GLASNIK MATEMATIČKI
Vol. 42(62)(2007), 257 – 272

A SERIES OF FINITE GROUPS AND RELATED SYMMETRIC DESIGNS

Dieter Held, Mario-Osvin Pavčević and Marcel Schmidt
Johannes Gutenberg-Universität, Germany, University of Zagreb, Croatia and Martin-Luther-Universität Halle-Wittenberg, Germany

Abstract. For any odd prime power $q = p^e$ we study a certain solvable group G of order $q^2 \cdot (\frac{q-1}{2})^2 \cdot 2$ and construct from its internal structure a symmetric design $\mathcal{D}$ with parameters $(2q^2+1, q^2, \frac{q^2-1}{2})$ on which G acts as an automorphism group. As a consequence we find that the full automorphism group of $\mathcal{D}$ contains a subgroup of order $|G| \cdot e^2$.

1. A Series of Groups

Let $q = p^e$ be an odd prime power. Starting from an infinite series of finite solvable groups of order $q^2 \cdot (\frac{q-1}{2})^2 \cdot 2$, we are going to construct an infinite series of symmetric designs (compare with [3, Theorem 1, p. 624]). For an introduction to design theory we refer the reader to [1] or [4]. Before going into details, we want to state the main theorem.

Main Theorem. *For every odd prime power $q = p^e$, there is a symmetric design $\mathcal{D}$ with parameters $(2q^2+1, q^2, \frac{q^2-1}{2})$ possessing an automorphism group A of order $q^2 \cdot (\frac{q-1}{2})^2 \cdot e^2 \cdot 2$ which is isomorphic to the subdirect product of the affine semilinear group $A\Gamma L_1(q)$ with itself with respect to a certain epimorphism $\psi : A\Gamma L_1(q) \to Z_2$ from $A\Gamma L_1(q)$ into the cyclic group Z_2, i.e. $A \cong A\Gamma L_1(q)\ \mathrm{sdp}_{(\psi,\psi)}\ A\Gamma L_1(q)$.*

We are going to prove this theorem in two steps. First we construct the symmetric design $\mathcal{D}$, whose existence is claimed in Theorem 3.1, and after that we give a detailed description of the group A and show that A is an automorphism group of $\mathcal{D}$ as stated in Corollary 3.2.

2000 *Mathematics Subject Classification.* 05E20, 05B05.
Key words and phrases. Symmetric design, automorphism group.
The second author is supported by a DAAD grant.

Let $\mathbb{F}_q$ be the Galois field with q elements. As usual, we denote by $\mathbb{F}_q^+$ the additive group of $\mathbb{F}_q$ which is isomorphic to the elementary abelian group of order q and by $\mathbb{F}_q^*$ the multiplicative group of $\mathbb{F}_q$ which is isomorphic to the cyclic group of order $q-1$. Put $\mathbb{F}_q^\# = \mathbb{F}_q \setminus \{0\}$. Thus $\mathbb{F}_q^\#$ is the set of all non-zero elements of $\mathbb{F}_q$. By 0, we denote the identity element of $\mathbb{F}_q^+$, and by 1, the identity element of $\mathbb{F}_q^*$. Let $D_+ = \mathbb{F}_q^2 \setminus \{0\} = \{x^2 \mid x \in \mathbb{F}_q^\#\}$ be the set of all non-zero squares in $\mathbb{F}_q$ and $D_- = \mathbb{F}_q^\# \setminus D_+$ the set of all non-squares in $\mathbb{F}_q$. We remark that the elements of D_+ form a subgroup of index 2 in $\mathbb{F}_q^*$ and thus D_- is a coset of D_+ in $\mathbb{F}_q^*$, which means $D_- = D_+t$, for any $t \in D_-$.

Consider the semidirect product $\mathbb{F}_q^+ \rtimes_\rho \mathbb{F}_q^*$ of $\mathbb{F}_q^+$ by $\mathbb{F}_q^*$ with respect to the monomorphism

$$\rho : \mathbb{F}_q^* \to Aut(\mathbb{F}_q^+),\ a \mapsto (\mathbb{F}_q^+ \to \mathbb{F}_q^+, x \mapsto ax)$$

from $\mathbb{F}_q^*$ into $Aut(\mathbb{F}_q^+)$, where ρ simply indicates that $\mathbb{F}_q^*$ acts on $\mathbb{F}_q^+$ by multiplication. Denote this extension, as usual, by $AGL_1(q)$, the 1-dimensional affine general linear group over $\mathbb{F}_q$, and note that the image of $\mathbb{F}_q^*$ under ρ in $Aut(\mathbb{F}_q^+) \cong GL_e(p)$ is usually called a Singer cycle. It should be mentioned that the subgroup of index 2 of the Singer cycle operates in exactly three orbits of respective lengths 1, $\frac{q-1}{2}$, and $\frac{q-1}{2}$ on $\mathbb{F}_q^+$, which we may identify with $\{0\}$, D_+ and D_- assuming that $\mathbb{F}_q^+$ is equipped with the multiplicative structure inherited from the field $\mathbb{F}_q$. Clearly, there is a unique normal subgroup N of index 2 in $AGL_1(q)$. Let $\varphi : AGL_1(q) \to AGL_1(q)/N$ be the natural epimorphism from our affine linear group onto its factor group modulo N of order 2. Then, the subdirect product of $AGL_1(q)$ with itself with respect to φ is given by

$$AGL_1(q)\ \mathrm{sdp}_{(\varphi,\varphi)}\ AGL_1(q) = \{(x,y) \in AGL_1(q) \times AGL_1(q) \mid \varphi(x) = \varphi(y)\}.$$

From now on, we denote this group by G and its maximal normal p-subgroup by $Q = O_p(G)$. In the following lemma, we list the main obvious properties of the groups just introduced without providing a proof.

Lemma 1.1. *The group G is solvable and its subgroup Q is a direct product of two elementary abelian normal subgroups V and W of G of order q. If $q > 3$, V and W are the only nontrivial normal subgroups of G contained in Q. Furthermore, Q is an elementary abelian self-centralizing normal Sylow p-subgroup of G of order q^2. The group G is a split extension of Q by a complement H of order $\frac{(q-1)^2}{2}$, which is a self-normalizing abelian subgroup of type $(\frac{q-1}{2}, q-1)$. The complement H acts on the set of its G-conjugates $ccl_G(H)$ in five orbits of respective lengths $1, q-1, q-1, \frac{(q-1)^2}{2}, \frac{(q-1)^2}{2}$.*

Remark that we may identify the elements of the conjugacy class $ccl_G(H)$ – which is equal to $ccl_Q(H)$ – with the elements of Q, since $\mathbb{N}_G(H) = H$. According to the previous lemma, we obtain precisely five H-orbits on the elements of Q, of respective lengths $1, q-1, q-1, \frac{(q-1)^2}{2}, \frac{(q-1)^2}{2}$. Throughout the following calculations we identify Q with the outer direct sum $\mathbb{F}_q^+ \oplus \mathbb{F}_q^+$. Therefore, $V = \mathbb{F}_q^+ \oplus \{0\}$ and $W = \{0\} \oplus \mathbb{F}_q^+$. In this sense, the five orbits of H on Q, which we denote by $O_0, O_1, \ldots, O_4$, may be expressed as follows:

$$\begin{aligned}
O_0 &= ccl_H\big((0,0)\big) = \{(0,0)\}\,,\\
O_1 &= ccl_H\big((1,0)\big) = (\mathbb{F}_q^{\#}, \{0\}) = \{(v,0) \mid v \in \mathbb{F}_q^{\#}\}\,,\\
O_2 &= ccl_H\big((0,1)\big) = (\{0\}, \mathbb{F}_q^{\#}) = \{(0,w) \mid w \in \mathbb{F}_q^{\#}\}\,,\\
O_3 &= ccl_H\big((1,1)\big) = (D_+, D_+) \cup (D_-, D_-)\\
&\qquad\qquad\quad = \{(v,w) \mid v,w \in D_+\} \cup \{(v,w) \mid v,w \in D_-\}\,,\\
O_4 &= ccl_H\big((1,t)\big) = (D_+, D_-) \cup (D_-, D_+)\\
&\qquad\qquad\quad = \{(v,w) \mid v \in D_+, w \in D_-\} \cup \{(v,w) \mid v \in D_-, w \in D_+\}\,,
\end{aligned}$$

where by $t \in D_-$ we denote a fixed non-square element from $\mathbb{F}_q$.

To be able to reduce the calculations which follow below, we shall make use of certain outer automorphisms of the group G. Let $Y = AGL_1(q) \wr_{reg} Z_2$ be the wreath product of $AGL_1(q)$ with Z_2. Since G is a subdirect product of $AGL_1(q)$ with itself, we may – in a natural way – consider G as a subgroup of the base group $Y^{\natural} = AGL_1(q) \times AGL_1(q)$ of the wreath product Y, which itself may be treated as a subgroup of the full automorphism group $Aut(G)$ of G. Choose an element $\tau \in AGL_1(q) \setminus N$, where N is the unique subgroup of index 2 in $AGL_1(q)$. It can be easily seen that $Y/G \cong Z_2 \times Z_2$. Thus, $Y/G = \langle \alpha G, \beta G \rangle$, where $\alpha, \beta \in Y$ are defined by $(x,y)^\alpha = (y,x)$, $(x,y)^\beta = (x^\tau, y)$, for all $(x,y) \in Y^{\natural}$. Obviously, α and β act on the orbits O_i, for $i \in \{0, \ldots, 4\}$, in the following way:

$$\begin{aligned}
O_1^\alpha &= O_2, \quad O_i^\alpha = O_i, \;\; i \in \{0,3,4\},\\
O_3^\beta &= O_4, \quad O_i^\beta = O_i, \;\; i \in \{0,1,2\},\\
O_1^{\alpha\beta} &= O_2, \; O_3^{\alpha\beta} = O_4, \;\; O_0^{\alpha\beta} = O_0.
\end{aligned}$$

2. Some Formulas

Throughout the following calculations we retain the notation introduced in the previous section.

Lemma 2.1. *Let $d \in \mathbb{F}_q$ and $t \in D_-$.*
(i) If $q \equiv 1 \pmod 4$, then:

$$|(D_+ + d) \cap D_-| = |(D_- + d) \cap D_+| = \begin{cases} 0, & \textit{for } d = 0 \\ \frac{q-1}{4}, & \textit{for } d \neq 0 \end{cases}, \tag{2.1}$$

$$|(D_+ + d) \cap D_+| = |(D_- + dt) \cap D_-| = \begin{cases} \frac{q-5}{4}, & \textit{for } d \in D_+ \\ \frac{q-1}{2}, & \textit{for } d = 0 \\ \frac{q-1}{4}, & \textit{for } d \in D_- \end{cases} . \tag{2.2}$$

(ii) If $q \equiv 3 \pmod 4$*, then:*

$$|(D_+ + d) \cap D_+| = |(D_- + d) \cap D_-| = \begin{cases} \frac{q-1}{2}, & \textit{for } d = 0 \\ \frac{q-3}{4}, & \textit{for } d \neq 0 \end{cases} , \tag{2.3}$$

$$|(D_+ + d) \cap D_-| = |(D_- + dt) \cap D_+| = \begin{cases} \frac{q+1}{4}, & \textit{for } d \in D_+ \\ 0, & \textit{for } d = 0 \\ \frac{q-3}{4}, & \textit{for } d \in D_- \end{cases} . \tag{2.4}$$

PROOF. (i) First note that for any $x \in D_+$, $y \in D_-$, and for any $z \in D_+$, one has $xz \in D_+$ and $yz \in D_-$. Thus, if an element $d \in \mathbb{F}_q^{\#}$ can be written as a difference $d = x - y$ with $x \in D_+$ and $y \in D_-$, then by multiplying with an element $z \in D_+$ one gets the element $dz = xz - yz$ as a difference of elements $xz \in D_+$ and $yz \in D_-$. Hence, all elements from D_+, as well as those from D_-, can be written in the same number of ways as a difference $x - y$, $x \in D_+$, $y \in D_-$. It remains to show that an element of D_+ has as many such representations as an element of D_-. Since $q \equiv 1 \pmod 4$, we have $-1 \in D_+$. If $d = x - y \in D_+$, with $x \in D_+$ and $y \in D_-$, and if $t \in D_-$, then $dt = xt - yt = -yt - (-xt)$, where $-yt \in D_+$ and $-xt \in D_-$, turns out to be the corresponding representation. That's why there is always the same number, say $\lambda' \in \mathbb{N}$, of possibilities to write an element of $\mathbb{F}_q^{\#}$ as a difference $x - y$ of two elements $x \in D_+$ and $y \in D_-$. Clearly, this is also true for the differences of the form $y - x$. By counting $|D_+ \times D_-|$ in two different ways, we get $\left(\frac{q-1}{2}\right)^2 = (q-1)\lambda'$, which results in $\lambda' = \frac{q-1}{4}$, and proves the equation (2.1). Equation (2.2) now follows easily from (2.1). Namely: The element 0 is contained in $D_+ + d$ if and only if $d \in D_+$. So, $|(D_+ + d) \cap (D_- \cup \{0\})|$ is either equal to $\lambda' + 1$ for $d \in D_+$ or to λ' for $d \in D_-$. As

$$|(D_+ + d) \cap D_+| = |D_+ + d| - |(D_+ + d) \cap (D_- \cup \{0\})|,$$

we get the result.

(ii) In the case $q \equiv 3 \pmod 4$, it is a well known fact, that D_+ and D_- are so-called Paley difference sets for the parameters $\left(q, \frac{q-1}{2}, \frac{q-3}{4}\right)$ in the elementary abelian group $\mathbb{F}_q^+$ (see for example [1, Theorem 1.12, p. 302]). Hence, (2.3) follows immediately. With almost the same methods as in (i), one can now also verify equation (2.4). □

For the purpose of calculating intersections of representatives of block orbits of the symmetric designs which we want to construct later, we shall calculate intersections for some specific subsets of the direct sum $\mathbb{F}_q^+ \oplus \mathbb{F}_q^+$.

Lemma 2.1 from above facilitates this task and here we will demonstrate this giving an example in the case where $q \equiv 1 \pmod 4$.

$$
\begin{aligned}
&|[(D_+, D_+) + (v,w)] \cap (D_+, D_+)| \\
&\qquad = |(D_+ + v, D_+ + w) \cap (D_+, D_+)| \\
&\qquad = |(D_+ + v) \cap D_+| \cdot |(D_+ + w) \cap D_+| \\
&\qquad = \left\{ \begin{array}{ll} \frac{q-5}{4}, & \text{for } v \in D_+ \\ \frac{q-1}{2}, & \text{for } v = 0 \\ \frac{q-1}{4}, & \text{for } v \in D_- \end{array} \right\} \cdot \left\{ \begin{array}{ll} \frac{q-5}{4}, & \text{for } w \in D_+ \\ \frac{q-1}{2}, & \text{for } w = 0 \\ \frac{q-1}{4}, & \text{for } w \in D_- \end{array} \right\} \\
&\qquad = \begin{cases} \left(\frac{q-5}{4}\right)^2, & \text{for } v, w \in D_+ \\ \left(\frac{q-1}{4}\right)^2, & \text{for } v, w \in D_- \\ \frac{q-5}{4}\frac{q-1}{4}, & \text{for } v \in D_+,\, w \in D_- \text{ or } v \in D_-,\, w \in D_+ \\ \frac{q-5}{4}\frac{q-1}{2}, & \text{for } v \in D_+,\, w = 0 \text{ or } v = 0,\, w \in D_+ \\ \frac{q-1}{4}\frac{q-1}{2}, & \text{for } v = 0,\, w \in D_- \text{ or } v \in D_-,\, w = 0 \end{cases} .
\end{aligned}
$$

Similarly, repeated application of the previous lemma leads directly to the following results, which will prove to be crucial for our further investigations.

LEMMA 2.2. *(i) If* $q \equiv 1 \pmod 4$, *then:*

$$
\begin{aligned}
&|[(D_+, D_+) + (v,w)] \cap (D_+, D_+)| \\
&\qquad = \begin{cases} \left(\frac{q-5}{4}\right)^2, & \textit{for } v, w \in D_+ \\ \left(\frac{q-1}{4}\right)^2, & \textit{for } v, w \in D_- \\ \frac{q-5}{4}\frac{q-1}{4}, & \textit{for } v \in D_+,\, w \in D_- \textit{ or } v \in D_-,\, w \in D_+ \\ \frac{q-5}{4}\frac{q-1}{2}, & \textit{for } v \in D_+,\, w = 0 \textit{ or } v = 0,\, w \in D_+ \\ \frac{q-1}{4}\frac{q-1}{2}, & \textit{for } v = 0,\, w \in D_- \textit{ or } v \in D_-,\, w = 0 \end{cases} , \\
&|[(D_-, D_-) + (v,w)] \cap (D_-, D_-)| \\
&\qquad = \begin{cases} \left(\frac{q-1}{4}\right)^2, & \textit{for } v, w \in D_+ \\ \left(\frac{q-5}{4}\right)^2, & \textit{for } v, w \in D_- \\ \frac{q-5}{4}\frac{q-1}{4}, & \textit{for } v \in D_+,\, w \in D_- \textit{ or } v \in D_-,\, w \in D_+ \\ \frac{q-1}{4}\frac{q-1}{2}, & \textit{for } v \in D_+,\, w = 0 \textit{ or } v = 0,\, w \in D_+ \\ \frac{q-5}{4}\frac{q-1}{2}, & \textit{for } v = 0,\, w \in D_- \textit{ or } v \in D_-,\, w = 0 \end{cases} , \\
&|[(D_+, D_+) + (v,w)] \cap (D_-, D_-)| \\
&\qquad = \begin{cases} \left(\frac{q-1}{4}\right)^2, & \textit{for } v \neq 0,\, w \neq 0 \\ 0, & \textit{for } v = 0 \textit{ or } w = 0 \end{cases} ,
\end{aligned}
$$

$$|[(D_-,D_-)+(v,w)]\cap(D_+,D_+)| = \begin{cases} \left(\frac{q-1}{4}\right)^2, & \textit{for } v\neq 0,\ w\neq 0\\ 0, & \textit{for } v=0 \textit{ or } w=0\end{cases},$$

$$|[(D_+,D_+)+(v,w)]\cap(D_+,D_-)| = \begin{cases} \frac{q-5}{4}\frac{q-1}{4}, & \textit{for } v\in D_+,\ w\neq 0\\ \left(\frac{q-1}{4}\right)^2, & \textit{for } v\in D_-,\ w\neq 0\\ \frac{(q-1)^2}{8}, & \textit{for } v=0,\ w\neq 0\\ 0, & \textit{for } w=0\end{cases},$$

$$|[(D_+,D_+)+(v,w)]\cap(D_-,D_+)| = \begin{cases} \frac{q-5}{4}\frac{q-1}{4}, & \textit{for } v\neq 0,\ w\in D_+\\ \left(\frac{q-1}{4}\right)^2, & \textit{for } v\neq 0,\ w\in D_-\\ \frac{(q-1)^2}{8}, & \textit{for } v\neq 0,\ w=0\\ 0, & \textit{for } v=0\end{cases},$$

$$|[(D_-,D_-)+(v,w)]\cap(D_+,D_-)| = \begin{cases} \left(\frac{q-1}{4}\right)^2, & \textit{for } v\neq 0,\ w\in D_+\\ \frac{q-5}{4}\frac{q-1}{4}, & \textit{for } v\neq 0,\ w\in D_-\\ \frac{(q-1)^2}{8}, & \textit{for } v\neq 0,\ w=0\\ 0, & \textit{for } v=0\end{cases},$$

$$|[(D_-,D_-)+(v,w)]\cap(D_-,D_+)| = \begin{cases} \left(\frac{q-1}{4}\right)^2, & \textit{for } v\in D_+,\ w\neq 0\\ \frac{q-5}{4}\frac{q-1}{4}, & \textit{for } v\in D_-,\ w\neq 0\\ \frac{(q-1)^2}{8}, & \textit{for } v=0,\ w\neq 0\\ 0, & \textit{for } w=0\end{cases}.$$

(ii) If $q\equiv 3 \pmod 4$*, then:*

$$|[(D_+,D_+)+(v,w)]\cap(D_+,D_+)| = \begin{cases} \left(\frac{q-3}{4}\right)^2, & \textit{for } v\neq 0,\ w\neq 0\\ \frac{q-1}{2}\frac{q-3}{4}, & \textit{for } v=0 \textit{ or } w=0\end{cases},$$

$$|[(D_-,D_-)+(v,w)]\cap(D_-,D_-)| = \begin{cases} \left(\frac{q-3}{4}\right)^2, & \textit{for } v\neq 0,\ w\neq 0\\ \frac{q-1}{2}\frac{q-3}{4}, & \textit{for } v=0 \textit{ or } w=0\end{cases},$$

$$|[(D_+,D_+)+(v,w)]\cap(D_-,D_-)| = \begin{cases} \left(\frac{q+1}{4}\right)^2, & \textit{for } v,w\in D_+\\ \left(\frac{q-3}{4}\right)^2, & \textit{for } v,w\in D_-\\ \frac{q+1}{4}\frac{q-3}{4}, & \textit{for } v\in D_+,\, w\in D_- \textit{ or } v\in D_-,\, w\in D_+\\ 0, & \textit{for } v=0 \textit{ or } w=0\end{cases},$$

$$|[(D_-,D_-)+(v,w)]\cap(D_+,D_+)| = \begin{cases} \left(\frac{q-3}{4}\right)^2, & \textit{for } v,w\in D_+\\ \left(\frac{q+1}{4}\right)^2, & \textit{for } v,w\in D_-\\ \frac{q+1}{4}\frac{q-3}{4}, & \textit{for } v\in D_+,\, w\in D_- \textit{ or } v\in D_-,\, w\in D_+\\ 0, & \textit{for } v=0 \textit{ or } w=0\end{cases},$$

$$|[(D_+,D_+)+(v,w)]\cap(D_+,D_-)| = \begin{cases} \frac{q-3}{4}\frac{q+1}{4}, & \textit{for } v\neq 0,\, w\in D_+\\ \left(\frac{q-3}{4}\right)^2, & \textit{for } v\neq 0,\, w\in D_-\\ \frac{q-1}{2}\frac{q+1}{4}, & \textit{for } v=0,\, w\in D_+\\ \frac{q-1}{2}\frac{q-3}{4}, & \textit{for } v=0,\, w\in D_-\\ 0, & \textit{for } w=0\end{cases},$$

$$|[(D_+,D_+)+(v,w)]\cap(D_-,D_+)| = \begin{cases} \frac{q-3}{4}\frac{q+1}{4}, & \textit{for } v\in D_+,\, w\neq 0\\ \left(\frac{q-3}{4}\right)^2, & \textit{for } v\in D_-,\, w\neq 0\\ \frac{q-1}{2}\frac{q+1}{4}, & \textit{for } v\in D_+,\, w=0\\ \frac{q-1}{2}\frac{q-3}{4}, & \textit{for } v\in D_-,\, w=0\\ 0, & \textit{for } v=0\end{cases},$$

$$|[(D_-,D_-)+(v,w)]\cap(D_+,D_-)| = \begin{cases} \left(\frac{q-3}{4}\right)^2, & \textit{for } v\in D_+,\, w\neq 0\\ \frac{q+1}{4}\frac{q-3}{4}, & \textit{for } v\in D_-,\, w\neq 0\\ \frac{q-1}{2}\frac{q-3}{4}, & \textit{for } v\in D_+,\, w=0\\ \frac{q-1}{2}\frac{q+1}{4}, & \textit{for } v\in D_-,\, w=0\\ 0, & \textit{for } v=0\end{cases},$$

$$|[(D_-,D_-)+(v,w)]\cap(D_-,D_+)| = \begin{cases} \left(\frac{q-3}{4}\right)^2, & \textit{for } v\neq 0,\ w\in D_+ \\ \frac{q+1}{4}\frac{q-3}{4}, & \textit{for } v\neq 0,\ w\in D_- \\ \frac{q-1}{2}\frac{q-3}{4}, & \textit{for } v=0,\ w\in D_+ \\ \frac{q-1}{2}\frac{q+1}{4}, & \textit{for } v=0,\ w\in D_- \\ 0, & \textit{for } w=0 \end{cases}.$$

Having the equations of the above Lemma 2.2 at our disposal we are now able to prove the following proposition.

Proposition 2.3. *For every $(v,w)\in Q\setminus\{(0,0)\}$ one has:*

(2.5)

$$|(O_1+(v,w))\cap O_1| = \begin{cases} q-2, & \textit{for } w=0 \\ 0, & \textit{for } w\neq 0 \end{cases},$$

(2.6)

$$|(O_2+(v,w))\cap O_2| = \begin{cases} q-2, & \textit{for } v=0 \\ 0, & \textit{for } v\neq 0 \end{cases},$$

(2.7)

$$|(O_3+(v,w))\cap O_3| = \frac{q-1}{2}\frac{q-3}{2} + \begin{cases} 1, & \textit{for } v,w\in D_+ \textit{ or } v,w\in D_- \\ 0, & \textit{otherwise} \end{cases},$$

(2.8)

$$|(O_4+(v,w))\cap O_4| = \frac{q-1}{2}\frac{q-3}{2} + \begin{cases} 1, & \textit{for } v\in D_+,\ w\in D_- \\ & \textit{or } v\in D_-,\ w\in D_+ \\ 0, & \textit{otherwise} \end{cases},$$

(2.9)

$$|(O_1+(v,w))\cap O_2| = |(O_2+(v,w))\cap O_1| = \begin{cases} 1, & \textit{for } v\neq 0,\ w\neq 0 \\ 0, & \textit{otherwise} \end{cases},$$

(2.10)

$$|(O_1+(v,w))\cap O_3| = |(O_3+(v,w))\cap O_1| = \begin{cases} \frac{q-3}{2}, & \textit{for } v,w\in D_+ \textit{ or } v,w\in D_- \\ 0, & \textit{for } w=0 \\ \frac{q-1}{2}, & \textit{for } v\in D_+,\ w\in D_- \textit{ or } v\in D_-,\ w\in D_+ \textit{ or } v=0 \end{cases},$$

(2.11)
$$|(O_1+(v,w))\cap O_4| = |(O_4+(v,w))\cap O_1| = \begin{cases} \frac{q-1}{2}, & \textit{for } v,w\in D_+ \textit{ or } v,w\in D_- \textit{ or } v=0 \\ 0, & \textit{for } w=0 \\ \frac{q-3}{2}, & \textit{for } v\in D_+,\, w\in D_- \textit{ or } v\in D_-,\, w\in D_+ \end{cases},$$

(2.12)
$$|(O_2+(v,w))\cap O_3| = |(O_3+(v,w))\cap O_2| = \begin{cases} \frac{q-3}{2}, & \textit{for } v,w\in D_+ \textit{ or } v,w\in D_- \\ 0, & \textit{for } v=0 \\ \frac{q-1}{2}, & \textit{for } v\in D_+,\, w\in D_- \textit{ or } v\in D_-,\, w\in D_+ \textit{ or } w=0 \end{cases},$$

(2.13)
$$|(O_2+(v,w))\cap O_4| = |(O_4+(v,w))\cap O_2| = \begin{cases} \frac{q-1}{2}, & \textit{for } v,w\in D_+ \textit{ or } v,w\in D_- \textit{ or } w=0 \\ 0, & \textit{for } v=0 \\ \frac{q-3}{2}, & \textit{for } v\in D_+,\, w\in D_- \textit{ or } v\in D_-,\, w\in D_+ \end{cases},$$

(2.14)
$$|(O_3+(v,w))\cap O_4| = |(O_4+(v,w))\cap O_3| = \begin{cases} \frac{q-1}{2}\frac{q-3}{2}, & \textit{for } v\neq 0,\, w\neq 0 \\ \frac{(q-1)^2}{4}, & \textit{for } v=0 \textit{ or } w=0 \end{cases}.$$

Proof. Throughout the following calculations we shall be using the formulas from Lemma 2.2 which depend on q being congruent to either 1 or 3 modulo 4.

First we consider the cardinality of all symmetric intersections, i.e. intersections between a set O_i and the shifted set $O_i+(v,w)$ for $i\in\{1,2,3,4\}$.

$$\begin{aligned} |(O_1+(v,w))\cap O_1| &= \left|[(\mathbb{F}_q^{\#},\{0\})+(v,w)]\cap(\mathbb{F}_q^{\#},\{0\})\right| \\ &= \left|(\mathbb{F}_q^{\#}+v,\{w\})\cap(\mathbb{F}_q^{\#},\{0\})\right| = \begin{cases} |\mathbb{F}_q\setminus\{0,v\}| = q-2, & \text{for } w=0 \\ 0, & \text{for } w\neq 0 \end{cases}, \end{aligned}$$

$$\begin{aligned} &|(O_2+(v,w))\cap O_2| \\ &\quad = |(O_1^{\alpha}+(w,v)^{\alpha})\cap O_1^{\alpha}| = |(O_1+(w,v))^{\alpha}\cap O_1^{\alpha}| \\ &\quad = |(O_1+(w,v))\cap O_1| = \begin{cases} q-2, & \text{for } v=0 \\ 0, & \text{for } v\neq 0 \end{cases}. \end{aligned}$$

In a similar way, using the symmetry provided by the automorphisms α and β, it can be shown that we do not need to prove explicitly the equations (2.8), (2.11), (2.12) and (2.13), once we have proved the equations (2.7) and (2.10).

If $q \equiv 1 \pmod 4$, we get for (2.7):

$$
\begin{aligned}
&|(O_3 + (v,w)) \cap O_3| \\
&\quad = \big|\big([(D_+,D_+) \cup (D_-,D_-)] + (v,w)\big) \cap [(D_+,D_+) \cup (D_-,D_-)]\big| \\
&\quad = \big|\big((D_+,D_+) + (v,w)\big) \cap (D_+,D_+)\big| + \big|\big((D_+,D_+) + (v,w)\big) \cap (D_-,D_-)\big| \\
&\qquad + \big|\big((D_-,D_-) + (v,w)\big) \cap (D_+,D_+)\big| + \big|\big((D_-,D_-) + (v,w)\big) \cap (D_-,D_-)\big| \\
&\quad = \begin{cases}
\left(\frac{q-5}{4}\right)^2 + 2\cdot\left(\frac{q-1}{4}\right)^2 + \left(\frac{q-1}{4}\right)^2 = \frac{(q-1)(q-3)}{4} + 1, & \text{for } v,w \in D_+ \\
& \text{or } v,w \in D_- \\
2\cdot\frac{q-5}{4}\frac{q-1}{4} + 2\cdot\left(\frac{q-1}{4}\right)^2 = \frac{(q-1)(q-3)}{4}, & \text{for } v \in D_+,\, w \in D_- \\
& \text{or } v \in D_-,\, w \in D_+ \\
\frac{q-5}{4}\cdot\frac{q-1}{2} + 2\cdot 0 + \frac{q-1}{4}\frac{q-1}{2} = \frac{(q-1)(q-3)}{4}, & \text{for } v = 0 \text{ or } w = 0
\end{cases} \\
&\quad = \frac{q-1}{2}\frac{q-3}{2} + \begin{cases} 1, & \text{for } v,w \in D_+ \text{ or } v,w \in D_- \\ 0, & \text{otherwise} \end{cases}.
\end{aligned}
$$

If $q \equiv 3 \pmod 4$, the same expression becomes:

$$
\begin{aligned}
&|(O_3 + (v,w)) \cap O_3| \\
&\quad = \big|\big([(D_+,D_+) \cup (D_-,D_-)] + (v,w)\big) \cap [(D_+,D_+) \cup (D_-,D_-)]\big| \\
&\quad = \big|\big((D_+,D_+) + (v,w)\big) \cap (D_+,D_+)\big| + \big|\big((D_+,D_+) + (v,w)\big) \cap (D_-,D_-)\big| \\
&\qquad + \big|\big((D_-,D_-) + (v,w)\big) \cap (D_+,D_+)\big| + \big|\big((D_-,D_-) + (v,w)\big) \cap (D_-,D_-)\big| \\
&\quad = \begin{cases}
2\cdot\left(\frac{q-3}{4}\right)^2 + \left(\frac{q+1}{4}\right)^2 + \left(\frac{q-3}{4}\right)^2 = \frac{(q-1)(q-3)}{4} + 1, & \text{for } v,w \in D_+ \\
& \text{or } v,w \in D_- \\
2\cdot\left(\frac{q-3}{4}\right)^2 + 2\cdot\frac{q+1}{4}\frac{q-3}{4} = \frac{(q-1)(q-3)}{4}, & \text{for } v \in D_+,\, w \in D_- \\
& \text{or } v \in D_-,\, w \in D_+ \\
2\cdot\frac{q-1}{2}\cdot\frac{q-3}{4} + 2\cdot 0 = \frac{(q-1)(q-3)}{4}, & \text{for } v = 0 \text{ or } w = 0
\end{cases} \\
&\quad = \frac{q-1}{2}\frac{q-3}{2} + \begin{cases} 1, & \text{for } v,w \in D_+ \text{ or } v,w \in D_- \\ 0, & \text{otherwise} \end{cases}.
\end{aligned}
$$

Now, we go on proving all equations which involve asymmetric intersections.

$$
\begin{aligned}
|(O_1 + (v,w)) \cap O_2| &= \big|[(\mathbb{F}_q^{\#},\{0\}) + (v,w)] \cap (\{0\},\mathbb{F}_q^{\#})\big| \\
&= \big|(\mathbb{F}_q \setminus \{v\},\{w\}) \cap (\{0\},\mathbb{F}_q^{\#})\big| = \begin{cases} 1, & \text{for } v \neq 0,\, w \neq 0 \\ 0, & \text{for } v = 0 \text{ or } w = 0 \end{cases}.
\end{aligned}
$$

Before we continue to prove the remaining formulas, we point out that it is sufficient to prove only one equation for each pair (2.9)–(2.14). We illustrate this by examining the counterpart of the above equation.

$$\begin{aligned}
&|(O_2 + (v, w)) \cap O_1| = |O_2 \cap (O_1 - (v, w))| \\
&\quad = |O_2 \cap (O_1 + (-v, -w))| = |(O_1 + (v, w)) \cap O_2|.
\end{aligned}$$

We are now going to verify equation (2.10):

$$\begin{aligned}
&|(O_1 + (v, w)) \cap O_3| = \left|[(\mathbb{F}_q^{\#}, \{0\}) + (v, w)] \cap [(D_+, D_+) \cup (D_-, D_-)]\right| \\
&\quad = \left|(\mathbb{F}_q \setminus \{v\}, \{w\}) \cap [(D_+, D_+) \cup (D_-, D_-)]\right| = \begin{cases} |D_+ \setminus \{v\}|, & \text{for } w \in D_+ \\ 0, & \text{for } w = 0 \\ |D_- \setminus \{v\}|, & \text{for } w \in D_- \end{cases} \\
&\quad = \begin{cases} \frac{q-3}{2}, & \text{for } v, w \in D_+ \text{ or } v, w \in D_- \\ 0, & \text{for } w = 0 \\ \frac{q-1}{2}, & \text{for } v \in D_+,\ w \in D_- \text{ or } v \in D_-,\ w \in D_+ \text{ or } v = 0 \end{cases} .
\end{aligned}$$

If $q \equiv 1 \pmod 4$, we get for (2.14):

$$\begin{aligned}
&|(O_3 + (v, w)) \cap O_4| \\
&\quad = \left|\big([(D_+, D_+) \cup (D_-, D_-)] + (v, w)\big) \cap [(D_+, D_-) \cup (D_-, D_+)]\right| \\
&\quad = \left|\big((D_+, D_+) + (v, w)\big) \cap (D_+, D_-)\right| + \left|\big((D_+, D_+) + (v, w)\big) \cap (D_-, D_+)\right| \\
&\qquad + \left|\big((D_-, D_-) + (v, w)\big) \cap (D_+, D_-)\right| + \left|\big((D_-, D_-) + (v, w)\big) \cap (D_-, D_+)\right| \\
&\quad = \begin{cases} 2 \cdot \frac{q-5}{4}\frac{q-1}{4} + 2 \cdot \left(\frac{q-1}{4}\right)^2 = \frac{(q-1)(q-3)}{4}, & \text{for } v, w \in D_+ \\ 2 \cdot \frac{q-5}{4}\frac{q-1}{4} + 2 \cdot \left(\frac{q-1}{4}\right)^2 = \frac{(q-1)(q-3)}{4}, & \text{for } v, w \in D_- \\ 2 \cdot \frac{q-5}{4}\frac{q-1}{4} + 2 \cdot \left(\frac{q-1}{4}\right)^2 = \frac{(q-1)(q-3)}{4}, & \text{for } v \in D_+,\ w \in D_- \\ 2 \cdot \frac{q-5}{4}\frac{q-1}{4} + 2 \cdot \left(\frac{q-1}{4}\right)^2 = \frac{(q-1)(q-3)}{4}, & \text{for } v \in D_-,\ w \in D_+ \\ 2 \cdot \frac{(q-1)^2}{8} + 2 \cdot 0 = \frac{(q-1)^2}{4}, & \text{for } v = 0,\ w \neq 0 \\ 2 \cdot \frac{(q-1)^2}{8} + 2 \cdot 0 = \frac{(q-1)^2}{4}, & \text{for } v \neq 0,\ w = 0 \end{cases} \\
&\quad = \begin{cases} \frac{q-1}{2}\frac{q-3}{2}, & \text{for } v \neq 0,\ w \neq 0 \\ \frac{(q-1)^2}{4}, & \text{for } v = 0 \text{ or } w = 0 \end{cases} .
\end{aligned}$$

If $q \equiv 3 \pmod 4$, the same expression becomes:

$$\begin{aligned}
&|(O_3 + (v, w)) \cap O_4| \\
&\quad = \left|\big([(D_+, D_+) \cup (D_-, D_-)] + (v, w)\big) \cap [(D_+, D_-) \cup (D_-, D_+)]\right| \\
&\quad = \left|\big((D_+, D_+) + (v, w)\big) \cap (D_+, D_-)\right| + \left|\big((D_+, D_+) + (v, w)\big) \cap (D_-, D_+)\right| \\
&\qquad + \left|\big((D_-, D_-) + (v, w)\big) \cap (D_+, D_-)\right| + \left|\big((D_-, D_-) + (v, w)\big) \cap (D_-, D_+)\right|
\end{aligned}$$

$$= \begin{cases} 2 \cdot \frac{q+1}{4}\frac{q-3}{4} + 2 \cdot \left(\frac{q-3}{4}\right)^2 = \frac{(q-1)(q-3)}{4}, & \text{for } v, w \in D_+ \\ 2 \cdot \frac{q+1}{4}\frac{q-3}{4} + 2 \cdot \left(\frac{q-3}{4}\right)^2 = \frac{(q-1)(q-3)}{4}, & \text{for } v, w \in D_- \\ 2 \cdot \frac{q+1}{4}\frac{q-3}{4} + 2 \cdot \left(\frac{q-3}{4}\right)^2 = \frac{(q-1)(q-3)}{4}, & \text{for } v \in D_+,\, w \in D_- \\ 2 \cdot \frac{q+1}{4}\frac{q-3}{4} + 2 \cdot \left(\frac{q-3}{4}\right)^2 = \frac{(q-1)(q-3)}{4}, & \text{for } v \in D_-,\, w \in D_+ \\ \frac{q-1}{2}\frac{q+1}{4} + \frac{q-1}{2}\frac{q-3}{4} + 2 \cdot 0 = \frac{(q-1)^2}{4}, & \text{for } v = 0,\, w \in D_+ \\ \frac{q-1}{2}\frac{q+1}{4} + \frac{q-1}{2}\frac{q-3}{4} + 2 \cdot 0 = \frac{(q-1)^2}{4}, & \text{for } v = 0,\, w \in D_- \\ \frac{q-1}{2}\frac{q+1}{4} + \frac{q-1}{2}\frac{q-3}{4} + 2 \cdot 0 = \frac{(q-1)^2}{4}, & \text{for } v \in D_+,\, w = 0 \\ \frac{q-1}{2}\frac{q+1}{4} + \frac{q-1}{2}\frac{q-3}{4} + 2 \cdot 0 = \frac{(q-1)^2}{4}, & \text{for } v \in D_-,\, w = 0 \end{cases}$$

$$= \begin{cases} \frac{q-1}{2}\frac{q-3}{2}, & \text{for } v \neq 0,\, w \neq 0 \\ \frac{(q-1)^2}{4}, & \text{for } v = 0 \text{ or } w = 0 \end{cases}.$$

□

3. The Series of Designs

Remember that we have denoted the maximal normal p-subgroup of G by Q and have identified it with $\mathbb{F}_q^+ \oplus \mathbb{F}_q^+$. The subgroup Q splits into 5 G-orbits under conjugation. Using the notation previously introduced we put

$$Q = O_0 \cup O_1 \cup O_2 \cup O_3 \cup O_4.$$

Take two further copies of Q and denote them by Q' and Q''. We consider Q, Q', and Q'' to be pairwise disjoint. As we did for Q, we put

$$Q' = O'_0 \cup O'_1 \cup O'_2 \cup O'_3 \cup O'_4 \text{ and } Q'' = O''_0 \cup O''_1 \cup O''_2 \cup O''_3 \cup O''_4.$$

Here, the O'_i and the O''_i play the same role for Q' and Q'', respectively, as the O_i do for Q. With that set-up we are able to define the following sets:

$$B_0 = Q', \quad B_1 = O_0 \cup O'_1 \cup O'_3 \cup O''_2 \cup O''_4 \quad \text{and} \quad B_2 = O'_2 \cup O'_4 \cup O''_0 \cup O''_2 \cup O''_4.$$

Further, we define the orbits of these blocks, which we get by adding to them the elements of Q as follows:

$$\mathcal{B}_i = B_i^Q = \{B_i + (v, w) \mid (v, w) \in Q\}, \;\; i \in \{0, 1, 2\},$$

where

$$B_i + (v, w) = \{(x + v, y + w) \mid (x, y) \in B_i\}.$$

When computing the sum $(x, y) + (v, w)$, the reader should be aware of the fact that the result $(x + v, y + w)$ belongs to the same copy of Q as (x, y). For the lengths of these block orbits we get $|\mathcal{B}_0| = 1$, $|\mathcal{B}_1| = |Q| = q^2$ and $|\mathcal{B}_2| = |Q| = q^2$.

THEOREM 3.1. *Let $\mathcal{P} = O_0 \cup Q' \cup Q''$ be the set of points and $\mathcal{B} = \mathcal{B}_0 \cup \mathcal{B}_1 \cup \mathcal{B}_2$ the set of blocks of a finite incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \in)$. Then $\mathcal{D}$ is a symmetric design with parameters $(2q^2+1, q^2, \frac{q^2-1}{2})$.*

PROOF. Clearly, $|\mathcal{P}| = |\mathcal{B}| = v = 2q^2+1$. As $|B_i| = q^2$, for $i \in \{0,1,2\}$, it is obvious that $|B| = k = q^2$ for each block $B \in \mathcal{B}$. It remains only to show that the intersection of any two different blocks from the set $\mathcal{B}$ consists of precisely $\lambda = \frac{q^2-1}{2}$ points. To do this we take advantage of the equations from Proposition 2.3. Obviously, it suffices to determine these cardinalities for the following intersections. Take first two blocks from $\mathcal{B}_1$. One gets:

$$\begin{aligned}
&|(B_1 + (v,w)) \cap B_1| \\
&\quad = \big|\big(O_0 + (v,w)\big) \cap O_0\big| + \big|\big([O_1' \cup O_3'] + (v,w)\big) \cap [O_1' \cup O_3']\big| \\
&\qquad + \big|\big([O_2'' \cup O_4''] + (v,w)\big) \cap [O_2'' \cup O_4'']\big| \\
&\quad = 1 + |(O_1 + (v,w)) \cap O_1| + |(O_1 + (v,w)) \cap O_3| \\
&\qquad + |(O_3 + (v,w)) \cap O_1| + |(O_3 + (v,w)) \cap O_3| \\
&\qquad + |(O_2 + (v,w)) \cap O_2| + |(O_2 + (v,w)) \cap O_4| \\
&\qquad + |(O_4 + (v,w)) \cap O_2| + |(O_4 + (v,w)) \cap O_4| \\
&\quad = \frac{q^2-1}{2}, \ \ \forall\, (v,w) \in Q \setminus \{(0,0)\}.
\end{aligned}$$

For two different blocks from $\mathcal{B}_2$ the calculation looks as follows:

$$\begin{aligned}
|(B_2 + (v,w)) \cap B_2| &= \big|\big([O_2' \cup O_4'] + (v,w)\big) \cap [O_2' \cup O_4']\big| \\
&\quad + \big|\big([O_0'' \cup O_2'' \cup O_4''] + (v,w)\big) \cap [O_0'' \cup O_2'' \cup O_4'']\big| \\
&= |(O_2 + (v,w)) \cap O_2| + |(O_2 + (v,w)) \cap O_4| \\
&\quad + |(O_4 + (v,w)) \cap O_2| + |(O_4 + (v,w)) \cap O_4| \\
&\quad + |(O_0 + (v,w)) \cap O_0| + |(O_0 + (v,w)) \cap O_2| + |(O_0 + (v,w)) \cap O_4| \\
&\quad + |(O_2 + (v,w)) \cap O_0| + |(O_2 + (v,w)) \cap O_2| + |(O_2 + (v,w)) \cap O_4| \\
&\quad + |(O_4 + (v,w)) \cap O_0| + |(O_4 + (v,w)) \cap O_2| + |(O_4 + (v,w)) \cap O_4| \\
&= \frac{q^2-1}{2}, \ \ \forall\, (v,w) \in Q \setminus \{(0,0)\}.
\end{aligned}$$

Finally, if we take two blocks from different block orbits, one from $\mathcal{B}_1$ and the other from $\mathcal{B}_2$, the intersections always summarize to the number expected:

$$\begin{aligned}
|(B_1 + (v,w)) \cap B_2| &= \big|\big([O_1' \cup O_3'] + (v,w)\big) \cap [O_2' \cup O_4']\big| \\
&\quad + \big|\big([O_2'' \cup O_4''] + (v,w)\big) \cap [O_0'' \cup O_2'' \cup O_4'']\big| \\
&= |(O_1 + (v,w)) \cap O_2| + |(O_1 + (v,w)) \cap O_4| \\
&\quad + |(O_3 + (v,w)) \cap O_2| + |(O_3 + (v,w)) \cap O_4| \\
&\quad + |(O_2 + (v,w)) \cap O_0| + |(O_2 + (v,w)) \cap O_2| + |(O_2 + (v,w)) \cap O_4|
\end{aligned}$$

$$+ |(O_4 + (v,w)) \cap O_0| + |(O_4 + (v,w)) \cap O_2| + |(O_4 + (v,w)) \cap O_4|$$
$$= \frac{q^2-1}{2}, \ \forall\, (v,w) \in Q.$$

□

From the construction of the design $\mathcal{D}$ it follows immediately that G acts on $\mathcal{D}$ as an automorphism group. We can derive even a slightly stronger result about the automorphisms of $\mathcal{D}$ from the above theorem. For that purpose, we first of all introduce the group

$$A\Gamma L_1(q) = \{x \mapsto a \cdot x^\sigma + b \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \text{ and } \sigma \in Aut(\mathbb{F}_q)\}$$

of all affine semilinear transformations of the field $\mathbb{F}_q$ considered as a 1-dimensional vector space over itself, which is called the 1-dimensional affine general semilinear group over $\mathbb{F}_q$. Evidently, the group of all field automorphisms $Aut(\mathbb{F}_q)$, which is cyclic of order e, as well as the 1-dimensional affine general linear group $AGL_1(q)$ of order $q \cdot (q-1)$, which had been used at the beginning of this paper in the process of defining the group G, are naturally embedded in $A\Gamma L_1(q)$, such that this group is a faithful split extension of the normal subgroup $AGL_1(q)$ by C, where $C = Aut(\mathbb{F}_q)$. For further details concerning the groups $A\Gamma L_n(q)$ in general we refer the reader to [1, pp. 185-186]. We know from our earlier investigation of $AGL_1(q)$, that this group contains a unique and therefore characteristic subgroup N of index 2, hence N is a normal subgroup of $A\Gamma L_1(q)$. Clearly, the product $M = NC$ is a normal subgroup of index 2 in $A\Gamma L_1(q)$. The reader should be aware of the fact that M is not necessarily the only subgroup of index 2 in $A\Gamma L_1(q)$, although this is known to be true for N in $AGL_1(q)$. Let

$$\psi : A\Gamma L_1(q) \to A\Gamma L_1(q)/M$$

be the natural epimorphism from $A\Gamma L_1(q)$ onto its factor group modulo M of order 2. We are now able to define

$$\begin{aligned} A &= A\Gamma L_1(q) \ \mathrm{sdp}_{(\psi,\psi)} \ A\Gamma L_1(q) \\ &= \{(x,y) \in A\Gamma L_1(q) \times A\Gamma L_1(q) \mid \psi(x) = \psi(y)\} \end{aligned}$$

to be the subdirect product of $A\Gamma L_1(q)$ with itself with respect to ψ, which obviously contains G as a normal subgroup and thus is a split extension of G by $C \times C$ of order $q^2 \cdot \left(\frac{q-1}{2}\right)^2 \cdot e^2 \cdot 2$. Since C preserves the multiplicative structure of $\mathbb{F}_q$ and in particular keeps the subsets $\{0\}$, D_+ and D_- of $\mathbb{F}_q$ invariant, the group $C \times C$ leaves the orbits $O_0, O_1, \ldots, O_4$ of H on Q invariant and hence belongs as well as H to each of the stabilizers of the base blocks B_0, B_1, and B_2. Therefore, the construction of the design $\mathcal{D}$ in Theorem 3.1 leads directly to the following conclusion.

Corollary 3.2. *For every odd prime power $q = p^e$ the group A – defined above – is contained in the full automorphism group $Aut(\mathcal{D})$ of the symmetric design $\mathcal{D}$.*

The corollary shows that the known part A of $Aut(\mathcal{D})$ contains G precisely then properly if $e \neq 1$, that means if $q = p^e$ is not a prime.

Finally, in the following remark, we want to formulate a conjecture – based on computations with GAP [2] – about the generic situation concerning the full automorphism group $Aut(\mathcal{D})$ of the symmetric design $\mathcal{D}$.

Remark 3.3. By inspection of $Aut(\mathcal{D})$ for some small values of $q = p^e$ we find that for almost every such q the group A always coincides with the full automorphism group $Aut(\mathcal{D})$ of the symmetric design $\mathcal{D}$, except for $q \in \{3, 5, 7\}$. In these three exceptional cases the group A is therefore properly contained in the full automorphism group $Aut(\mathcal{D})$ which is, for every $q \in \{3, 5, 7\}$, always isomorphic to a split extension of an elementary abelian group E_{q^2} of order q^2 by a certain complement acting faithfully on E_{q^2}. It turns out that by the property of being a faithful split extension the three automorphism groups are uniquely determined up to isomorphism. For these three values of q the structure of $Aut(\mathcal{D})$ is as follows:

1. If $q = 3$, then $Aut(\mathcal{D}) \cong E_9 : D_8$ and has order 72.
2. If $q = 5$, then $Aut(\mathcal{D}) \cong E_{25} : (S_3 \times Z_4)$ and has order 600.
3. If $q = 7$, then $Aut(\mathcal{D}) \cong E_{49} : (SL_2(3) \times Z_3)$ and has order 3528.

It seems to be natural to assume that for every odd prime power $q = p^e$, except for $q \in \{3, 5, 7\}$, the full automorphism group $Aut(\mathcal{D})$ of the symmetric design $\mathcal{D}$ is equal to the group A.

References

[1] T. Beth, D. Jungnickel and H. Lenz, Design Theory, Volume I, Second Edition, Cambridge University Press, 1999.

[2] The GAP Group, "GAP – Groups, Algorithms, and Programming", Version 4.4, `http://www.gap-system.org` (2004).

[3] D. Held and M.-O. Pavčević, *A Series of Hadamard Designs with Large Automorphism Groups*, J. Algebra **234** (2000), 620-626.

[4] E. Lander, Symmetric Designs: An Algebraic Approach, Cambridge University Press, 1983.

D. Held
Fachbereich Mathematik
Johannes Gutenberg-Universität
D-55128 Mainz
Germany
E-mail: `held@mathematik.uni-mainz.de`

M.-O. Pavčević
Department of applied mathematics
Faculty of electrical engineering
University of Zagreb
Unska 3
HR-10000 Zagreb
Croatia
E-mail: mario.pavcevic@fer.hr

M. Schmidt
Institut für Mathematik
Martin-Luther-Universität Halle-Wittenberg
Theodor-Lieser-Straße 5
D-06120 Halle (Saale)
Germany
E-mail: mail@marcel-schmidt.net

Received: 16.2.2007.