THE ORDER OF THE AUTOMORPHISM GROUP OF A
BINARY $q$-ANALOG OF THE FANO PLANE IS AT MOST TWO

MICHAEL KIERMAIER, SASCHA KURZ, AND ALFRED WASSERMANN

Abstract. It is shown that the automorphism group of a binary $q$-analog of
the Fano plane is either trivial or of order 2.

Keywords: Steiner triple systems; $q$-analogs of designs; Fano plane; automor-
phism group

MSC: 51E20; 05B07, 05A30

1. Introduction

Motivated by the connection to network coding, $q$-analogs of designs have re-
ceived an increased interest lately. Arguably the most important open problem in
this field is the question for the existence of a $q$-analog of the Fano plane [6]. Its
existence is open over any finite base field GF($q$). The most important single case
is the binary case $q = 2$, as it is the smallest one. Nonetheless, so far the binary
$q$-analog of the Fano plane has withstood all computational or theoretical attempts
for its construction or refutation.

Following the approach for other notorious putative combinatorial objects as, e.g., a
projective plane of order 10 or a self-dual binary [72, 36, 16] code, the possible
 automorphisms of a binary $q$-analog of the Fano plane have been investigated in
[4]. As a result [4, Theorem 1], its automorphism group is at most of order 4, and
up to conjugacy in GL(7, 2) it is represented by a group in the following list:

(a) The trivial group.
(b) The group of order 2

$$G_2 = \langle \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \rangle.$$

(c) One of the following two groups of order 3:

$$G_{3,1} = \langle \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \rangle \quad \text{and} \quad G_{3,2} = \langle \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \rangle.$$

(d) The cyclic group of order 4

$$G_4 = \langle \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \rangle.$$

For the groups of order 2, the above result was achieved as a special case of
a more general result on restrictions of the automorphisms of order 2 of a binary

\footnotesize
The second and the third author were supported in part by the project Integer Linear Pro-
gramming Models for Subspace Codes and Finite Geometry (KU 2430/3-1, WA 1666/9-1) from
the German Research Foundation.

1
$q$-analog of Steiner triple systems [4, Theorem 2]. All the remaining groups have been excluded computationally applying the method of Kramer and Mesner.

In this article, we will extend these results as follows. In Section 3 automorphisms of order 3 of general binary $q$-analogs of Steiner triple systems $\text{STS}_2(v)$ will be investigated. The main result is Theorem 2, which excludes about half of the conjugacy types of elements of order 3 in $\text{GL}(v,2)$ as the automorphism of an $\text{STS}_2(v)$. In the special case of ambient dimension 7, the group $\text{GL}(7,2)$ has 3 conjugacy types $G_{3,1}$, $G_{3,2}$ and $G_{3,3}$ of subgroups of order 3. Theorem 2 shows that the group $G_{3,2}$ is not the automorphism group of a binary $q$-analogue of the Fano plane. Furthermore, Theorem 2 provides a purely theoretical argument for the impossibility of $G_{3,3}$, which previously has been shown computationally in [4].

In Section 4, the groups $G_4$ and $G_{3,1}$ will be excluded computationally by showing that the Kramer-Mesner equation system does not have a solution. Both cases are fairly large in terms of computational complexity. To bring the problems to a feasible level, the solution process is parallelized and executed on the high performance Linux cluster of the University of Bayreuth. For the latter and harder case $G_{3,1}$, we additionally make use of the inherent symmetry of the search space given by the normalizer of the prescribed group, see also [8].

Finally, the combination of the results of Sections 3 and 4 yields

**Theorem 1.** The automorphism group of a binary $q$-analogue of the Fano plane is either trivial or of order 2. In the latter case, up to conjugacy in $\text{GL}(7,2)$ the automorphism group is represented by

$$\langle \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \rangle.
$$

2. Preliminaries

Throughout the article, $V$ is a vector space over $\text{GF}(2)$ of finite dimension $v$.

2.1. The subspace lattice. For simplicity, a subspace of $V$ of dimension $k$ will be called a $k$-subspace. The set of all $k$-subspaces of $V$ is called the Grassmannian and is denoted by $[V]_k$. As in projective geometry, the 1-subspaces of $V$ are called points, the 2-subspaces lines and the 3-subspaces planes. Our focus lies on the case $q = 2$, where the 1-subspaces $(x)_{\text{GF}(2)} \in [V]_2$ are in one-to-one correspondence with the nonzero vectors $x \in V \setminus \{0\}$. The number of all $r$-subspaces of $V$ is given by the Gaussian binomial coefficient

$$\# [V]_{k} = \binom{v}{k}_q = \begin{cases} (q^v-1)\cdots(q^r+r+1-1) \\ (q-1)\cdots(q-1) \end{cases} \quad \text{if } k \in \{0, \ldots, v\};$$

otherwise.

The set $\mathcal{L}(V)$ of all subspaces of $V$ forms the subspace lattice of $V$. There are good reasons to consider the subset lattice as a subspace lattice over the unary “field” $\text{GF}(1)$ [5].

By the fundamental theorem of projective geometry, for $v \geq 3$ the automorphism group of $\mathcal{L}(V)$ is given by the natural action of $\text{PGL}(V)$ on $\mathcal{L}(V)$. In the case that $q$ is prime, the group $\text{PGL}(V)$ reduces to $\text{PGL}(V)$, and for the case of our interest $q = 2$, it reduces further to $\text{GL}(V)$. After a choice of a basis of $V$, its elements are represented by the invertible $v \times v$ matrices $A$, and the action on $\mathcal{L}(V)$ is given by the vector-matrix-multiplication $v \mapsto vA$. 

2.2. Designs.

**Definition 1.** Let \( t, v, k \) be integers with \( 0 \leq t \leq k \leq v \) and \( \lambda \) another positive integer. A set \( D \subseteq \binom{V}{k} \) is called a \( t-(v, k, \lambda)_q \) subspace design if each \( t \)-subspace of \( V \) is contained in exactly \( \lambda \) elements (called blocks) of \( D \). When \( \lambda = 1 \), \( D \) is called a \( q \)-Steiner system. If additionally \( t = 2 \) and \( k = 3 \), \( D \) is called a \( q \)-Steiner triple system and denoted by \( \text{STS}_q(v) \).

Classical combinatorial designs can be seen as the limit case \( q = 1 \) of a design over a finite field. Indeed, quite a few statements about combinatorial designs have a generalization to designs over finite fields, such that the case \( q = 1 \) reproduces the original statement [3, 9, 10, 15].

One example of such a statement is the following [18, Lemma 4.1(1)]: If \( D \) is a \( t-(v, k, \lambda)_q \) design, then \( D \) is also an \( s-(v, k, \lambda)_q \) for all \( s \in \{0, \ldots, t\} \), where

\[
\lambda_s := \lambda \frac{\binom{v-s}{t-s}_q}{\binom{k-s}{t-s}_q}.
\]

In particular, the number of blocks in \( D \) equals

\[
\#D = \lambda_0 = \lambda \frac{\binom{v}{t}_q}{\binom{k}{t}_q}.
\]

So, for a design with parameters \( t-(v, k, \lambda)_q \), the numbers \( \lambda \frac{\binom{v-s}{t-s}_q}{\binom{k-s}{t-s}_q} \) necessarily are integers for all \( s \in \{0, \ldots, t\} \) (integrality conditions). In this case, the parameter set \( t-(v, k, \lambda)_q \) is called admissible. It is further called realizable if a \( t-(v, k, \lambda)_q \) design actually exists.

For designs over finite fields, the action of \( \text{Aut}(\mathcal{L}(V)) \cong \text{P}GL(V) \) on \( \mathcal{L}(V) \) provides a notion of isomorphism. Two designs in the same ambient space \( V \) are called isomorphic if they are contained in the same orbit of this action (extended to the power set of \( \mathcal{L}(V) \)). The automorphism group \( \text{Aut}(D) \) of a design \( D \) is its stabilizer with respect to this group action. If \( \text{Aut}(D) \) is trivial, we will call \( D \) rigid. Furthermore, for \( G \leq \text{P}GL(V) \), \( D \) will be called \( G \)-invariant if it is fixed by all elements of \( G \) or equivalently, if \( G \leq \text{Aut}(D) \). Note that if \( D \) is \( G \)-invariant, then \( D \) is also \( H \)-invariant for all subgroups \( H \leq G \).

2.3. Steiner triple systems. For an \( \text{STS}_q(v) \) we have

\[
\lambda_1 = \frac{\binom{v-1}{2}_q}{\binom{3-1}{2}_q} = \frac{q^{v-1} - 1}{q^2 - 1} \quad \text{and}
\]

\[
\lambda_0 = \frac{\binom{v}{2}_q}{\binom{3}{2}_q} = \frac{(q^v - 1)(q^{v-1} - 1)}{(q^3 - 1)(q^2 - 1)}.
\]

As a consequence, the parameter set of an ordinary or a \( q \)-analog Steiner triple system \( \text{STS}_q(v) \) is admissible if and only if \( v \equiv 1, 3 \mod 6 \) and \( v \geq 3 \). For \( q = 1 \), the existence question is completely answered by the result that a Steiner triple system is realizable if and only if it is admissible [11]. However in the \( q \)-analog case, our current knowledge is quite sparse. Apart from the trivial \( \text{STS}_q(3) \) given by \( \{V\} \), the only decided case is \( \text{STS}_2(13) \), which has been constructed in [1].

The smallest admissible case of a non-trivial \( q \)-Steiner triple system is \( \text{STS}_q(7) \), whose existence is open for any prime power value of \( q \). It is known as a \( q \)-analog of the Fano plane, since the unique Steiner triple system \( \text{STS}_1(7) \) is the Fano plane. It is worth noting that there are cases of Steiner systems without a \( q \)-analog, as the famous large Witt design with parameters \( 5-(24, 8, 1) \) does not have a \( q \)-analog for any prime power \( q \) [9].
2.4. Group actions. Let $G$ be a group acting on a set $X$ via $x \mapsto x^g$. The stabilizer of $x$ in $G$ is given by $G_x = \{ g \in G \mid x^g = x \}$, and the $G$-orbit of $x$ is given by $x^G = \{ x^g \mid g \in G \}$. By the action of $G$, the set $X$ is partitioned into orbits. For all $x \in X$, there is the correspondence $x^g \mapsto G_x g$ between the orbit $x^G$ and the set $G_x \setminus G$ of the right cosets of the stabilizer $G_x$ in $G$. For finite orbit lengths, this implies the orbit-stabilizer theorem stating that $\#x^G = [G : G_x]$. In particular, the orbit lengths $\#x^G$ are divisors of the group order $\#G$.

For all $g \in G$ we have

\[ G_{x^g} = g^{-1}G_x g. \]

This leads to the following observations:

(a) The stabilizers of elements in the same orbit are conjugate in $G$, and any conjugate subgroup of $G_x$ is the $G$-stabilizer of some element in the $G$-orbit of $x$.

(b) Equation (1) shows that $G_{x^g} = G_x$ for all $g \in N_G(G_x)$, where $N_G$ denotes the normalizer in $G$. Consequently, for any subgroup $H \leq G$ the normalizer $N_G(H)$ acts on the elements of $x \in X$ with $N_x = H$.

The above observations greatly benefit our original problem, which is the investigation of all the subgroups $H$ of $G = \text{GL}(7, 2)$ for the existence of a binary $q$-analog $D$ of the Fano plane whose stabilizer $G_D$ equals $H$: By observation 2.4, we may restrict the search to representatives of subgroups of $G$ up to conjugacy. Furthermore, having fixed some subgroup $H$, by observation 2.4 the normalizer $N = N_G(H)$ is acting on the solution space. Consequently, we can notably speed up the search process by applying isomorph rejection with respect to the action of $N$.

2.5. The method of Kramer and Mesner. The method of Kramer and Mesner [13] is a powerful tool for the computational construction of combinatorial designs. It has been successfully adopted and used for the construction of designs over a finite field [2, 14]. For example, the hitherto only known $q$-analog of a Steiner triple system in $[1]$ has been constructed by this method. Here we give a short outline, for more details we refer the reader to [2]. The Kramer-Mesner matrix $M_{t,k}^{G}$ is defined to be the matrix whose rows and columns are indexed by the $G$-orbits on the set $\binom{V}{t}$ of $t$-subspaces and on the set $\binom{V}{k}$ of $k$-subspaces of $V$, respectively. The entry of $M_{t,k}^{G}$ with row index $T^G$ and column index $K^G$ is defined as $\#\{K' \in K^G \mid T \leq K'\}$. Now there exists a $G$-invariant $t-(v, k, \lambda)_q$ design if and only if there is a zero-one solution vector $x$ of the linear equation system

\[ M_{t,k}^{G} x = \lambda \mathbf{1}, \]

where $\mathbf{1}$ denotes the all-one column vector. More precisely, if $x$ is a zero-one solution vector of the system (2), a $t-(v, k, \lambda)_q$ design is given by the union of all orbits $K^G$ where the corresponding entry in $x$ equals one. If $x$ runs over all zero-one solutions, we get all $G$-invariant $t-(v, k, \lambda)_q$ designs in this way.

3. Automorphisms of order 3

In this section, automorphisms of order 3 of binary $q$-analogs of Steiner triple systems are investigated. While the techniques are not restricted to $q = 2$ or order 3, we decided to stay focused on our main case of interest. In parts, we follow [4, Section 3] where automorphisms of order 2 have been analyzed.

We will assume that $V = \text{GF}(2)^v$, allowing us to identify $\text{GL}(V)$ with the matrix group $\text{GL}(v, 2)$. 
Lemma 1. In $\text{GL}(v, 2)$, there are exactly $[v/2]$ conjugacy classes of elements of order 3. Representatives are given by the block-diagonal matrices $A_{v,f}$ with $f \in \{0, \ldots, v - 1\}$ and $v - f$ even, consisting of $\frac{v - f}{2}$ consecutive $2 \times 2$ blocks $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, followed by a $f \times f$ unit matrix.

Proof. Let $A \in \text{GL}(v, 2)$ and $m_A \in \text{GF}(2)[X]$ be its minimal polynomial. The matrix is of order 3 if and only if $m_A$ divides $X^3 - 1 = (X + 1)(X^2 + X + 1)$ but $m_A \not\equiv X + 1$. Now the enumeration of the possible rational normal forms of $A$ yields the stated classification. \hfill $\Box$

For a matrix $A$ of order 3, the unique conjugate $A_{v,f}$ given by Lemma 1 will be called the type of $A$. The action of $\langle A_{v,f} \rangle$ partitions the point set $[\text{GF}(2)^v]^2$ into orbits of size 1 or 3. An orbit of length 3 may either consist of three collinear points (orbit line) or of a triangle (orbit triangle).

Lemma 2. The action of $\langle A_{v,f} \rangle$ partitions $[\text{GF}(2)^v]^2$ into

(i) $2^f - 1$ fixed points;
(ii) $\frac{2^v - f - 1}{3}$ orbit lines;
(iii) $\frac{(2^v - f - 1)(2^f - 1)}{3}$ orbit triangles.

Proof. Let $G = \langle A_{v,f} \rangle$. The eigenspace of $A_{v,f}$ corresponding to the eigenvalue 1 is of dimension $f$ and equals $F = \{e_{v-f+1}, e_{v-f+2}, \ldots, e_v\}$. The fixed points are exactly the $2^f - 1$ elements of $[F]^2$. Furthermore, for a non-zero vector $x \in \text{GF}(2)^v$, the orbit $(x)^{G_{\text{GF}(2)}}$ is an orbit line if and only if $A_{v,f}^2 x + A_{v,f} x + x = 0$ or equivalently,

$$x \in K := \ker(A_{v,f}^2 + A_{v,f} + I_v) = \langle e_1, e_2, \ldots, e_{v-f} \rangle.$$ 

Thus, the number of orbit lines is $\left[ \frac{\dim(K)}{v} \right]_2 / 3 = \frac{(2^v - f - 1)}{3}$. The remaining $\left[ \frac{v}{1} \right]_2 - \left[ \frac{v}{1} \right]_2 - \left[ \frac{v}{1} \right]_2 = \frac{(2^v - f - 1)(2^f - 1)}{3}$ points are partitioned into orbit triangles. \hfill $\Box$

Example 1. We look at the classical Fano plane as the points and lines in $\text{PG}(2, 2) = \text{PG}(\text{GF}(2)^3)$. Its automorphism group is $\text{GL}(3, 2)$. By Lemma 1, there is a single conjugacy class of automorphisms of order 3, represented by

$$A_{3,1} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$ 

By Lemma 2, the action of $\langle A_{3,1} \rangle$ partitions the point set $[\text{GF}(2)^3]^2$ into the fixed point

$$\langle (0, 0, 1) \rangle_{\text{GF}(2)},$$

the orbit line

$$\{ \langle (1, 0, 0) \rangle_{\text{GF}(2)}, \langle (0, 1, 0) \rangle_{\text{GF}(2)}, \langle (1, 1, 0) \rangle_{\text{GF}(2)} \},$$

and the orbit triangle

$$\{ \langle (1, 0, 1) \rangle_{\text{GF}(2)}, \langle (0, 1, 1) \rangle_{\text{GF}(2)}, \langle (1, 1, 1) \rangle_{\text{GF}(2)} \}.$$ 

Now we look at planes $E$ fixed under the action of $\langle A_{v,f} \rangle$. Here, the restriction of the automorphism $x \mapsto A_{v,f} x$ to $E$ yields an automorphism of $E \equiv \text{GF}(2)^3$ whose order divides 3. If its order is 1, then $E$ consists of 7 fixed points and we call $E$ of type 7. Otherwise, the order is 3. So, by Example 1 it is of type $A_{3,1}$, and $E$ consists of 1 fixed point, 1 orbit line and 1 orbit triangle. Here, we call $E$ of type 1.
Lemma 3. Under the action of $\langle A_{v,f} \rangle$,
\[
\#\text{fixed planes of type } 7 = \left[ \frac{f}{3} \right]_2 = \frac{(2^f - 1)(2^{f-1} - 1)(2^{f-2} - 1)}{21},
\]
\[
\#\text{fixed planes of type } 1 = \#\text{orbit triangles} = \frac{(2^f - 1)(2^{v-f} - 1)}{3}.
\]

Proof. The fixed planes of type 7 are precisely the planes in the space of all fixed points of dimension $f$. Each fixed plane of type 3 is uniquely spanned by an orbit triangle. \hfill \Box

Example 2. By Lemma 1, the conjugacy classes of elements of order 3 in $\text{GL}(7,2)$ are represented by

\[
A_{7,1} = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix},
A_{7,3} = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix},
A_{7,5} = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

By Lemma 2 and Lemma 3, we get the following numbers:

|                      | $A_{7,1}$ | $A_{7,3}$ | $A_{7,5}$ |
|----------------------|-----------|-----------|-----------|
| #fixed points        | 1         | 7         | 31        |
| #orbit lines         | 21        | 5         | 1         |
| #orbit triangles     | 21        | 35        | 31        |
| #fixed planes of type 7 | 0   | 1         | 155       |
| #fixed planes of type 1 | 21  | 35        | 31        |

In the following, $D$ denotes an $\text{STS}_2(v)$ with an automorphism $A_{v,f}$ of order 3. From the admissibility we get $v \equiv 1, 3 \pmod{6}$ and hence $f$ odd. The fixed points are given by the 1-subspaces of the eigenspace of $A_{v,f}$ corresponding to the eigenvalue 1, which will be denoted by $F$. The set of fixed planes in $D$ of type 7 and 1 will be denoted by $F_7$ and $F_1$, respectively.

Lemma 4. Let $L \in \binom{V}{2}$, be a fixed line. Then the block passing through $L$ is a fixed block.

Proof. From the design property, there is a unique block $B \in D$ passing through $L$. For all $A \in \langle A_{v,f} \rangle$, we have $B \cdot A \in D$ and $B \cdot A > L \cdot A = L$, so $B \cdot A = B$ by the uniqueness of $B$. Hence $B$ is a fixed block. \hfill \Box

Lemma 5. The blocks in $F_7$ form an $\text{STS}_2(f)$ on $F$.

Proof. Obviously, each fixed block of type 7 is contained in $F$. Let $L \in \binom{F}{2}$. By Lemma 4, there is a unique fixed block $B \in D$ passing through $L$. Since $L$ consists of 3 fixed points, $B$ must be of type 7. Hence $B \leq F$. \hfill \Box

The admissibility of $\text{STS}_2(f)$ yields $f \equiv 1, 3 \equiv 6$, so:

Corollary 1. An $\text{STS}_2(v)$ does not have an automorphism of order 3 of type $A_{v,f}$ with $f \equiv 2 \pmod{3}$.

In particular, a binary $q$-analog of the Fano plane does not have an automorphism of order 3 and type $A_{7,5}$. This gives a theoretical confirmation of the computational result of [4], where the group $\langle A_{7,5} \rangle$ has been excluded computationally.

Lemma 6.

\[
\#F_7 = \frac{(2^f - 1)(2^{f-1} - 1)}{21};
\]
\[
\#F_1 = \#\text{orbit lines} = \frac{2^{v-f} - 1}{3}.
\]
Proof. By Lemma 5, the number \( \#F_7 \) equals the \( \lambda_0 \)-value of an STS_2(f).

For \( \#F_1 \), we double count the set \( X \) of all pairs \((L, B)\) where \( L \) is an orbit line, \( B \in F_1 \) and \( L < B \). By Lemma 2, the number of choices for \( L \) is \( \frac{2^{v-1}-1}{3} \). Lemma 4 yields a unique fixed block \( B \) passing through \( L \). Since \( B \) contains the orbit line \( L \), \( B \) has to be of type 1. So \( \#X = \frac{2^{v-1}-1}{3} \). On the other hand, there are \( \#F_1 \) possibilities for \( B \) and each such \( B \) contains a single orbit line. So \( \#X = \#F_1 \), verifying Equation (4).

\[ \square \]

Lemma 7. An STS_2(v) with \( v \geq 7 \) does not have an automorphism of order 3 of type \( A_{v,f} \) with \( f > \frac{v-3}{2} \) and \( f \not\equiv v \mod 3 \).

Proof. Assume that \( v \geq 7 \) and \( f \not\equiv v \mod 3 \). Let \( P \in \left[ F \right]_2 \) and \( X \) be the set of all blocks passing through \( P \) which are not of type 7. The number of blocks passing through \( P \) is \( \lambda_1 = \frac{2^{v-1}-1}{3} \). By Lemma 5, \( F_7 \) is an STS_2(f) on \( F \). So the number of blocks of type 7 passing through \( P \) is given by the \( \lambda_1 \)-value of an STS_2(f), which equals \( \frac{2^{v-1}-2f-1}{3} \). Hence \( \#X = \frac{2^{v-1}-2f-1}{3} \). Since \( P \) is a fixed point, the action of \( \langle A_{v,f} \rangle \) partitions \( X \) into orbits of size 1 and 3. Depending on \( v \) and \( f \), the remainder of \( \#X \) modulo 3 is shown below:

| \( v \equiv 1 \mod 6 \) | \( f \equiv 1 \mod 6 \) | \( f \equiv 3 \mod 6 \) | \( f \equiv 5 \mod 6 \) |
|------------------------|------------------------|------------------------|------------------------|
| \( v \equiv 3 \mod 6 \) | 0                       | 1                       | 2                       |
|                        | 2                       | 0                       | 1                       |

In our case \( f \not\equiv v \mod 3 \), we see that \( \#X \) is not a multiple of 3, implying the existence of at least one fixed block in \( X \), which must be of type 1. Thus, it contains only 1 fixed point, showing that the type 1 blocks coming from different points \( P \in \left[ F \right]_2 \) are pairwise distinct. In this way, we see that

\[
2^f - 1 = \#\text{fixed points} \leq \#F_1 = \frac{2^{v-f}-1}{3},
\]

where the last equality comes from Lemma 6. Using the preconditions \( v \geq 7 \) and \( v, f \) odd, we get that this inequality is violated for all \( f > \frac{v-3}{2} \). \[ \square \]

Remark 1. [\((a)\)]

1. The condition \( v \geq 7 \) cannot be dropped since the automorphism group of the trivial STS_2(3) is the full linear group GL(3, 2) containing an automorphism of type \( A_{3,1} \).

2. In the case that the remainder of \( \#X \) modulo 3 equals 2, we could use the stronger inequality \( 2(2^f - 1) \leq \#F_1 \). However, the final condition on \( f \) is the same.

Lemma 7 allows us to exclude one of the groups left open in [4, Theorem 1]:

Corollary 2. There is no binary \( q \)-analog of the Fano plane invariant under \( G_{3,2} := \langle A_{7,3} \rangle \).

As a combination of Lemma 1, Corollary 1 and Lemma 7, we get:

Theorem 2. Let \( D \) be an STS_2(v) with an automorphism \( A \) of order 3. Then \( A \) has the type \( A_{v,f} \) with \( f \not\equiv 2 \mod 3 \). If \( f \equiv v \mod 3 \), then either \( v = 3 \) or \( f \leq \frac{v-3}{2} \).
Example 3. Theorem 2 excludes about half of the conjugacy types of elements of order 3. Below, we list the remaining ones for small admissible values of $v$:

| $\#$ fixed points $|$ $A_{7,1}$ $|$ $A_{9,1}$ $|$ $A_{9,2}$ $|$ $A_{13,1}$ $|$ $A_{13,3}$ $|$ $A_{13,7}$ |
|----------------|--------|--------|--------|--------|--------|--------|
| $\#$ orbit lines $|$ $1$ $|$ $1$ $|$ $7$ $|$ $1$ $|$ $7$ $|$ $127$ |
| $\#$ orbit triangles $|$ $21$ $|$ $85$ $|$ $21$ $|$ $1365$ $|$ $341$ $|$ $21$ |
| $\#$ fixed planes of type 7 $|$ $21$ $|$ $85$ $|$ $147$ $|$ $1365$ $|$ $2387$ $|$ $2667$ |
| $\#$ fixed planes of type 1 $|$ $0$ $|$ $0$ $|$ $1$ $|$ $0$ $|$ $1$ $|$ $11811$ |
| $\#F_7$ $|$ $0$ $|$ $0$ $|$ $1$ $|$ $0$ $|$ $1$ $|$ $381$ |
| $\#F_1$ $|$ $21$ $|$ $85$ $|$ $21$ $|$ $1365$ $|$ $341$ $|$ $21$ |

We conclude this section with an investigation of the case $A_{v,1}$, which has not been excluded for any value of $v$. The computational treatment of the open case $A_{7,1}$ in Section 4 will make use of the structure result of the following lemma.

Lemma 8. Let $D$ be a STS$(v)$ with an automorphism of type $A_{v,1}$. Then $D$ contains $2^{v-1}v^{-1}$ fixed blocks of type 1. The remaining blocks of $D$ are partitioned into orbits of length 3. Furthermore, $V$ can be represented as $V = W + X$ with GF$(2)$ vector spaces $W$ and $X$ of dimension $v - 1$ and 1, respectively, such that the fixed blocks of type 1 are given by the set $\{L + X : L \in \mathcal{L}\}$, where $\mathcal{L}$ is a Desarguesian line spread of PG$(W)$.

Proof. Let $W = GF(2^{v-1})$, which will be considered as a GF$(2)$ vector space if not stated otherwise. Let $\zeta \in W$ be a primitive third root of unity. We consider the automorphism $\varphi : x \mapsto \zeta x$ of $W$ of order 3. Since $\varphi$ does not have fixed points in $\{W\}_{1/2}$, $\varphi$ is of type $A_{v-1,0}$. The set $\mathcal{L} = [W]_3$ is a Desarguesian line spread of PG$(W)$. It consists of all lines of PG$(W)$ with $\varphi(L) = L$. Since PG$(W)$ does not contain any fixed points under the action of $\varphi$, $\mathcal{L}$ is the set of the $(2^{v-1} - 1)/3$ orbit lines.

Now let $X$ be a GF$(2)$ vector space of dimension 1. The map $\tilde{\varphi} = \varphi \times \text{id}_X$ is an automorphism of $V = W \times X$ of order 3 and type $A_{v,1}$. Let $\tilde{\mathcal{L}} = \{L + X : L \in \mathcal{L}\}$. Under the action of $\tilde{\varphi}$, the elements of $\tilde{\mathcal{L}}$ are fixed planes of type 1. By Lemma 3, the total number of fixed planes of type 1 equals $\#\tilde{\mathcal{L}} = \#\mathcal{L}$, so $\tilde{\mathcal{L}}$ is the full set of fixed planes of type 1. Moreover, Lemma 6 gives $\#F_1 = (2^{v-1} - 1)/3 = \#\tilde{\mathcal{L}}$, on the one hand, so all these planes have to be blocks of $D$, and $\#F_7 = 0$ on the other hand, so the remaining blocks are partitioned into orbits of length 3.

4. Computational results

The automorphism groups $G_{3,1}$ and $G_4$ of a tentative STS$_2(7)$ are excluded computationally by the method of Kramer and Mesner from Section 2.5. The matrix $M_{7,1}^{G_{3,1}}$ consists of 693 rows and 2439 columns, the matrix $M_{7,1}^{G_{3,1}}$ has 903 rows and 3741 columns. In both cases, columns containing entries larger than 1 had been ignored since from equation (2) it is immediate that the corresponding 3-orbits cannot be part of a Steiner system.

One of the fastest methods for exhaustively searching all 0/1 solutions of such a system of linear equations where all coefficients are in $\{0,1\}$ is the backtrack algorithm dancing links [12]. We implemented a parallel version of the algorithm which is well suited to the job scheduling system Torque of the Linux cluster of the University of Bayreuth. The parallelization approach is straightforward: In a first step all paths of the dancing links algorithm down to a certain level are stored. In the second step every such path is started as a separate job on the computer cluster, where initially the algorithm is forced to start with the given path.
For the group $G_4$ the search was divided into 192 jobs. All of these determined that there is no STS$_2(7)$ with automorphism group $G_4$. Together, the exhaustive search of all these 192 sub-problems took approximately 5500 CPU-days.

The group $G_{3,1}$ was even harder to tackle. The estimated run time (see [12]) for this problem is 27 600 000 CPU-days. In order to break the symmetry of this search problem and avoid unnecessary computations, the normalizer $N(G_{3,1})$ of $G_{3,1}$ in $GL(7,2)$ proved to be useful. According to GAP [7], the normalizer is generated by

$$N(G_{3,1}) = \langle \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \rangle$$

and has order 362 880.

As discussed in Section 2.4, if for a prescribed group $G$, $s_1, s_2$ are two solutions of the Kramer-Mesner equations (2), then $s_1$ and $s_2$ correspond to two designs $D_1$ and $D_2$ both having $G$ as full automorphism group. A permutation $\sigma_n$ which maps the 1-entries of $s_1$ to the 1-entries of $s_2$ can be represented by an element $n \in GL(7,2)$.

In other words, $D_1^n = D_2$. Since $G$ is the full automorphism group of $D_1$ and $D_2$ it follows for all $g \in G$:

$$D_1^{ng} = D_2^g = D_2 = D_1^n.$$  

This shows that $n \in N(G)$.

This can be used as follows in the search algorithm. We force one orbit $K_i^G$ to be in the design. If dancing links shows that there is no solution which contains this orbit, all $k$-orbits in $(K_i^G)^N$ can be excluded from being part of a solution, i.e. the corresponding columns of $M_i^{G,k}$ can be removed.

In the case $G_{3,1}$, the set of $k$-orbits is partitioned into four orbits under the normalizer $N(G_{3,1})$. Two of this four orbits, let’s call them $K_1^G$ and $K_2^G$, can be excluded with dancing links in a few seconds. The third orbit $K_3^G$ needs more work, see below. After excluding the third orbit, also the fourth orbit is excluded in a few seconds.

For the third orbit $K_3^G$ we iterate this approach and fix two $k$-orbits simultaneously, one of them being $K_3^G$. That is, we consider all cases of fixed pairs $(K_3^G, K_4^G)$, where $K_4^G \notin (K_1^G)^N \cup (K_2^G)^N$. If there is no design which contains this pair of $k$-orbits, all $k$-orbits of the orbit $(K_i^G)^S$ can be excluded too, where $S = G_{K_i^G}$ is the stabilizer of the orbit $K_i^G$ under the action of $N(G)$.

This process could be repeated for triples, but run time estimates show that fixing pairs of $k$-orbits minimizes the computing time. Under the stabilizer of $K_i^G$, the set of pairs $(K_3^G, K_4^G)$ of $k$-orbits is partitioned into 14 orbits. Seven of these 14 pairs representing the orbits lead to problems which could be solved in a few seconds. The remaining seven sub-problems were split into 49 050 separate jobs with the above approach for parallelization. These jobs could be completed by dancing links in approximately 23 600 CPU-days on the computer cluster, determining that there is no STS$_2(7)$ with automorphism group $G_{3,1}$.

For the group $G_2$ the estimated run time is 3 020 000 000 000 000 CPU-days which seems out of reach with the methods of this paper.

\footnote{If iterated till the end, this type of search algorithm is known as orderly generation, see e.g. [16, 17].}
Acknowledgements

The authors would like to acknowledge the financial support provided by COST – European Cooperation in Science and Technology – within the Action IC1104 Random Network Coding and Designs over GF(q). The authors also want to thank the IT service center of the University Bayreuth for providing the excellent computing cluster, and especially Dr. Bernhard Winkler for his support.

References

[1] Braun, M., Etzion, T., Östergård, P., Vardy, A., Wassermann, A.: Existence of q-analogs of steiner systems (2013)
[2] Braun, M., Kerber, A., Laue, R.: Systematic construction of q-analogs of t-(v, k, λ)-designs. Des. Codes Cryptogr. 34(1), 55–70 (2005). DOI 10.1007/s10623-003-4194-z
[3] Braun, M., Kiermaier, M., Kohnert, A., Laue, R.: Large sets of subspace designs (2014)
[4] Braun, M., Kiermaier, M., Nakić, A.: On the automorphism group of a binary q-analog of the Fano plane. European J. Combin. 51, 443–457 (2016). DOI 10.1016/j.ejc.2015.07.014
[5] Cohn, H.: Projective geometry over U1 and the Gaussian binomial coefficients. Amer. Math. Monthly 111(6), 487–495 (2004). DOI 10.2307/4145067
[6] Etzion, T., Storme, L.: Galois geometries and coding theory. Des. Codes Cryptogr. 78(1), 311–350 (2016). DOI 10.1007/s10623-015-0156-5
[7] The GAP Group: GAP – Groups, Algorithms, and Programming, Version 4.8.3 (2016). URL http://www.gap-system.org
[8] Kaski, P.: Isomorph-free exhaustive generation of designs with prescribed groups of automorphisms. SIAM J. Discrete Math. 19(3), 664–690 (2005).
[9] Kiermaier, M., Laue, R.: Derived and residual subspace designs. Adv. Math. Commun. 9(1), 105–115 (2015). DOI 10.3934/amc.2015.9.105
[10] Kiermaier, M., Pavčević, M.O.: Intersection numbers for subspace designs. J. Combin. Des. 23(11), 463–480 (2015). DOI 10.1002/jcd.21403
[11] Kirkman, T.P.: On a problem in combinatorics. Cambridge and Dublin Math. J. 2, 191–204 (1847)
[12] Knuth, D.E.: Dancing links. In: J. Davies, B. Roscoe, J. Woodcock (eds.) Millennial Perspectives in Computer Science: Proceedings of the 1999 Oxford-Microsoft Symposium in Honour of Sir Tony Hoare. Palgrave (2000)
[13] Kramer, E.S., Mesner, D.M.: t-designs on hypergraphs. Discrete Math. 15(3), 263–296 (1976). DOI 10.1016/0012-365X(76)90030-3
[14] Miyakawa, M., Munemasa, A., Yoshiara, S.: On a class of small 2-designs over GF(q). J. Combin. Des. 3(1), 61–77 (1995). DOI 10.1002/jcd.3180030108
[15] Nakić, A., Pavčević, M.O.: Tactical decompositions of designs over finite fields. Des. Codes Cryptogr. 77(1), 49–60 (2015). DOI 10.1007/s10623-014-9988-7
[16] Read, R.C.: Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. Ann. Discrete Math. 2, 107–120 (1978)
[17] Royle, G.F.: An orderly algorithm and some applications in finite geometry. Discrete Math. 185(1–3), 105–115 (1998). DOI http://dx.doi.org/10.1016/S0012-365X(97)00167-2
[18] Suzuki, H.: On the inequalities of t-designs over a finite field. European J. Combin. 11(6), 601–607 (1990). DOI 10.1016/S0195-6698(13)80045-5

M. Kiermaier Mathematisches Institut, Universität Bayreuth, 95447 Bayreuth, Germany, http://www.mathe2.uni-bayreuth.de/michaelk/
E-mail address: michael.kiermaier@uni-bayreuth.de

S. Kurz Mathematisches Institut, Universität Bayreuth, 95447 Bayreuth, Germany
E-mail address: sascha.kurz@uni-bayreuth.de

A. Wassermann Mathematisches Institut, Universität Bayreuth, 95447 Bayreuth, Germany
E-mail address: alfred.wassermann@uni-bayreuth.de