ON SKEW HADAMARD DIFFERENCE SETS

MIKHAIL MUZYCHUK

Abstract. In this paper we construct exponentionally many non-isomorphic skew Hadamard difference sets over an elementary abelian group of order q^3.

1. Introduction

During last 5 years there was ongoing activity related to skew Hadamard difference sets (all necessary definitions are given in the next section). Apart the classical family of such sets there are only few infinite series built quite recently. We refer the reader to the papers [4],[2],[5] where the topic is surveyed.

The initial point for this paper was Feng's construction of skew Hadamard difference sets [5] over non-abelian groups of order p^3 (see the last section where the history of this paper is presented). An analysis of Feng's construction shows that the automorphism group of the design obtained from his difference set contains an elementary abelian regular subgroup of order p^3. This means that this design could be constructed from a difference set over an elementary abelian group of order p^3. This gives a clue how to generalize the construction to elementary abelian groups of order q^3. We take a finite field $\mathbb{F}_q, q \equiv 3 (\mathrm{mod}\, 4)$ and consider the orbits of a certain subgroup $A \leq \mathsf{GL}_3(\mathbb{F}_q)$ (see Section 3 for definition of A) on the vector space $\mathbb{F}_q^3$. The first main result of the paper (Theorem 5.2) enumerates all A-invariant skew Hadamard difference sets. It turns out that the number of such sets is $4\binom{q}{\frac{q+1}{2}}$. The second main result (Theorem 6.1) of the paper solves isomorphism problem for designs generated by the constructed difference sets. It turns out that the number of the design isomorphism classes is at least $2^{q+1}/q^4$.

Each design obtained in that way is invariant under the action of the group $V \rtimes A$ of order $q^4 \frac{q-1}{2}$. If $p > 3$, then the group $V \rtimes A$ contains a non-abelian subgroup isomorphic to $UT_3(q)$ acting regularly on the point set. Therefore in the case of $p > 3$ each design may be also derived from a skew Hadamard difference set over the non-abelian group $UT_3(q)$.

2. Preliminaries

Let H be a finite group written multiplicatively with unit element 1_H. We write $\mathbb{Z}[H]$ for the group algebra of H over the integers. Given an element $x = \sum_{h\in H} x_h h \in \mathbb{Z}[H]$, we write $x^{(-1)}$ for the element $\sum_{h\in H} x_h h^{-1}$. For a subset $D \subseteq H$ we set $D^{(-1)} := \{d^{-1} \mid d \in D\}$ and $\underline{D} := \sum_{d\in D} d \in \mathbb{Z}[H]$.

2.1. **Schur rings.** Given a partition $\mathcal{S}$ of H, we denote by $\mathcal{S}(h), h \in H$ a unique class of $\mathcal{S}$ containing h.

Definition 2.1. A partition $\mathcal{S}$ of H is called a *Schur partition* iff it satisfies the following conditions

(S1) $\mathcal{S}(1_H) = \{1_H\}$;
(S2) $\mathcal{S}(h^{-1}) = \mathcal{S}(h)^{(-1)}$ for each $h \in H$;
(S3) the free $\mathbb{Z}$-submodule $\mathbb{Z}[\underline{\mathcal{S}}]$ spanned by $\underline{S}, S \in \mathcal{S}$ is a subalgebra of $\mathbb{Z}[H]$. This subalgebra is called a *Schur ring/algebra* spanned by $\mathcal{S}$.

If H is abelian, then each Schur partition $\mathcal{S}$ defines a *dual* Schur partition $\mathcal{S}^*$ over the dual group $\mathsf{Irr}(H)$.Two irreducible characters $\chi, \eta \in \mathsf{Irr}(H)$ belong to the same class of $\mathcal{S}^*$ if and only if $\chi(\underline{S}) = \eta(\underline{S})$ holds for each $S \in \mathcal{S}$. A *character table* of $\mathcal{S}$ describes all irreducible complex representations of $\mathbb{C}[\underline{\mathcal{S}}]$. It's rows are parametrized by the sets of $\mathcal{S}^*$ while the columns are parametrized by the sets of $\mathcal{S}$. The entry of the table corresponding to a pair $R \in \mathcal{S}^*$,$S \in \mathcal{S}$ is equal to $\chi(\underline{S})$ where $\chi \in R$.

If Φ is a group of automorphisms of H, then the orbits of Φ on H always form a Schur partition. If H is abelian, then the dual Schur partition is formed by the orbits of a natural action of Φ on $\mathsf{Irr}(H)$.

2.2. **Difference sets and Cayley designs.** A subset D is called a (v, k, λ)-*difference set* iff $v = |H|, k = |D|$ and the following equation is satisfied

$$\underline{D}\,\underline{D}^{(-1)} = (k - \lambda)1_H + \lambda\underline{H} \tag{1}$$

A difference set D is called a *skew Hadamard difference set* (SHDS for short) if $H \setminus \{1_H\} = D \cup D^{(-1)}$ and $D \cap D^{(-1)} = \emptyset$. It is not difficult to check that a subset $D \subseteq H$ is an SHDS iff the partition $\{1_H\}, D, D^{(-1)}$ is a Schur partition of H. The parameters of an SHDS over H are $(|H|, \frac{|H|-1}{2}, \frac{|H|-3}{4})$.

Every (v, k, λ) difference set $D \subset H$ produces a $2 - (v, k, \lambda)$ symmetric design with point set H and block set $\mathsf{Dev}(H, D) := \{Dh \,|\, h \in H\}$. If the group H is clear from the context, then we write just $\mathsf{Dev}(D)$ instead of $\mathsf{Dev}(H, D)$.

In general, the set $\mathsf{Dev}(D)$ could be built for any subset D of H. In what follows we call the set $\mathsf{Dev}(D)$ *a Cayley design generated by* D. In the case when H is an abelian group written additively we call $\mathsf{Dev}(D)$ a *translation design* generated by D.

The *automorphism group* of a design $(H, \mathcal{D}), \mathcal{D} = \mathsf{Dev}(D)$, notation $\mathsf{Aut}(\mathcal{D})$, consists of all permutations $g \in \mathsf{Sym}(H)$ which permute the blocks $B \in \mathcal{D}$. It always contains a subgroup $H_* := \{h_* \,|\, h \in H\}$ where $h_* \in \mathsf{Sym}(H)$ is a right translation [1] by $h \in H$ (that is $x^{h_*} = xh$). The group H_* acts regularly on points and transitively on the blocks of the design $(H, \mathcal{D})$. This property is characteristic for Cayley designs. More precisely, a simple design is isomorphic to a Cayley design $\mathsf{Dev}(H, D)$ iff the automorphism group of the design contains a subgroup isomorphic to H which acts regularly on points and transitively on blocks. Below we collect some elementary properties of Cayley designs which will be used in the paper.

Proposition 2.2. *Let $\mathcal{D} := \mathsf{Dev}(H, D)$ be a Cayley design s.t. $|\mathcal{D}| = |H|$ and G a subgroup of $\mathsf{Aut}(\mathcal{D})$ which contains H_*. Assume that a point stabilizer $G_p, p \in H$ fixes some block $B \in \mathcal{D}$. Then*

1. *If G_p fixes a point $q \in H$, then G_p fixes also a block $Bp^{-1}q$;*
2. *If G_p fixes a block $Bh, h \in H$, then G_p also fixes a point ph^{-1};*
3. *there exists $F \leq H$ such that*

$$\mathsf{Fix}_H(G_p) = \{pf \,|\, f \in F\}, \mathsf{Fix}_{\mathcal{D}}(G_B) = \{Bf \,|\, f \in F\}.$$

[1] In the case when H is an abelian group written additively we write h_+ instead of h_*.

PROOF. PART (1). Let $g \in G_p$ be an arbitrary element. Then $(Bp^{-1}q)^g = Bh$ for some $h \in H$. Equivalently, $B^{p_*^{-1}q_*g} = Bh$. Since $G_pH = HG_p$, there exist $g_1 \in G_p$ and $r \in H$ such that $p_*^{-1}q_*g = g_1r_*$. This implies that $Bh = B^{g_1r_*} = Br$. Also

$$p^{p_*^{-1}q_*g} = p^{g_1r_*} \implies q^g = pr \implies q = pr \implies r = p^{-1}q.$$

Thus $(Bp^{-1}q)^g = Bh = Br = Bp^{-1}q$.

PART (2). It follows from $(Bh)^{G_p} = Bh$ that $h_*G_ph_*^{-1} \leq G_B$. By assumption $G_p \leq G_B$. Since $|G_B| = |G|/|\mathcal{D}| = |G|/|H| = |G_p|$, we obtain $G_p = G_B$. Thus $h_*G_ph_*^{-1} = G_p$ implying

$$(ph^{-1})^{G_p} = (ph^{-1})^{h_*G_ph_*^{-1}} = ph^{-1}.$$

PART (3). It is well-known that $\mathsf{Fix}_H(G_p) = p^{\mathbf{N}_G(G_p)}$. It follows from $G = G_pH_*$ that $\mathbf{N}_G(G_p) = G_pF_*$ for a uniquely determined subgroup $F \leq H$. Now we obtain that

$$\mathsf{Fix}_H(G_p) = p^{\mathbf{N}_G(G_p)} = p^{G_pF_*} = pF.$$

The second equality follows from $G_B = G_p$. □

3. THE GROUP A AND ITS ORBITS

For the rest of the paper it is assumed that $q = p^n$ is an odd power of a prime p which is congruent 3 modulo 4. Let $V = \mathbb{F}_q^3$. We write the elements of V as column vectors $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ and the elements of the dual space V^* are written as row vectors. For $v = (v_1, v_2, v_3) \in V^*, w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} \in V$ their product $v_1w_1 + v_2w_2 + v_3w_3$ is written as vw. For $w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}$ we set $w^* := (w_3, w_2, w_1)$. Analogously $(v_1, v_2, v_3)^* := \begin{pmatrix} v_3 \\ v_2 \\ v_1 \end{pmatrix}$. Notice that $vw = w^*v^*$.

For each $x \in \mathbb{F}_q$ we set

$$E(x) := \begin{pmatrix} 1 & x & x^2/2 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}.$$

The set $E := \{E(x) \mid x \in \mathbb{F}_q\}$ is an elementary abelian subgroup of $GL_3(\mathbb{F}_q)$ isomorphic to $(\mathbb{F}_q, +)$. Let also $S := \{sI_3 \mid s \in \mathbb{F}_q^{*2}\}$. The group $A := ES$ is an abelian group of odd order $q(q-1)/2$. In what follows V is considered as a left A-space while V^* is considered as a right A-space. The following formula is straightforward

$$\forall_{v \in V}\ \forall_{g \in A}\ (gv)^* = v^*g. \tag{2}$$

To describe the orbits of A on V and V^* we introduce a certain set which will be used as an index set for A-orbits. Define $I := \mathbb{F}_q \cup \{\infty, \bullet\}$ and for each $i \in I$

define the A-orbits $O_i, i \in I$ and $O_i^*, i \in I$ as follows. For $i \in \mathbb{F}_q$ we set

$$O_i = A \begin{pmatrix} i \\ 0 \\ 1 \end{pmatrix} = \left\{ \begin{pmatrix} s\left(\frac{x^2}{2} + i\right) \\ sx \\ s \end{pmatrix} \middle| x \in \mathbb{F}_q, s \in \mathbb{F}_q^{*2} \right\}, O_i^* := (O_i)^*$$

$$O_\infty := A \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} x \\ s \\ 0 \end{pmatrix} \middle| x \in \mathbb{F}_q, s \in \mathbb{F}_q^{*2} \right\}, O_\infty^* := (O_\infty)^*$$

$$O_\bullet := A \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} s \\ 0 \\ 0 \end{pmatrix} \middle| s \in \mathbb{F}_q^{*2} \right\}, O_\bullet^* := (O_\bullet)^*$$

Proposition 3.1. *The sets $\{O_i, -O_i \,|\, i \in I\}$ and $\{O_i^*, -O_i^* \,|\, i \in I\}$ form complete sets of non-zero orbits of A on V and V^*, respectively.*

In what follows we set $\mathcal{O} := \{O_i \,|\, i \in I\}, -\mathcal{O} := \{-O_i \,|\, i \in I\}$ and analogously for duals.

The orbits of A on V form a Schur partition $\mathcal{S}$ while the A-orbits on V^* form a dual Schur partition $\mathcal{S}^*$. A linear map * between V and V^* yields an isomorphism between these S-rings. Notice that $\mathcal{S} := \mathcal{O} \cup -\mathcal{O} \cup \{\{0\}\}$ and $\mathcal{S}^* := \mathcal{O}^* \cup -\mathcal{O}^* \cup \{\{0\}\}$.

4. The character table of $\mathcal{S}$.

Let $\omega_p \in \mathbb{C}$ be a p-th primitive root of unity and $\tau : \mathbb{F}_q \to \mathbb{C}$ be the map defined by $\tau(x) := \omega_p^{tr(x)}$ where $tr(x)$ is an $\mathbb{F}_p$-trace of $x \in \mathbb{F}_q$. Clearly that $\tau(x+y) = \tau(x)\tau(y)$ for $x, y \in \mathbb{F}_q$.

The additive characters of V are parametrized by the vectors of V^* and the value $\chi_v(w)$ of the character χ_v (where $v \in V^*, w \in V$) is equal to $\tau(vw)$.

For the rest of the text we set $\mathsf{z} := \sum_{x \in \mathbb{F}_q^{*2}} \tau(x)$ and $\Delta := \mathsf{z} - \overline{\mathsf{z}}$. It is well-known that

$$\mathsf{z} = \frac{-1 \pm \sqrt{-q}}{2}, \mathsf{z} + \overline{\mathsf{z}} = -1, \Delta = \pm\iota\sqrt{q}$$

(here and later on $\overline{z}$ means a complex conjugate of z).

The principal part of the character table of $\mathcal{S}$ is a square matrix of size $2(q+2)$, its columns are parametrized by the non-zero A-orbits on V while the rows are parametrized by the non-zero A-orbits on V^*. The value of the character table, denoted as $[R, O]$, corresponding to a pair of A-orbits $O \subset V, R \subset V^*$ is computed by the formula

$$[R, O] = \sum_{w \in O} \chi_v(w).$$

where $v \in R$ is an arbitrary element.

It follows from

$$[R, -O] = [R, -O] = \overline{[R, O]} \text{ and } [-R, -O] = [R, O].$$

that it is sufficient to compute only the numbers $[O_i^*, O_j]$ for $i, j \in I$.

In what follows we write $\sigma(x), x \in \mathbb{F}_q^*$ for an automorphism of $\mathbb{C}$ which is identical if x is a square and complex conjugation if x is a non-square. Notice that for $a \in \mathbb{F}_q^*$ we always have that $\sum_{s \in \mathbb{F}_q^{*2}} \tau(as) = \mathsf{z}^{\sigma(a)}$.

Proposition 4.1. *The values of* $[O_i^*, O_j]$ *are given in the following table*

	$j \in \mathbb{F}_q$	$j = \infty$	$j = \bullet$
$i \in \mathbb{F}_q$	$P(i,j)$	0	z
$i = \infty$	0	$q\mathsf{z}$	$\frac{q-1}{2}$
$i = \bullet$	$q\mathsf{z}$	$q\frac{q-1}{2}$	$\frac{q-1}{2}$

Table 1

where

$$P(i,j) = \begin{cases} \frac{q-1}{2}(1+2\mathsf{z}^{\sigma(2)}) & i+j=0; \\ \mathsf{z}^{\sigma(i+j)}(1+2\mathsf{z}^{\sigma(2)}) & i+j\neq 0 \end{cases}. \tag{3}$$

Proof. First we show that

$$\frac{[O_i^*, O_j]}{|O_j|} = \frac{[O_j^*, O_i]}{|O_i|}.$$

Pick arbitrary $v \in O_i, w \in O_j$. Then

$$[O_i^*, O_j] = \sum_{u\in O_j} \chi_{v^*}(u) = \frac{|O_j|}{|G|}\sum_{g\in G}\chi_{v^*}(gw) = \frac{|O_j|}{|G|}\sum_{g\in G}\tau(v^*(gw)).$$

It follows from (2) that

$$v^*(gw) = (v^*g)w = w^*(v^*g)^* = w^*(gv).$$

Therefore

$$[O_i^*, O_j] = \frac{|O_j|}{|G|}\sum_{g\in G}\tau(w^*(gv)) = \frac{|O_j|}{|G|}\sum_{g\in G}\chi_{w^*}(gv) = \frac{|O_j|}{|G|}\cdot\frac{|G|}{|O_i|}[O_j^*, O_i] = \frac{|O_j|}{|O_i|}[O_j^*, O_i].$$

Thus it is sufficient to check Table 1 for 6 cases only:

$$i,j \in \mathbb{F}_q;\ i=\infty, j\in\mathbb{F}_q;\ i=\bullet, j\in F_q;\ i=j=\infty;\ i=\bullet, j=\infty;\ i=j=\bullet.$$

Each of these cases is checked below separately.

Case A. $i,j \in \mathbb{F}_q$. Since the value of $[O_i^*, O_j]$ does not depend on a choice of $v \in O_i^*$ we can take $v = (1,0,i)$. Then

$$[O_i^*, O_j] = \sum_{w\in O_j}\chi_v(w) = \sum_{w\in O_j}\tau(vw) = \sum_{s\in\mathbb{F}_q^{*2}, x\in\mathbb{F}_q}\tau\left((1,0,i)\begin{pmatrix} s\left(\frac{x^2}{2}+j\right) \\ sx \\ s\end{pmatrix}\right) =$$

$$\sum_{s\in\mathbb{F}_q^{*2}, x\in\mathbb{F}_q}\tau\left(s\left(\frac{x^2}{2}+j\right)+si\right) = \sum_{s\in\mathbb{F}_q^{*2}, x\in\mathbb{F}_q}\tau\left(s\frac{x^2}{2}+s(i+j)\right) =$$

$$\sum_{s\in\mathbb{F}_q^{*2}}\sum_{x\in\mathbb{F}_q}\tau\left(s\frac{x^2}{2}\right)\tau(s(i+j)) = \sum_{s\in\mathbb{F}_q^{*2}}\tau(s(i+j))\sum_{x\in\mathbb{F}_q}\tau\left(\frac{x^2}{2}\right) =$$

$$\sum_{s\in\mathbb{F}_q^{*2}}\tau(s(i+j))(1+2\mathsf{z}^{\sigma(2)}).$$

If $i+j=0$, then the latter sum equals to $(1+2\mathsf{z}^{\sigma(2)})\frac{q-1}{2}$. If $i+j\neq 0$, then the latter sum is $\mathsf{z}^{\sigma(i+j)}(1+\mathsf{z}^{\sigma(2)})$.

Case B. $i=\infty, j\in\mathbb{F}_q$.
For $v=(0,1,0)\in O^*_\infty$ we obtain

$$[O^*_\infty,O_j]=\sum_{w\in O_j}\chi_{(0,1,0)}(w)\sum_{s\in\mathbb{F}_q^{*2},x\in\mathbb{F}_q}\tau\left((0,1,0)\begin{pmatrix} s\left(\frac{x^2}{2}+j\right)\\ sx\\ s\end{pmatrix}\right)=\sum_{s\in\mathbb{F}_q^{*2},x\in\mathbb{F}_q}\tau(sx)=0.$$

Case C. $i=\bullet, j\in\mathbb{F}_q$.
For $v=(0,0,1)\in O^*_\bullet$ we obtain

$$[O^*_\bullet,O_j]=\sum_{w\in O_j}\chi_{(0,0,1)}(w)=\sum_{s\in\mathbb{F}_q^{*2},x\in\mathbb{F}_q}\tau\left((0,0,1)\begin{pmatrix} s\left(\frac{x^2}{2}+j\right)\\ sx\\ s\end{pmatrix}\right)=\sum_{s\in\mathbb{F}_q^{*2},x\in\mathbb{F}_q}\tau(s)=q\mathsf{z}.$$

Case D. $i=j=\infty$.
Take $(0,1,0)\in O^*_\infty$. Then

$$[O^*_\infty,O_\infty]=\sum_{w\in O_\infty}\chi_{(0,1,0)}(w)=\sum_{s\in\mathbb{F}_q^{*2},x\in\mathbb{F}_q}\tau\left((0,1,0)\begin{pmatrix} x\\ s\\ 0\end{pmatrix}\right)=\sum_{s\in\mathbb{F}_q^{*2},x\in\mathbb{F}_q}\tau(s)=q\mathsf{z}.$$

Case E. $i=\bullet, j=\infty$.
Take $(0,0,1)\in O^*_\bullet$. Then

$$[O^*_\bullet,O_\infty]=\sum_{w\in O_\infty}\chi_{(0,0,1)}(w)=\sum_{s\in\mathbb{F}_q^{*2},x\in\mathbb{F}_q}\tau\left((0,0,1)\begin{pmatrix} x\\ s\\ 0\end{pmatrix}\right)=\sum_{s\in\mathbb{F}_q^{*2},x\in\mathbb{F}_q}\tau(0)=q\frac{q-1}{2}.$$

Case F. $i=j=\bullet$.
Take $(0,0,1)\in O^*_\bullet$. Then

$$[O^*_\bullet,O_\bullet]=\sum_{w\in O_\bullet}\chi_{(0,0,1)}(w)=\sum_{s\in\mathbb{F}_q^{*2}}\tau\left((0,0,1)\begin{pmatrix} s\\ 0\\ 0\end{pmatrix}\right)=\sum_{s\in\mathbb{F}_q^{*2}}\tau(0)=\frac{q-1}{2}.$$

□

5. A-invariant skew Hadamard difference sets

Proposition 5.1. *A subset $D\subseteq V\setminus\{0\}$ is a skew Hadamard difference set iff it satisfies the following conditions:*

(SH1) $-D\cap D=\emptyset$;
(SH2) $-D\cup D=V\setminus\{0\}$;
(SH3) $\chi_v(D)-\overline{\chi_v(D)}=\pm\iota q\sqrt{q}$ *for each* $v\in V^*\setminus\{0\}$.

Proof. If D satisfies (SH1)-(SH2), then $\chi_v(D)+\overline{\chi_v(D)}=-1$ for each $v\in V^*\setminus\{0\}$, Together with (SH3) this implies that $\chi_v(D)=\frac{1\pm\sqrt{-q^3}}{2}$ for each $v\in V^*\setminus\{0\}$. By [1], Lemma 2.5 D is a skew Hadamard difference set.

Vice versa, if D is a skew Hadamard difference set, then (SH1)-(SH2) follow directly from the definition. The condition (SH3) is a consequence of Lemma 2.5, [1]. □

Let $\mathfrak{D}$ denote the set of all A-invariant skew Hadamard difference sets, that is $D \in \mathfrak{D}$ iff D is a union of A-orbits. It follows from (SH1)-(SH2) that a subset $D \in \mathfrak{D}$ contains exactly one orbit from $\{O_i, -O_i\}$ for each $i \in I$. In other words, the intersection $D \cap (O_i \cup -O_i)$ is either O_i or $-O_i$. Therefore we can write $D \cap (O_i \cup -O_i) = \varepsilon(i)O_i$ where $\varepsilon(i) = \pm 1$. Thus any A-invariant skew Hadamard difference set is uniquely determined by a function $\varepsilon : I \to \{\pm 1\}$. In what follows we denote $D_\varepsilon := \bigcup_{i \in I} \varepsilon(i)O_i$.

Although there are 2^{q+2} functions from I into $\{\pm 1\}$, not every one of them yields a SHDS. A subset D_ε will be a SHDS iff it satisfies condition (SH3). Notice that

$$D_{-\varepsilon} = -D_\varepsilon, D_{-\varepsilon} \cap D_\varepsilon = \emptyset, D_{-\varepsilon} \cup D_\varepsilon = V \setminus \{0\}.$$

Thus D_ε is a SHDS iff $D_{-\varepsilon}$ is a SHDS (the complementary SHDS).

In order to describe all A-invariant SHDS we define $J_\varepsilon := \{i \in \mathbb{F}_q \,|\, \varepsilon(i) = 1\}$.

Theorem 5.2. *Let $\varepsilon : I \to \{\pm 1\}$ be an arbitrary function. Then $D_\varepsilon \in \mathfrak{D}$ iff $|J_\varepsilon| = \frac{q+\mu}{2}$ and $\varepsilon(\bullet) = \left(\frac{2}{p}\right)\mu$ where $\mu = \pm 1$.*

Proof. Pick an arbitrary vector $v \in V^* \setminus \{0\}$. Then

$$\chi_v(D_\varepsilon) - \overline{\chi_v(D_\varepsilon)} = \sum_{i \in I} \chi_v(\varepsilon(i)O_i) - \overline{\chi_v(\varepsilon(i)O_i)}$$

Taking into account that $\chi_v(-T) = \overline{\chi_v(T)}$ we may rewrite the above equality as follows

$$\chi_v(D_\varepsilon) - \overline{\chi_v(D_\varepsilon)} = \sum_{i \in I} \varepsilon(i)(\chi_v(O_i) - \overline{\chi_v(O_i)}) \tag{4}$$

Thus a subset D_ε will satisfy (SH3) (and, therefore, will be a SHDS) iff the above expression will be equal to $\pm \iota q\sqrt{q}$ for all $v \in V^* \setminus \{0\}$. The value of the above sum depend only on the orbit to which the vector v belongs. Moreover it follows from $\chi_{-v}(T) = \overline{\chi_v(T)}$ that it is enough to check (4) only for $v \in O_i^*, i \in I$.

Now we build a square matrix T of order $q+2$ the rows and columns of which are indexed by the elements of I and $T_{i,j}$ is the value $\chi_v(O_j) - \overline{\chi_v(O_j)}$ where $v \in O_i^*$.

Using this matrix one can reformulate the condition for ε to produce a skew Hadamard difference set. Namely, the function ε produces a skew Hadamard difference set iff $T\varepsilon^t$ is a column vector with entries $\pm \iota q\sqrt{q}$.

If $i, j \in \mathbb{F}_q$, then by (3) we obtain that

$$T_{i,j} = \begin{cases} (q-1)(\mathsf{z}_1 - \overline{\mathsf{z}_1}) & i + j = 0; \\ \mathsf{z}_2(1 + 2\mathsf{z}_1) - \overline{\mathsf{z}_2(1 + 2\mathsf{z}_1)} & i + j \neq 0 \end{cases} \tag{5}$$

where $\mathsf{z}_1 = \mathsf{z}^{\sigma(2)}$ and $\mathsf{z}_2 = \mathsf{z}^{\sigma(i+j)}$.

If $i + j = 0$, then $T_{i,j} = (q-1)\Delta^{\sigma(2)}$.

Assume now that $i + j \neq 0$.

If $\sigma(i + j) = \sigma(2)$, then $\mathsf{z}_2 = \mathsf{z}_1$ and

$$T_{i,j} = \mathsf{z}_1(1 + 2\mathsf{z}_1) - \overline{\mathsf{z}_1(1 + 2\mathsf{z}_1)} = (\mathsf{z}_1 - \overline{\mathsf{z}_1})(1 + 2(\mathsf{z}_1 + \overline{\mathsf{z}_1})) = \overline{\mathsf{z}_1} - \mathsf{z}_1.$$

If $\sigma(i + j) \neq \sigma(2)$, then $\mathsf{z}_2 = \overline{\mathsf{z}_1}$ and

$$T_{i,j} = \overline{\mathsf{z}_1}(1 + 2\mathsf{z}_1) - \mathsf{z}_1(1 + 2\overline{\mathsf{z}_1}) = \overline{\mathsf{z}_1} - \mathsf{z}_1.$$

Thus $T_{i,j} = \overline{\mathsf{z}_1} - \mathsf{z}_1 = -\Delta^{\sigma(2)}$ whenever $i + j \neq 0$.

Using Table 1 one can finally compute T. It is more convenient to replace T be the matrix T' obtained from T by row permuatation $i \mapsto -i, i \in \mathbb{F}_q$ (the rows and $\infty, \bullet$ are not moved). The matrix T' has the following block form

$$T' = \left(\begin{array}{c|c|c|c} & \mathbb{F}_q & \infty & \bullet \\ \hline \mathbb{F}_q & \Delta^{\sigma(2)}(q\mathbf{I}_q - \mathbf{J}_q) & \mathbf{0}^t & \Delta\mathbf{1}^t \\ \hline \infty & \mathbf{0} & q\Delta & 0 \\ \hline \bullet & q\Delta\mathbf{1} & 0 & 0 \end{array}\right)$$

where $\mathbf{0}$ and $\mathbf{1}$ are zero and all-one row vectors of length q; and $\mathbf{I}_q$,$\mathbf{J}_q$ are the identity and all-one matrices of size q. In order to compute the product $T'\varepsilon^t$ we write ε^t in a block form

$$\varepsilon^t = \begin{pmatrix} \varepsilon_0^t \\ \varepsilon(\infty) \\ \varepsilon(\bullet) \end{pmatrix}$$

where $\varepsilon_0 := \varepsilon_{\mathbb{F}_q}$ is the restriction of ε onto $\mathbb{F}_q$. In this notation $T'\varepsilon^t$ has the following form

(6)

$$\left(\begin{array}{c|c|c} \Delta^{\sigma(2)}(q\mathbf{I}_q - \mathbf{J}_q) & \mathbf{0}^t & \Delta\mathbf{1}^t \\ \hline \mathbf{0} & q\Delta & 0 \\ \hline q\Delta\mathbf{1} & 0 & 0 \end{array}\right) \begin{pmatrix} \varepsilon_0^t \\ \varepsilon(\infty) \\ \varepsilon(\bullet) \end{pmatrix} = \begin{pmatrix} q\Delta^{\sigma(2)}\varepsilon_0^t + (\Delta\varepsilon(\bullet) - \Delta^{\sigma(2)}\mu)\mathbf{1}^t \\ q\Delta\varepsilon(\infty) \\ q\Delta\mu \end{pmatrix},$$

where μ is the coordinate sum of the vector ε_0. The entries of the right side of (6) are equal to $\pm\iota q\sqrt{q} = \pm q\Delta$ iff $\mu = \pm 1$ and $\Delta\varepsilon(\bullet) = \Delta^{\sigma(2)}\mu$. Together with $\Delta^{\sigma(2)} = \left(\frac{2}{p}\right)\Delta$ we obtain that $\varepsilon(\bullet) = \left(\frac{2}{p}\right)\mu$. To finish the proof it remains to notice that $|J_\varepsilon| = \frac{q+\mu}{2}$. □

An elementary counting shows that there are $4\binom{q}{\frac{q+1}{2}}$ functions satisfying the conditions of Theorem 5.2. Therefore we obtain $4\binom{q}{\frac{q+1}{2}} > 2^{q+2}/q$ skew Hadamard difference sets (including complements). Notice that two distinct difference sets may be equivalent, and, therefore, produce isomorphic designs. For example, any element $g \in \mathbf{N}_{\mathsf{Aut}(V)}(A)$ permutes the A-orbits, and therefore, also permutes the elements of $\mathfrak{D}$ mapping each set $D \in \mathfrak{D}$ to an equivalent one.

6. Isomorphisms between the translation designs

The main result of this section solves the isomorphism problem for translation designs generated by difference sets from $\mathfrak{D}$.

Theorem 6.1. *Given $D, D' \in \mathfrak{D}$, the designs $\mathsf{Dev}(D)$ and $\mathsf{Dev}(D')$ are isomorphic iff they are isomorphic by an element of $\mathbf{N}_{\mathsf{Aut}(V)}(A)$.*

This Theorem gives us a lower bound for the number of non-isomorphic designs obtained from the difference sets constructed in the previous sections. The number of distinct designs is $4\binom{q}{\frac{q+1}{2}}$. Each design is A-invariant. Therefore each orbit of $\mathbf{N}_{\mathsf{Aut}(V)}(A)$ contains at most $[\mathbf{N}_{\mathsf{Aut}(V)}(A) : A]$ designs. In the next subsection we'll show that $|\mathbf{N}_{\mathsf{Aut}(V)}(A)| = n(q-1)^2q^2$. Therefore $[\mathbf{N}_{\mathsf{Aut}(V)}(A) : A] = 2n(q-1)q$ implying that the number of non-isomorphic designs is at least

$$\frac{4\binom{q}{\frac{q+1}{2}}}{2n(q-1)q} > \frac{2^{q+2}/q}{2nq(q-1)} > \frac{2^{q+1}}{q^4}.$$

6.1. **Computation of $\mathbf{N}_{\mathsf{Aut}(V)}(A)$.** In order to describe the group in the title we'll write each automorphism of V as 3×3-matrix the entries of which are elements of the $\mathbb{F}_p$-algebra $\mathsf{End}(\mathbb{F}_q)$ (the algebra of $\mathbb{F}_p$-linear endomorphisms of $\mathbb{F}_q$). The field $\mathbb{F}_q$ is considered as a subalgebra of $\mathsf{End}(\mathbb{F}_q)$ where the field element α is identified with the endomorphism $x\mapsto \alpha x, x\in\mathbb{F}_q$.

For each $\alpha,\beta\in\mathbb{F}_q^*$ and $\ell\in\mathsf{End}(\mathbb{F}_q)$ we set

$$K(\alpha,\beta):=\begin{pmatrix}\alpha & 0 & 0\\ 0 & \alpha\beta & 0\\ 0 & 0 & \alpha\beta^2\end{pmatrix}, \hat{\ell}:=\begin{pmatrix}1 & 0 & \ell\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

Notice that $K:=\{K(\alpha,\beta)\,|\,\alpha,\beta\in\mathbb{F}_q^*\}$, $L:=\{\hat{\ell}\,|\,\ell\in\mathsf{End}(\mathbb{F}_q)\}$ are abelian subgroups of $\mathsf{Aut}(V)$. The first one is isomorphic to $\mathbb{Z}_{q-1}\times\mathbb{Z}_{q-1}$ while the second one is an elementary abelian group isomorphic to $(\mathsf{End}(\mathbb{F}_q),+)$. A direct check shows that both subgroups normalize E. Moreover $[E,L]=1$.

Another subgroup of $\mathsf{Aut}(V)$ normalizing E comes from field automorphisms. More precisely each $f\in\mathsf{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ induces an $\mathbb{F}_p$-linear automorphism of V: $(x,y,z)\mapsto(f(x),f(y),f(z))$. We denote this automorphism by the same letter f. The subgroup of $\mathsf{Aut}(V)$ consisting of all Galois automorphisms $f\in\mathsf{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ will be denoted as F. So, F is a cyclic subgroup of $\mathsf{Aut}(V)$ of order n. A direct check shows that

$$[F,E]\le E, [K,E]\le E, [L,E]=1, [F,K]\le K, [F,L]\le L, [K,L]\le L$$

In particular, any two subgroups from the list $\{E,F,K,L\}$ are permutable. Therefore $FKEL$ is a subgroup of $\mathsf{Aut}(V)$. It's order is equal to $|F||K||E||L|=n(q-1)^2q^{n+1}$.

Proposition 6.2. *It holds that*

(1) $\mathbf{N}_{\mathsf{Aut}(V)}(E)=FKLE$;
(2) $\mathbf{N}_{\mathsf{Aut}(V)}(SE)=FKEU$ *where* $U:=\{\hat{\gamma}\,|\,\gamma\in\mathbb{F}_q\}$;

Proof. Part (1). The subgroups $\mathbf{C}_V(E)=\{(x,0,0)^t|x\in\mathbb{F}_q\}, [E,V]=\{(x,y,0)^t|x,y\in\mathbb{F}_q\}$ are $\mathbf{N}_{\mathsf{Aut}(V)}(E)$-invariant. Therefore each element $N\in\mathbf{N}_{\mathsf{Aut}(V)}(E)$ has the following form

$$N=\begin{pmatrix}a & b & c\\ 0 & d & e\\ 0 & 0 & f\end{pmatrix} \text{ where } a,d,f\in\mathsf{GL}(\mathbb{F}_q) \text{ and } b,c,e\in\mathsf{End}(\mathbb{F}_q).$$

Since $E\cong\mathbb{F}_q$, there exists an automorphism $n\in\mathsf{GL}(\mathbb{F}_q)$ such that

$$\forall_{\alpha\in\mathbb{F}_q}\ NE(\alpha)N^{-1}=E(n(\alpha)) \iff NE(\alpha)=E(n(\alpha))N.$$

After multiplication and equating we obtain the following equations which hold for each $\alpha\in\mathbb{F}_q$

$$(7)\qquad \begin{cases} a\alpha &= n(\alpha)d,\\ d\alpha &= n(\alpha)f,\\ \frac{1}{2}a\alpha^2+b\alpha &= \frac{1}{2}n(\alpha)^2f+n(\alpha)e\end{cases} \iff \begin{cases} a\alpha &= n(\alpha)d,\\ d\alpha &= n(\alpha)f,\\ b\alpha &= n(\alpha)e\end{cases}$$

After substitution $\alpha = 1$ we obtain $a = \beta d, d = \beta f, b = \beta e$ where $\beta := n(1)$. Now the equations (7) yield us

$$\forall_{\alpha\in\mathbb{F}_q}\left\{\begin{array}{rcl} d\alpha d^{-1} & = & \beta^{-1}n(\alpha),\\ f\alpha f^{-1} & = & \beta^{-1}n(\alpha),\\ e\alpha e^{-1} & = & \beta^{-1}n(\alpha)\end{array}\right. \tag{8}$$

Thus each of the elements e, d, f normalizes the subalgebra $\mathbb{F}_q$ of $\mathsf{End}(\mathbb{F}_q)$. Therefore each of them may be written in a form $e = \epsilon e_0, d = \delta d_0, f = \phi f_0$ where $e_0, d_0, f_0 \in \mathsf{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and $\epsilon, \delta, \phi \in \mathbb{F}_q$. It follows from (8) that conjugation by a, d, f induce the same automorphism of $\mathbb{F}_q$. Therefore $e_0 = d_0 = f_0$. Thus we obtain the following

$$a = \beta d = \beta^2 f = \beta^2\phi f_0; d = \beta f = \beta\phi f_0; e = \epsilon f_0, b = \beta e = \beta\epsilon f_0$$

implying that

$$N = \left(\begin{array}{ccc} \beta^2\phi f_0 & \beta\epsilon f_0 & c\\ 0 & \beta\phi f_0 & \beta\epsilon f_0\\ 0 & 0 & \phi f_0\end{array}\right) \in FKEL$$

Part (2). Since SE is a coprime product of S and E, we conclude $\mathbf{N}_{\mathsf{Aut}(V)}(SE) = \mathbf{N}_{\mathsf{Aut}(V)}(S) \cap \mathbf{N}_{\mathsf{Aut}(V)}(E) = \mathbf{N}_{FKEL}(S)$. Since F, K and E normalize S, we can write $\mathbf{N}_{FKEL}(S) = (FKE)\mathbf{N}_L(S)$. So, it remains to find $\mathbf{N}_L(S)$. A straightforward computation shows that $\mathbf{N}_L(S) = U$.

□

6.2. **An automorphism group of a concrete translation design.** Let us fix a function $\varepsilon : I \to \{\pm 1\}$ such that $D := D_\varepsilon \in \mathfrak{D}$. We also set $J := J_\varepsilon$, $\mathcal{D} := \mathsf{Dev}(V, D)$, $G := \mathsf{Aut}(\mathcal{D})$. We also denote by F_p a unique Sylow p-subgroup of F.

Since F normalizes U, it's Sylow p-subgroup F_p normalizes U as well. Therefore $F_pU = UF_p$ is a subgroup of $\mathsf{Aut}(V)$. Let $Q := (UF_p)_D$ be a setwise stabilizer of D in UF_p. Since $UF_p \cong \mathbb{F}_q \rtimes F_p$, the group Q is a subgroup of $\mathbb{F}_q \rtimes F_p$.

Proposition 6.3. *The subgroup Q consists of all products $\hat{\alpha}f, \alpha \in \mathbb{F}_q, f \in F_p$ which satisfies the condition $f(J) + \alpha = J$.*

Proof. It follows from the definition of U that for each $\hat{\alpha} \in U, \alpha \in \mathbb{F}_q$ and $i \in \mathbb{F}_q$ the following equalities hold

$$\hat{\alpha}O_i = O_{i+\alpha}, \hat{\alpha}O_\infty = O_\infty, \hat{\alpha}O_\bullet = O_\bullet.$$

Also for each $f \in F$

$$fO_i = O_{f(i)}, fO_\infty = O_\infty, fO_\bullet = O_\bullet.$$

Hence

$$\hat{\alpha}fD = \left(\bigcup_{i\in F_q}\varepsilon(i)O_{f(i)+\alpha}\right)\bigcup\varepsilon(\infty)O_\infty\bigcup\varepsilon(\bullet)O_\bullet.$$

Therefore $\hat{\alpha}fD = D$ holds if and only if $\varepsilon(f(i) + \alpha) = \varepsilon(i)$ for each $i \in \mathbb{F}_q$. This is equivalent to $f(J) + \alpha = J$. □

The subgroup $Q \cap U$ consists of those $\hat{\alpha}, \alpha \in \mathbb{F}_q$ which satisfy $J + \alpha = J$. Thus J is a union of $\langle\alpha\rangle$-cosets. Since $|J|$ is coprime to p, we conclude that $Q \cap U$ is trivial. This implies that Q is embedded into F_p. In particular, Q is a cyclic p-group.

Since F and U normalize EV_+, the group Q normalizes EV_+ too. Therefore QEV_+ is a subgroup of G.

Theorem 6.4. *QEV_+ is a Sylow p-subgroup of G.*

In order to prove this Theorem we first need some properties of QEV_+. Recall that the Thompson subgroup $\mathbf{J}(P)$ of a p-group P is the subgroup generated by all elementary abelian subgroups of P of maximal order. Clearly $\mathbf{J}(P)$ is characteristic in P. Also the subgroup $\mathbf{J}_2(P)$ defined by $\mathbf{J}_2(P)/\mathbf{J}(P) = \mathbf{J}(P/\mathbf{J}(P))$ is characteristic in P.

Proposition 6.5. *Every elementary abelian subgroup of EV_+ of order $\geq q^2p$ is contained in V_+. In particular, $\mathbf{J}(EV_+) = V_+$.*

Proof. Let T be an elementary abelian subgroup of EV_+ of order $\geq q^2p$. Assume towards a contradiction that $T \not\leq V_+$. It follows from $|V_+ \cap T| \geq qp$ that $|\mathbf{C}_{V_+}(t)| \geq qp$ for each $t \in T$. Take $t \in T \setminus V_+$. Then $t = ev_+$ for some $e \in E \setminus \{1\}$ and $v \in V$ implying $\mathbf{C}_{V_+}(t) = \mathbf{C}_{V_+}(e)$. But any non-identical element of E centralizes q elements of V_+. A contradiction. □

Proposition 6.6. *If $g \in FEV_+ \setminus V_+$, then the index of $\mathbf{C}_{V_+}(g)$ in V_+ is at least p^2.*

Proof. Let $g = fev_+$ be an element from $FEV_+ \setminus V_+$ where $f \in F, e \in E, v \in V$. Then $\mathbf{C}_{V_+}(g) = \mathbf{C}_{V_+}(fe) = (\mathsf{Fix}_V(fe))_+$. Thus we have to prove that $[V : \mathsf{Fix}_V(fe)] \geq p^2$.

If $f = 1$, then $\mathsf{Fix}_V(e) = W$ where $W := \{(x, 0, 0,)^t \mid x \in \mathbb{F}_q\}$ and we are done

If $f \neq 1$, then the intersection $\mathsf{Fix}_V(fe) \cap W = \mathsf{Fix}_W(f)$ consists of those vectors $(x, 0, 0,)^t$ which satisfy $f(x) = x$. Hence

$$[V : \mathsf{Fix}_V(fe)] \geq [W : \mathsf{Fix}_W(fe)] = [W : \mathsf{Fix}_W(f)] = [\mathbb{F}_q : \mathsf{Fix}_{\mathbb{F}_q}(f)] > p^2.$$

□

Proposition 6.7. *$\mathbf{J}(QEV_+) = V_+, \mathbf{J}(QE) = E$ and $\mathbf{J}_2(QEV_+) = EV_+$*

Proof. Let Y be an elementary abelian subgroup of QEV_+ of maximal order. Then $|Y| \geq q^3$. We are going to prove that $Y = V_+$.

Since $QEV_+/(EV_+) \cong Q$ is cyclic and Y is elementary abelian, the image of Y in the factor-group $QEV_+/(EV_+)$ has order at most p. Therefore $|Y \cap EV_+| \geq |Y|/p \geq q^3/p$. If $q > p$, then $|Y \cap EV_+| \geq q^2p$. If $q = p$, then Q is trivial and $|Y \cap EV_+| = |Y| \geq q^3$. Thus in any case $|Y \cap EV_+| \geq q^2p$. By Proposition 6.5 $Y \cap EV_+ \leq V_+$ implying that $|Y \cap V_+| = |Y \cap EV_+| \geq |Y|/p \geq q^3/p$. If Y is contained in V_+, then $Y = V_+$ and we are done. If $Y \not\leq V_+$, then an element $y \in Y \setminus V_+$ centralizes at least q^3/p elements of V_+, contrary to Proposition 6.6. Thus $Y = V_+$, and, consequently, $\mathbf{J}(QEV_+) = V_+$

Consider now the factor-group $QEV_+/V_+ \cong QE$. The group E is isomorphic to $\mathbb{F}_q$, while Q is a cyclic p-group acting on E as a group of field automorphisms. In this case E is the only elementary abelian p-subgroup of maximal order. Therefore $\mathbf{J}(QE) = E$ and $\mathbf{J}_2(QEV_+) = EV_+$. □

Proof of Theorem 6.4.
Let P be a Sylow p-subgroup of G containing QEV_+ and $N := \mathbf{N}_P(QEV_+)$. By Proposition 6.7 the subgroups V_+ and EV_+ are characteristic in QEV_+. Therefore both V_+ and EV_+ are normal in N. This implies that $N \leq \mathbf{N}_{\mathsf{Sym}(V)}(V_+) = \mathsf{Aut}(V)V_+$ where $\mathsf{Aut}(V) \cong GL_{3n}(p)$. Since $EV_+ \trianglelefteq N$, the point stabilizer N_0 satisfies the following inequality $E \trianglelefteq N_0 \leq \mathsf{Aut}(V)$. By Proposition 6.2 $N_0 \leq FKLE$.

Since N_0 is a p-group, it is contained in a Sylow's p-subgroup of $FKLE$. W.l.o.g. we may assume that $N_0 \leq F_pLE$. It follows from $E \leq N_0 \leq (F_pL)E$ that $N_0 = (N_0 \cap F_pL)E$. In order to prove Theorem 6.4 it is sufficient to show that $N_0 \cap F_pL = Q$. Notice that the inclusion $Q \leq N_0$ follows from the inclusion $QEV_+ \leq N$.

The rest of the proof is given in the following two statements.

Proposition 6.8. *N_0 fixes D setwise.*

PROOF. First, notice that we can assume that $O_\bullet \subseteq D$ (otherwise we can replace D by $-D$).

The subgroup N_0 permutes the blocks of $\mathcal{D}$ containing 0. The number of such blocks is $\frac{q-1}{2}$ - coprime to p. Since N_0 is a p-group, it fixes at least one of these blocks, say $D+w$. It follows from $E \leq N_0$ that $D+w$ is also fixed by E. Since E fixes 0, D and $D+w$, it fixes also w (Proposition 2.2, part (2)). Therefore $w \in \mathsf{Fix}_V(E) = W := \{(x,0,0)^t \mid x \in \mathbb{F}_q\}$,

Since N normalizes EV_+, the center $\mathbf{Z}(EV_+) = \mathbf{C}_E(V_+) = W_+$ is normal in N. Therefore the orbits of W_+ (which are the cosets of W) form an imprimitivity system of N. Hence the block W is N_0-invariant and N_0 fixes $(D+w) \cap W = (D \cap W) + w = O_\bullet + w$ setwise. The restriction N_0^W is contained in the automorphism group of the subdesign $\mathcal{D}_W := \{D' \cap W \mid D' \in \mathcal{D}\}$ (which is a Paley design over $\mathbb{F}_q$). Since $N_0 \leq FEL$ and $FELO_\bullet = O_\bullet$, the subgroup N_0 stabilizes $O_\bullet$ setwise. Since $Q_\bullet \subset D$, both $O_\bullet$ and $O_\bullet + w$ are blocks of the design $\mathcal{D}_W$ fixed by N_0. By Proposition 2.2, part (2) applied to $\mathcal{D}_W$ we conclude that $w^{N_0} = w$. Now Proposition 2.2, part (1) yields us $D^{N_0} = D$. □

Proposition 6.9. *$Q = N_0 \cap (F_pL)$.*

PROOF. Since F normalizes L, we can replace $N_0 \cap (F_pL)$ by $N_0 \cap (LF_p)$. Let $\hat{\ell} f, \ell \in \mathsf{End}(\mathbb{F}_q), f \in \mathsf{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ be an element of the intersection $N_0 \cap (LF_p)$. By Proposition 6.8 $\hat{\ell} f D = D$. Pick arbitrary $i \in \mathbb{F}_q$ and $s \in \mathbb{F}_q^{*2}$. By definition of D the vector $v := \varepsilon(i) \begin{pmatrix} s\left(\frac{x^2}{2} + i\right) \\ sx \\ s \end{pmatrix}$ is contained in D. Therefore

$$\hat{\ell} f v \in D \iff \varepsilon(i) \begin{pmatrix} f(s)\left(\frac{(f(x))^2}{2} + f(i)\right) + \ell(f(s)) \\ f(s)f(x) \\ f(s) \end{pmatrix} \in D$$

Since $\begin{pmatrix} f(s)\left(\frac{(f(x))^2}{2} + f(i)\right) + \ell(f(s)) \\ f(s)f(x) \\ f(s) \end{pmatrix} \in O_{i'}$ where $i' = f(i) + f(s)^{-1}\ell(f(s))$,

we conclude that $D \cap \varepsilon(i)O_{i'} \neq \emptyset$ .But $D \cap (O_{i'} \cup -O_{i'}) = \varepsilon(i')O_{i'}$. Therefore $\varepsilon(i') = \varepsilon(i)$ implying that $\varepsilon(i) = \varepsilon(f(i) + f(s)^{-1}\ell(f(s)))$ holds for all $i \in \mathbb{F}_q$ and $s \in \mathbb{F}_q^{*2}$. This implies that $f(J) + s^{-1}\ell(s) = J$ holds for each $s \in \mathbb{F}_q^{*2}$. If $s^{-1}\ell(s) \neq t^{-1}\ell(t)$ for some $t, s \in \mathbb{F}_q^{*2}$, then $J + u = J$ where $u = s^{-1}\ell(s) - t^{-1}\ell(t)$. In this case J would be a union of $\langle u \rangle$-cosets which is impossible because $|J| = (q \pm 1)/2$. Therefore $s^{-1}\ell(s), s \in \mathbb{F}_q^{*2}$ is constant, or, in other words, $\ell(s) = \alpha s, s \in \mathbb{F}_q^{*2}$ for some $\alpha \in \mathbb{F}_q$. Since ℓ is $\mathbb{F}_p$-linear, we conclude that $\ell(x) = \alpha x, x \in \mathbb{F}_q$, or, equivalently, $\ell = \alpha$.

Thus $\hat{\ell} \in U$ and $\hat{\ell}f \in UF_p$. Since $f(J) + \alpha = J$, Proposition 6.3 implies that $\hat{\ell}f$ stabilizes D setwise, that is $\hat{\ell}f \in Q$. □

6.3. **Proof of Theorem 6.1.** Let $D_\varepsilon, D_\delta \in \mathfrak{D}$ be two difference sets for which the designs $\mathcal{D}_\varepsilon := \mathsf{Dev}(V, D_\varepsilon), \mathcal{D}_\delta := \mathsf{Dev}(V, D_\delta)$ are isomorphic. Then there exists a permutation $g \in \mathsf{Sym}(V)$ such that $\mathcal{D}_\delta^g = \mathcal{D}_\varepsilon$. Clearly that $G_\delta^g = G_\varepsilon$ where G_δ, G_ε are the automorphism groups of the corresponding designs. This implies that $(Q_\delta EV_+)^g$ is a Sylow p-subgroup of G_ε. Since $Q_\varepsilon EV_+$ is also a Sylow p-subgroup of G_ε, there exists $h \in G_\varepsilon$ such that $(Q_\delta EV_+)^{gh} = Q_\varepsilon EV_+$. Hence $\mathbf{J}_2((Q_\delta EV_+)^{gh}) = \mathbf{J}_2(Q_\varepsilon EV_+)$. It follows from the definition of $\mathbf{J}_2$ and $\mathbf{J}$ that $\mathbf{J}((Q_\delta EV_+)^{gh}) = \mathbf{J}(Q_\delta EV_+)^{gh}$ and $\mathbf{J}_2((Q_\delta EV_+)^{gh}) = \mathbf{J}_2(Q_\delta EV_+)^{gh}$. Applying now Proposition 6.7 we obtain that $V_+^{gh} = V_+$ and $(EV_+)^{gh} = EV_+$. It follows from $\mathsf{Fix}(E) \neq \emptyset$ that $\mathsf{Fix}(E^{gh}) \neq \emptyset$. Therefore $E^{gh} \leq (EV_+)_v$ for some $v \in V$. Together with $|(EV_+)_0| = |E| = q^3$ we obtain that E^{gh} is a point stabilizer of EV_+. Therefore there exists $b \in EV_+$ such that $E^{ghb} = E$. Denoting $g' := ghb$ we obtain that $E^{g'} = E, V_+^{g'} = V_+$, $\mathcal{D}_\delta^{g'} = \mathcal{D}_\varepsilon^{hb} = \mathcal{D}_\varepsilon$ and $G_\delta^{g'} = G_\varepsilon$. Thus $g' \in \mathbf{N}_{\mathsf{Sym}(V)}(V_+) \cap \mathbf{N}_{\mathsf{Sym}(V)}(E) = \mathbf{N}_{\mathsf{Aut}(V)V_+}(E)$. The factor-group $\mathbf{N}_{\mathsf{Aut}(V)V_+}(E)V_+/V_+$ is embedded into $\mathbf{N}_{\mathsf{Aut}(V)}(E) = FKLE$. Together with $FKLE \leq \mathbf{N}_{\mathsf{Aut}(V)V_+}(E)$ we obtain that $\mathbf{N}_{\mathsf{Aut}(V)V_+}(E) = FKLE(\mathbf{N}_{\mathsf{Aut}(V)V_+}(E) \cap V_+) = FKLE\mathbf{N}_{V_+}(E)$. A direct computation shows that $\mathbf{N}_{V_+}(E) = W_+$ where $W = \{(x, 0, 0)^t \,|\, x \in \mathbb{F}_q\}$. Thus $g' \in FKLEW_+$.

We claim that $S^{g'}$ and S are conjugate by an element of EW_+. First we notice that $S^{g'} \leq FKLEW_+$ because $S \leq FKLEW_+$. The subgroup S is a cyclic subgroup of $\mathbf{N}_{\mathsf{Aut}(V)V_+}(E)$ of order $\frac{q-1}{2}$ which centralizes E. Since $E^{g'} = E$, $(V_+)^{g'} = V_+$ and $[S, E] = 1$, the subgroup $S^{g'}$ centralizes E too. Thus the subgroup $T := \langle S, S^{g'} \rangle$ is contained in $\mathbf{C}_{FKLEW_+}(E)$. Since LEW_+ centralizes E, we can write $\mathbf{C}_{FKLEW_+}(E) = \mathbf{C}_{FK}(E)LEW_+$. A direct computation shows that $\mathbf{C}_{FK}(E) = K_0$ where $K_0 := \{K(\alpha, 1) \,|\, \alpha \in \mathbb{F}_q^*\}$. Therefore $T \leq K_0LEW_+$. Since $[L, E] = [E, W_+] = [L, W_+] = 1$, the subgroup LEW_+ is elementary abelian. The images of S and $S^{g'}$ in the factor-group $K_0LEW_+/(LEW_+) \cong K_0 \cong \mathbb{F}_q^*$ coincide. Therefore $T = S(T \cap LEW_+)$. Since LEW_+-orbit of 0 coincides with $W = W_+0$, we can write that $T \cap LEW \leq (T \cap LEW_+)_0W_+$. Since LEW_+ centralizes E and normalizes V_+, the subgroup $(T \cap LEW_+)_0$ normalizes EV_+. Therefore $(T \cap LEW_+)_0EV_+$ is a p-subgroup of G_ε. Hence it is contained in the Sylow's p-subgroup P of G_ε. It follows from Theorem 6.4 and Proposition 6.7 that the order of a maximal elementary abelian subgroup of the point stabilizer P_0 is equal to q. The subgroup $(T \cap LEW_+)_0E$ is contained in P_0 and is elementary abelian of order at least $q = |E|$. Therefore $(T \cap LEW_+)_0E = E$ implying that $(T \cap LEW_+)_0 \leq E$, and, consequently, $T \cap LEW_+ \leq EW_+$.

Finally $T \leq SEW_+$ implying $S^{g'} \leq SEW_+$. Both S and $S^{g'}$ are Hall p'-subgroups of SEW_+. Therefore they are conjugate in SEW_+, say by an element t. Since $t \in SEW_+$, it is an automorphism of $\mathcal{D}_\varepsilon$ implying that $\mathcal{D}_\delta^{g't} = \mathcal{D}_\varepsilon$. But the element $g't$ normalizes E,S and V_+. Therefore $g't \in \mathbf{N}_{\mathsf{Aut}(V)V_+}(SE)$. Since $g't$ normalizes SE, it fixes $\mathsf{Fix}_V(SE)$ setwise. But $\mathsf{Fix}_V(SE)$ contains a unique point, namely 0. Hence $g't$ fixes 0 implying $g't \in \mathbf{N}_{\mathsf{Aut}(V)}(SE)$. □

7. Concluding Remarks.

The first time I heard about Feng's result was this August when I met Qing Xiang at Rogla's Conference (Slovenia). Next month Bill Kantor communicated me about this result independently, he also conjectured that the construction proposed by Feng should also work for non-abelian groups of order q^3, where q is 3 modulo 4. Finally provided information as well as fruitful discussions with Bill during his stay in Israel served for me as the source of inspiration to work on this project. I am very grateful to Bill Kantor for his attention and fruitful ideas expressed by him. The author also thanks Misha Klin for helpful phone conversations related to this project. My special thanks to Matan Ziv-Av who made computer computations (using GAP) for the group $\mathbb{Z}_7^3$ and thus confirmed and clarified experimentally the initial idea, which was generalized later for arbitrary q.

It seems that a modification of the construction given here could also work in the case when q congruent 1 modulo 4. In this case one should obtain exponentially many partial difference sets with Paley parameters.

References

[1] G. Weng, L. Hu. Some results on skew Hadamard difference sets. Des. Codes Cryptogr. (2009) 50, pp 93-105.
[2] C. Ding, J. Yuan. A family of skew Hadamard difference sets. J. Combin. Theory (A) 113, 15261535 (2006).
[3] C. Ding, Z. Wang, Q. Xiang. Skew Hadamard difference sets from Ree-Tits slice symplectic spreads in $PG(3, 3^{2h+1})$. J. Combin. Theory Ser. A 114, 867887 (2007)
[4] G.Weng , W. Qiu, Z. Wang, Q. Xiang . Pseudo-Paley graphs and skew Hadamard difference sets from presemifields Des. Codes Cryptogr. (2007) 44:4962
[5] T. Feng. Non-abelian skew Hadamard difference sets fixed by a prescribed automorphism. J. Combin. Theory Ser. A (2010) (in press), doi:10.1016/j.jcta.2009.11.004

Netanya Academic College, Netanya, Israel
E-mail address: muzy@netanya.ac.il