}/2$ times. Since $\sum_{x\in G_i^*} \psi_i(x) = -1$ for any nontrivial ψ_i, we have

$$\sum_{y\in E_S} \psi_{|R_S}(y) = \psi_{|R_S\cap J_\psi}(E_{S|R_S\cap J_\psi}) = (-1)^t(q-1)^{|R_S|-t}/2.$$

This completes the proof of the lemma. □

We are now ready for proving Theorem 8.

Proof of Theorem 8. Let $\psi = (\psi_0, \psi_1, \ldots, \psi_{n-1})$ be a nontrivial character of G. We show that $\psi(D) = \sum_{k=0}^{\frac{n-1}{2}} \sum_{S\in\mathcal{S}_{n,k}} \psi(D_S) \in \{\frac{-1\pm\sqrt{-q^n}}{2}\}$. Let $I_{\psi,i}$, $i = 1, 2, \ldots, r$, be the subsets of I_ψ partitioning I_ψ so that each $I_{\psi,i}$ consists of consecutive numbers with respect to the ordering $0 \to 1 \to \cdots \to n-1 \to 0$ and any two elements from distinct $I_{\psi,i}$ and $I_{\psi,j}$ are not consecutive. Denote the size of each $I_{\psi,i}$ by t_i. Then, we can write $I_{\psi,i} = \{e_i, e_i+1, \ldots, e_i+t_i-1\}$ for some integer e_i.

We consider only subsets $S \in \bigcup_{k=0}^{\frac{n-1}{2}} \mathcal{S}_{n,k}$ such that S^+ contained in I_ψ; otherwise we have $S^+ \cap J_\psi \neq \varnothing$; then $\psi(D_S) = 0$ by Lemma 16. Let $\mathcal{S}_\psi = \{S \in \bigcup_{k=0}^{\frac{n-1}{2}} \mathcal{S}_{n,k} : S^+ \subseteq I_\psi\}$.

Let $S_1 = S_1^+ = \varnothing$. For all $I_{\psi,i}$, we add $e_i+t_i-1, e_i+t_i-3, e_i+t_i-5, \ldots, \in I_{\psi,i}$ into S_1^+ and their neighbors $e_i+t_i-2, e_i+t_i-4, e_i+t_i-6, \ldots$ into S_1. Then, $S_1 \in \mathcal{S}_\psi$ is the unique element satisfying that $S_1^+ \cap J_\psi = \varnothing$ and ψ_i is nontrivial for any $i \in R_{S_1}$. Then, by Lemma 17, we have

$$\psi(D_{S_1}) = \frac{-q^{|S_1|} \pm \sqrt{-q^n}}{2}. \tag{12}$$

We now evaluate $\psi(D \setminus D_{S_1}) = \sum_{S\in\mathcal{S}_\psi\setminus\{S_1\}} \psi(D_S)$. By Lemma 18, we have

$$\sum_{S\in\mathcal{S}_\psi\setminus\{S_1\}} \psi(D_S) = -\frac{1}{2}\sum_{S\in\mathcal{S}_\psi} q^{|S|}(-q+1)^{|I_\psi\cap R_S|} + \frac{1}{2}q^{|S_1|}(-q+1)^{|I_\psi\cap R_{S_1}|}. \tag{13}$$

Here, $\frac{1}{2}q^{|S_1|}(-q+1)^{|I_\psi\cap R_{S_1}|} = \frac{1}{2}q^{|S_1|}$ since $|I_\psi \cap R_{S_1}| = 0$. Furthermore, $\sum_{S\in\mathcal{S}_\psi} q^{|S|}(-q+1)^{|I_\psi\cap R_S|}$ is factorized into

$$\prod_{i=1}^{r}\left(\sum_{h=0}^{\lfloor\frac{t_i}{2}\rfloor}\binom{t_i-h}{h}q^h(-q+1)^{t_i-2h} + \sum_{h=1}^{\lceil\frac{t_i}{2}\rceil}\binom{t_i-h}{h-1}q^h(-q+1)^{t_i-2h+1}\right), \tag{14}$$

where $\binom{t_i-h}{h}$ (resp. $\binom{t_i-h}{h-1}$) means the number of choices of a subset of size h of S^+ from $I_{\psi,i}$ so that $e_i \notin S^+$ (resp. $e_i \in S^+$). By applying Lemmas 13 and 14 as $x = q$, we have

$$\sum_{h=0}^{\lfloor\frac{t_i}{2}\rfloor}\binom{t_i-h}{h}q^h(-q+1)^{t_i-2h} + \sum_{h=1}^{\lceil\frac{t_i}{2}\rceil}\binom{t_i-h}{h-1}q^h(-q+1)^{t_i-2h+1} = P_{t_i,1}(q) + qP_{t_i,2}(q) = 1.$$

Hence, continuing from (14), we have $\sum_{S\in\mathcal{S}_\psi} q^{|S|}(-q+1)^{|I_\psi\cap R_S|}=1$. Finally, by (12) and (13), we obtain

$$\begin{aligned}\psi(D) &= \psi(D_{S_1}) + \sum_{S\in\mathcal{S}_\psi\setminus\{S_1\}} \psi(D_{S_1})\\ &= \frac{-q^{|S_1|}\pm\sqrt{-q^n}}{2} - \frac{1}{2} + \frac{q^{|S_1|}}{2} = \frac{-1\pm\sqrt{-q^n}}{2}.\end{aligned}$$

This completes the proof of the theorem. □

4 Concluding Remarks

We checked by a computer to see how many inequivalent skew Hadamard difference sets in $(\mathbb{F}_q^n,+)$ can be obtained from our construction with $G_i=\mathbb{F}_q$ in the cases where

$$(q,n)=(7,3),(11,3),(19,3),(23,3),(3,5).$$

Example 19. We consider the case where $n=3$. In this case, we need six skew Hadamard difference sets in $(\mathbb{F}_q,+)$ to apply Theorem 8. We choose either the Paley difference set or its inverse in $\mathbb{F}_q$ as the six skew Hadamard difference sets in $(\mathbb{F}_q,+)$. Then, there are 2^6 possible choices. In the cases where $q=7,11,19$ and 23, we obtained exactly two inequivalent skew Hadamard difference sets D in $(\mathbb{F}_q^3,+)$ from the 2^6 candidates, both of which satisfy $\#\mathsf{Aut}(\mathrm{Dev}(D))=3\cdot(\frac{q-1}{2})^3\cdot q^3$.

From Example 19, the following problem naturally arises.

Problem 20. If $q>3$ is a prime and $n=3$, does the construction give rise to at least two inequivalent skew Hadamard difference sets with $\#\mathsf{Aut}(\mathrm{Dev}(D))=3\cdot(\frac{q-1}{2})^3\cdot q^3$?

Example 21. We next consider the case where $n=5$. In this case, we need 25 skew Hadamard difference sets in $(\mathbb{F}_q,+)$ to apply Theorem 8. As in Example 19, we take either the Paley difference set or its inverse in $\mathbb{F}_q$ as the 25 skew Hadamard difference sets in $(\mathbb{F}_q,+)$. Then, there are 2^{25} possible choices. In the cases where $q=3$, we obtained exactly nine inequivalent skew Hadamard difference sets D in $(\mathbb{F}_q^5,+)$ from the 2^{25} candidates, four of which satisfy $\#\mathsf{Aut}(\mathrm{Dev}(D))=5\cdot q^5$ and five of which satisfy $\#\mathsf{Aut}(\mathrm{Dev}(D))=q^5$.

The number of skew Hadamard difference sets as input for our construction increases according to the growth of n. Hence, the following question naturally arises.

Problem 22. We apply the recursive construction as $G_i=\mathbb{F}_q$ and $H_{S,i,j}$ either the Paley difference set in $(\mathbb{F}_q,+)$ or its inverse. Does the number of inequivalent skew Hadamard difference sets in $(\mathbb{F}_q^n,+)$ obtained from the construction increase according to the growth of n?

The fact that we could have a recursive construction implies that there exist skew Hadamard difference sets in abundance. In fact, as already mentioned, if one finds a skew Hadamard difference set in a nonelementary abelian group, we obtain infinite families of skew Hadamard difference sets in nonelementary abelian groups by applying our recursive construction. Therefore, the author feels that Conjecture 2 is doubtful. Hence, we close this paper with the following important problem.

Problem 23. Can one find a skew Hadamard difference set in a nonelementary abelian group?

Acknowledgment

The author would like to thank the reviewers for their helpful comments. In particular, one of the reviewers suggested to mention about the formula (3).

References

[1] L. Carlitz. A theorem on permutations in a finite field. *Proc. Amer. Math. Soc.*, 11:456–459, 1960.

[2] Y. Q. Chen and T. Feng. Abelian and non-abelian Paley type group schemes. *Des. Codes Cryptogr.*, 68:313–317, 2013.

[3] Y. Q. Chen and T. Feng. Paley type sets from cyclotomic classes and Arasu-Dillon-Player difference sets. *Des. Codes Cryptogr.*, 74:581–600, 2015.

[4] Y. Q. Chen, Q. Xiang, and S. K. Sehgal. An exponent bound on skew Hadamard abelian difference sets. *Des. Codes Cryptogr.*, 4:313–317, 1994.

[5] C. Ding and J. Yuan. A family of skew Hadamard difference sets. *J. Combin. Theory, Ser. A*, 113:1526–1535, 2006.

[6] C. Ding, Z. Wang, and Q. Xiang. Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in $\mathrm{PG}(3, 3^{2h+1})$. *J. Combin. Theory, Ser. A*, 114:867–887, 2007.

[7] C. Ding, A. Pott, and Q. Wang. Skew Hadamard difference sets from Dickson polynomials of order 7. *J. Combin. Des.*, 23:436–461, 2015.

[8] T. Feng and Q. Xiang. Cyclotomic constructions of skew Hadamard difference sets. *J. Combin. Theory, Ser. A*, 119:245–256, 2012.

[9] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science, 2nd edn.* Addison-Wesley Professional, 1994.

[10] W. M. Kantor. 2-transitive symmetric designs. *Trans. Amer. Math. Soc.*, 146:1–28, 1969.

[11] T. Koshy. *Fibonacci and Lucas Numbers with Applications.* John Wiley & Sons Inc., 2001.

[12] K. Momihara. Skew Hadamard difference sets from cyclotomic strongly regular graphs. *SIAM J. Discrete Math.*, 27:1112–1122, 2013.

[13] K. Momihara. Inequivalence of skew Hadamard difference sets and triple intersection numbers modulo a prime. *Electron. J. Combin.*, 20:#P35, 2013.

[14] M. E. Muzychuk. On skew Hadamard difference sets. arXiv:1012.2089, 2010.

[15] S. M. Ruiz. An algebraic identity leading to Wilson's theorem. *Math. Gazette*, 80:579–582, 1996.

[16] G. Weng, W. Qiu, Z. Wang, and Q. Xiang. Pseudo-Paley graphs and skew Hadamard difference sets from presemifields. *Des. Codes Cryptogr.*, 44:49–62, 2007.

Corrigendum – Added June 9, 2021

In [2], the author gave a recursive construction for skew Hadamard difference sets. However, the author recently realized that the construction method given in [2] is essentially covered by Turyn's product theorem [3] for skew or symmetric C-matrices though not all of the results in [2] are covered. Here, note that no researcher working in the area of skew Hadamard difference sets has mentioned that Turyn's construction is applicable to skew Hadamard difference sets though many papers on skew Hadamard difference sets were published in recent years. This may have happened because the condition for the existence of skew Hadamard difference sets is stronger than that of ordinary skew Hadamard matrices in general. However, it is not difficult to see that Turyn's product theorem for C-matrices is also applicable to skew Hadamard difference sets and Paley type partial difference sets since the construction is based on Kronecker products of matrices. In fact, one can use group-invariant matrices as the initial input of the construction, and then the resulting matrix is again group-invariant with respect to the direct product of the groups involved. More detailed comparisons between the results in [2] and [3] are given below.

(1) General skew or symmetric C-matrices were treated in [3] while only group-invariant skew C-matrices, that is, skew Hadamard difference sets, were treated in [2].

(2) The matrix notation was used for the construction in [3] while the set notation was used in [2].

(3) The proofs in [3] and [2] are completely different; $WW^\top$ for the core W of a C-matrix was directly calculated in [3] while the character values of a skew Hadamard difference set (that is, the eigenvalues of $(J-I+W)/2$) were computed in [2]. There is a nontrivial contribution of our proof for generalizing the construction to that for partial difference sets, see [1].

(4) The flexibility of the construction was discussed in more details in [2]. In fact, the variation of the construction using different designs as initial input was treated only in the case where the number of products is three in [3] while the general case was treated in [2]. In this sense, the construction given in [2] can be viewed as a generalization of that given in [3] for skew C-matrices. For example, Example 1.3 in [2] allows six different skew Hadamard difference sets as the initial input for the recursion but the example given soon after corollary in [3, P. 534] allows only three different C-matrices as the initial input. Thus, the construction in [2] is a generalization of that in [3] even in the case where the number of products is three.

(5) The inequivalence and the automorphism groups of skew Hadamard difference sets obtained from the construction were also discussed in [2].

References

[1] K. Hayashida, K. Momihara, Note on a construction of partial difference sets, https://www.educ.kumamoto-u.ac.jp/~momihara/Note_PDS.pdf.

[2] K. Momihara, A recursive construction for skew Hadamard difference sets, *Electron. J. Combin.* **27(3)** (2020), #3.36.

[3] R. J. Turyn, On C-matrices of arbitrary powers, *Can. J. Math.*, **23** (1971), 531–535.