THE CLASSIFICATION OF FLAG-TRANSITIVE STEINER 3-DESIGNS

MICHAEL HUBER

ABSTRACT. We solve the long-standing open problem of classifying all 3-(v, k, 1) designs with a flag-transitive group of automorphisms (cf. A. Delandtsheer, Geom. Dedicata 41 (1992), p. 147; and in: “Handbook of Incidence Geometry”, ed. by F. Buekenhout, Elsevier Science, Amsterdam, 1995, p. 273; but presumably dating back to 1965). Our result relies on the classification of the finite 2-transitive permutation groups.

1. Introduction

For positive integers \( t \leq k \leq v \) and \( \lambda \), we define a \( t-(v, k, \lambda) \) design to be a finite incidence structure \( \mathcal{D} = (X, \mathcal{B}, I) \), where \( X \) denotes a set of points, \( |X| = v \), and \( \mathcal{B} \) a set of blocks, \( |\mathcal{B}| = b \), with the properties that each block \( B \in \mathcal{B} \) is incident with \( k \) points, and each \( t \)-subset of \( X \) is incident with \( \lambda \) blocks. A flag of \( \mathcal{D} \) is an incident point-block pair, that is \( x \in X \) and \( B \in \mathcal{B} \) such that \( (x, B) \in I \). We consider automorphisms of \( \mathcal{D} \) as pairs of permutations on \( X \) and \( \mathcal{B} \) which preserve incidence, and call a group \( G \leq \text{Aut}(\mathcal{D}) \) of automorphisms of \( \mathcal{D} \) flag-transitive (respectively block-transitive, point \( t \)-transitive) if \( G \) acts transitively on the flags (respectively transitively on the blocks, \( t \)-transitively on the points) of \( \mathcal{D} \). For short, \( \mathcal{D} \) is said to be, e.g., flag-transitive if \( \mathcal{D} \) admits a flag-transitive group of automorphisms.

We call a \( t-(v, k, 1) \) design a Steiner \( t \)-design (sometimes this is also known as Steiner system). We note that in this case each block is determined by the set of points which are incident with it, and thus can be identified with a \( k \)-subset of \( X \) in a unique way. If furthermore \( t < k < v \) holds, then we speak of a non-trivial Steiner \( t \)-design.

As a consequence of the classification of the finite simple groups, it has been possible in recent years to characterize Steiner \( t \)-designs, mainly for \( t = 2 \), with sufficiently strong transitivity properties (for an overview, see [5].

Received by the editors April 24, 2003.

2000 Mathematics Subject Classification. Primary 51E10; Secondary 05B05, 20B25.

Key words and phrases. Steiner design, flag-transitive group of automorphisms, 2-transitive permutation group.

The author gratefully acknowledges support by the Deutsche Forschungsgemeinschaft (DFG).
Sect. 1, 2\]) \text{ and } [25, \text{ Sect. 2}]). Probably the most general results have been the classification of all point 2-transitive Steiner 2-designs in 1985 by W. M. Kantor [24, Thm. 1], and the almost complete determination of all flag-transitive Steiner 2-designs announced in 1990 by F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck and J. Saxl [6, 13, 27, 30] (see also [25, Sect. 3] for the incomplete case with a 1-dimensional affine group of automorphisms).

Nevertheless, for Steiner 3-designs such characterizations have remained challenging open problems. In particular, the classification of all flag-transitive Steiner 3-designs is known as “a long-standing and still open problem” (cf. [11, p. 147] and [12, p. 273]). Presumably, H. Lüneburg [28] in 1965 has been the first dealing with part of the problem characterizing flag-transitive Steiner 3-designs with block size $k = 4$ under the additional strong assumption that every non-identity element of the group of automorphisms fixes at most two points. This result has been generalized recently by the author [20], omitting the additional assumption. Moreover, in [21] the author determined all flag-transitive Steiner 3-designs with block size $k \leq 7$.

In this article, we completely classify all flag-transitive Steiner 3-designs with arbitrary block size. Our approach makes use of the classification of the finite 2-transitive permutation groups, which in turn relies on the classification of the finite simple groups. We state our result:

The classification of all non-trivial Steiner 3-designs with a flag-transitive group of automorphisms is as follows

**Main Theorem.** Let $D = (X, B, I)$ be a non-trivial Steiner 3-design. Then $G \leq \text{Aut}(D)$ acts flag-transitively on $D$ if and only if one of the following occurs:

1. $D$ is isomorphic to the $3$-$(2^d, 4, 1)$ design whose points and blocks are the points and planes of the affine space $AG(d, 2)$, and one of the following holds:
   (i) $d \geq 3$, and $G \cong AGL(d, 2)$,
   (ii) $d = 3$, and $G \cong AGL(1, 8)$ or $AFL(1, 8)$,
   (iii) $d = 4$, and $G_0 \cong A_7$,
   (iv) $d = 5$, and $G \cong AFL(1, 32)$,

2. $D$ is isomorphic to a $3$-$(q^e + 1, q + 1, 1)$ design whose points are the elements of the projective line $GF(q^e) \cup \{\infty\}$ and whose blocks are the images of $GF(q) \cup \{\infty\}$ under $PGL(2, q^e)$ (respectively $PSL(2, q^e)$, $e$ odd) with a prime power $q \geq 3$, $e \geq 2$, and the derived design at any given point is isomorphic to the $2$-$(q^e, q, 1)$ design whose points and blocks are the points and lines of $AG(e, q)$, and $PSL(2, q^e) \leq G \leq PGL(2, q^e)$,
(3) \( \mathcal{D} \) is isomorphic to a \( 3-(q+1,4,1) \) design whose points are the elements of \( GF(q) \cup \{ \infty \} \) with a prime power \( q \equiv 7 \pmod{12} \) and whose blocks are the images of \( \{0,1,\varepsilon,\infty\} \) under \( PSL(2,q) \), where \( \varepsilon \) is a primitive sixth root of unity in \( GF(q) \), and the derived design at any given point is isomorphic to the Netto triple system \( N(q) \), and \( PSL(2,q) \leq G \leq P\Sigma L(2,q) \).

(4) \( \mathcal{D} \) is isomorphic to the Witt \( 3-(22,6,1) \) design, and \( G \geq M_{22} \).

A detailed description of the Netto triple system \( N(q) \) can be found in [14, Sect. 3].

2. Definitions and Preliminary Results

If \( \mathcal{D} = (X, \mathcal{B}, I) \) is a \( t-(v,k,\lambda) \) design with \( t \geq 2 \), and \( x \in X \) arbitrary, then the derived design with respect to \( x \) is \( \mathcal{D}_x = (X_x, \mathcal{B}_x, I_x) \), where \( X_x = X \setminus \{x\}, \mathcal{B}_x = \{B \in \mathcal{B} : (x, B) \in I\} \) and \( I_x = I|_{X_x \times \mathcal{B}_x} \). In this case, \( \mathcal{D} \) is also called an extension of \( \mathcal{D}_x \). Obviously, \( \mathcal{D}_x \) is a \( (t-1)-(v-1,k-1,\lambda) \) design.

Let \( G \) be a permutation group on a non-empty set \( X \). For \( g \in G \), let \( \text{Fix}(g) \) denote the set of fixed points of \( g \) in \( X \). We call \( G \) semi-regular if the identity is the only element that fixes a point of \( X \). If additionally \( G \) is transitive, then it is said to be regular. If \( \{x_1, \ldots, x_m\} \subseteq X \), let \( G_{x_1,\ldots,x_m} \) be its setwise stabilizer and \( G_{x_1,\ldots,x_m} \) its pointwise stabilizer (for short, we often write \( G_{x_1,\ldots,x_m} \) in the latter case).

For \( \mathcal{D} = (X, \mathcal{B}, I) \) a Steiner \( t \)-design with \( G \leq \text{Aut}(\mathcal{D}) \), let \( G_B \) denote the setwise stabilizer of a block \( B \in \mathcal{B} \), and for \( x \in X \), we define \( G_{xB} = G_x \cap G_B \).

Let \( \mathbb{N} \) be the set of positive integers (in this article, \( 0 \notin \mathbb{N} \)). For \( d \in \mathbb{N} \), let \( \Phi_d(x) \) denote the \( d \)-th cyclotomic polynomial in \( \mathbb{Q}[x] \), and for \( 2 \leq q \in \mathbb{N} \), we define

\[
\Phi_d^*(q) = \frac{1}{f^n} \Phi_d(q),
\]

where \( f = (d, \Phi_d(q)) \) and \( f^n \) is the largest power of \( f \) dividing \( \Phi_d(q) \) if \( f \neq 1 \), and \( n = 1 \) otherwise (cf. [18, p. 431]).

Let \( m \) and \( n \) be integers and \( p \) a prime. Then \( (m,n) \) is the greatest common divisor of \( m \) and \( n \). We write \( m \mid n \) if \( m \) divides \( n \), and \( p^m \parallel n \) if \( p^m \) divides \( n \) but \( p^{m+1} \) does not divide \( n \). For \( 2 \leq q \in \mathbb{N} \), we mean by \( \mathfrak{p} \perp q^n - 1 \) that \( \mathfrak{p} \) divides \( q^n - 1 \) but not \( q^m - 1 \) for all \( 1 \leq m < n \).

For any \( x \in \mathbb{R} \), let \( \lfloor x \rfloor \) (respectively \( \lceil x \rceil \)) denote the greatest positive integer which is at most (respectively the smallest positive integer which is at least) \( x \).

All other notation is standard.
The starting point for our investigation to determine all flag-transitive Steiner 3-designs is the following result.

**Proposition 1.** Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner $t$-design with $t \geq 3$. If $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on $\mathcal{D}$, then $G$ also acts point 2-transitively on $\mathcal{D}$.

**Proof.** Let $x \in X$ arbitrary. As $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on $\mathcal{D}$, obviously $G_x$ acts block-transitively on the derived Steiner $(t - 1)$-design $\mathcal{D}_x$. Since block-transitivity implies point-transitivity for non-trivial Steiner $t$-designs with $t \geq 2$ by a theorem of Block [4, Thm. 2], $G_x$ also acts point-transitively on $\mathcal{D}_x$, and the claim follows. □

We note that if $t = 2$, then it is elementary that conversely the point 2-transitivity of $G \leq \text{Aut}(\mathcal{D})$ implies its flag-transitivity.

The above proposition allows us to make use of the classification of all finite 2-transitive permutation groups, which itself relies on the classification of all finite simple groups (cf. [10, 17, 18, 19, 22, 24, 29]).

The list of groups is as follows.

Let $G$ be a finite 2-transitive permutation group on a non-empty set $X$. Then $G$ is either of

(A) **Affine Type:** $G$ contains a regular normal subgroup $T$ which is elementary Abelian of order $v = p^d$, where $p$ is a prime. If $a$ divides $d$, and if we identify $G$ with a group of affine transformations

$$x \mapsto x^g + u$$

of $V = V(d, p)$, where $g \in G_0$ and $u \in V$, then particularly one of the following occurs:

1. $G \leq \text{AGL}(1, p^d)$
2. $G_0 \cong \text{SL}(\frac{d}{a}, p^a)$, $d \geq 2a$
3. $G_0 \cong \text{Sp}(\frac{2d}{a}, p^a)$, $d \geq 2a$
4. $G_0 \cong G_2(2^a)'$, $d = 6a$
5. $G_0 \cong A_6$ or $A_7$, $v = 2^4$
6. $G_0 \cong SL(2, 3)$ or $SL(2, 5)$, $v = p^2$, $p = 5, 7, 11, 19, 23, 29$ or 59, or $v = 3^4$
7. $G_0$ contains a normal extraspecial subgroup $E$ of order $2^5$, and $G_0/E$ is isomorphic to a subgroup of $S_5$, $v = 3^4$
8. $G_0 \cong SL(2, 13)$, $v = 3^6$, or

(B) **Almost Simple Type:** $G$ contains a simple normal subgroup $N$, and $N \leq G \leq \text{Aut}(N)$. In particular, one of the following holds, where $N$ and $v = |X|$ are given as follows:
(1) $A_v, v \geq 5$

(2) $PSL(d, q), d \geq 2, v = \frac{q^d - 1}{q - 1}, \text{ where } (d, q) \neq (2, 2), (2, 3)$

(3) $PSU(3, q^2), v = q^3 + 1, q > 2$

(4) $Sz(q), v = q^2 + 1, q = 2^{2e+1} > 2$ (Suzuki groups)

(5) $Re(q), v = q^3 + 1, q = 3^{2e+1} > 3$ (Ree groups)

(6) $Sp(2d, q), d \geq 3, v = 2^{2d-1} + 2^{d-1}$

(7) $PSL(2, 11), v = 11$

(8) $PSL(2, 8), v = 28$ (N is not 2-transitive)

(9) $M_v, v = 11, 12, 22, 23, 24$ (Mathieu groups)

(10) $M_{11}, v = 12$

(11) $A_7, v = 15$

(12) $HS, v = 176$ (Higman-Sims group)

(13) $Co_3, v = 276.$ (smallest Conway group)

For basic properties of the listed groups, we refer, e.g., to [9] and [20, Ch. 2, 5].

We will now indicate some helpful combinatorial tools on which we rely in the sequel. Let $r$ (respectively $\lambda_2$) denote the total number of blocks incident with a given point (respectively pair of distinct points), and let all further parameters be as defined at the beginning of Section 1.

Obvious is the subsequent fact.

**Lemma 2.** Let $D = (X, \mathcal{B}, I)$ be a Steiner $t$-design. If $G \leq \text{Aut}(D)$ acts flag-transitively on $D$, then, for any $x \in X$, the division property

$$r \mid |G_x|$$

holds.

Elementary counting arguments give the following standard assertions.

**Lemma 3.** If $D = (X, \mathcal{B}, I)$ is a $t$-$(v, k, \lambda)$ design, then the following holds:

(a) $bk = vr$.

(b) $\left(\begin{array}{c} v \\ t \end{array}\right) \lambda = b \left(\begin{array}{c} k \\ t \end{array}\right)$.

(c) $r(k - 1) = \lambda_2(v - 1)$ for $t \geq 2$, where $\lambda_2 = \frac{\lambda(v - 2)}{k - 2}$.

(d) In particular, if $t = 3$, then $(k - 2)\lambda_2 = v - 2.$
For non-trivial Steiner $t$-designs lower bounds for $v$ in terms of $k$ and $t$ can be indicated.

**Proposition 4.** (Cameron [7].) Let $D = (X, B, I)$ be a non-trivial Steiner $t$-design. Then the following holds:

(a) $v \geq (t+1)(k-t+1)$.
(b) $v - t + 1 \geq (k-t+2)(k-t+1)$ for $t > 2$. If equality holds, then $(t, k, v) = (3, 4, 8), (3, 6, 22), (3, 12, 112), (4, 7, 23)$, or $(5, 8, 24)$.

We note that (a) is stronger for $k < 2(t-1)$, while (b) for $k > 2(t-1)$.

As we are in particular interested in the case when $t = 3$, we deduce from (b) the following upper bound for the positive integer $k$.

**Corollary 5.** Let $D = (X, B, I)$ be a non-trivial Steiner 3-design. Then the block size $k$ can be estimated by

$$k \leq \left\lfloor \sqrt{v + \frac{3}{2}} \right\rfloor.$$

**Remark 6.** If $G \leq \text{Aut}(D)$ acts flag-transitively on any Steiner 3-design $D$, then applying Proposition 4 and Lemma 3 (b) yields the equation

$$b = \frac{v(v-1)(v-2)}{k(k-1)(k-2)} = \frac{v(v-1)|G_{xy}|}{|G_B|},$$

where $x$ and $y$ are two distinct points in $X$ and $B$ is a block in $B$, and thus

$$v - 2 = (k-1)(k-2)\frac{|G_{xy}|}{|G_B|} \text{ if } x \in B.$$

### 3. Cases with a Group of Automorphisms of Affine Type

In the following, we begin with the proof of the Main Theorem. Using the notation as before, let $D = (X, B, I)$ be a non-trivial Steiner 3-design with $G \leq \text{Aut}(D)$ acting flag-transitively on $D$. Let us recall that in view of Proposition 1 we can restrict ourselves to the inspection of the finite 2-transitive permutation groups listed in Section 2. Before we consider in this section successively those cases where $G$ is of affine type, we prove some lemmas which will be required for Case (1).

**Lemma 7.** Let $q = p^d$ with $p \neq 2$ a prime. Furthermore, let $2^m \parallel p-1$, $2^m \parallel p+1$ and $2^n \parallel d$ for some integers $m$, $n$, and $n$. Then $2^{m+n} \parallel q-1$, unless $p \equiv 3 \pmod{4}$ and $d \equiv 0 \pmod{2}$, in which case $2^{m+n} \parallel q-1$.

**Proof.** This follows from Lemma 3.2] using induction over $n$. \qed
Maintaining the same parameters, we obtain

**Lemma 8.** Let $G \leq A\Gamma L(1, q)$ be a 2-transitive permutation group, where $q = p^d$ with $p \neq 2$ a prime, and $P$ a Sylow $2$-subgroup of $G$. Then we have $|P \cap AGL(1, q)| \geq 2^n$. Moreover, if $p \equiv 3 \pmod{4}$ and $d \equiv 0 \pmod{2}$, then $|P \cap AGL(1, q)| \geq 2^m$.

**Proof.** Clearly,

$$\frac{|P|}{|P \cap AGL(1, q)|} \cdot d.$$ 

As $q(q - 1) | |G|$ by the 2-transitivity of $G$, Lemma 7 yields

$$2^{m+n} \cdot |P| \cdot |P \cap AGL(1, q)| \cdot 2^n,$$

and therefore

$$2^m \cdot |P \cap AGL(1, q)|.$$ 

If $p \equiv 3 \pmod{4}$ and $d \equiv 0 \pmod{2}$, then we have $2^{m+n} | q - 1$, and hence $2^m | |P \cap AGL(1, q)|$. □

**Lemma 9.** Let $G \leq A\Gamma L(1, q)$ be a 2-transitive permutation group, where $q = p^d$ with $p \neq 2$ a prime. Then $G$ contains an involution which fixes exactly one point.

**Proof.** Clearly, $AGL(1, q)_0$ is isomorphic to $GL(1, q)$, and hence cyclic. It has index $q$, which is odd, and contains therefore a Sylow 2-subgroup of $AGL(1, q)$. Thus, each involution in $AGL(1, q)$ has exactly one fixed point, and the claim follows by applying Lemma 8 □

We shall now turn to the examination of those cases where $G \leq \text{Aut}(\mathcal{D})$ is of affine type.

**Case (1):** $G \leq A\Gamma L(1, v)$, $v = p^d$.

First, we will show by contradiction that $v$ is a power of 2. Indeed, we suppose that $p \neq 2$. Let $T$ denote the translation subgroup of $G$. By Lemma 9, we know that $G$ contains an involution $\tau$ which has exactly one fixed point $x \in X$. Then, for distinct $x, y \in X$, the 3-subset $S = \{x, y, y^\tau\}$ is invariant under $\tau$. But, $S$ is incident with a unique block $B \in \mathcal{B}$ by the definition of Steiner 3-designs, hence $\tau \in G_B$. Since $G$ is flag-transitive, $G_B$ acts transitively on the points of $B$. Therefore, for each point $x \in B$, there exists an involution $\tau_x$ having only $x$ as fixed point. Hence

$$U := \langle \tau_x^{G_B} \rangle \leq \langle \tau_x^{A\Gamma L(1, v)} \rangle = \langle \tau_x \rangle \cdot T,$$

whereas for the latter we use that $\tau_x$ induces on $T$ the inverse map $\alpha : x \mapsto x^{-1}$ because any involutory automorphism of $T$ which has no fixed point distinct
from 1 must be equal to $\alpha$. Therefore, we have $\tau_x \in AGL(1, v) \aleq AGL(1, v)$. Then, by Dedekind’s law,

$$U = \langle \tau_x \rangle \cdot (U \cap T).$$

But, as $U$ acts transitively on the points of $B$ and clearly $\langle \tau_x \rangle \cap (U \cap T) = 1$, it follows from the orbit-stabilizer property that $U \cap T$ acts also transitively on the points of $B$. Thus, $B$ is a point-orbit under $U \cap T$ and therefore a subspace of $AG(d, p)$. Since $G$ is block-transitive, we conclude that all blocks must be affine subspaces.

Let $G$ be a line in $AG(d, p)$ with distinct points $x, y \in G$. Let $B$ and $\overline{B}$ be two distinct blocks containing $\{x, y\}$. As $p \neq 2$ and since affine subspaces contain with any two distinct points also the line connecting them, it follows that $G \subseteq B \cap \overline{B}$ with $|G| > 2$, a contradiction. Thus, we have shown that $v = 2^d$.

In the following, we will prove that if the block size $k$ is a power of 2, then only $k = 4$ can occur. Therefore, we can use the classification of all flag-transitive Steiner quadruple systems [20], which gives the designs described in part (1) of the Main Theorem with the assertions (ii) and (iv). To exclude trivial Steiner 3-designs, let $k = 2^a$, $1 < a < d$. As $d = 3$ yields $k = 4$, we may assume that $d > 3$. From Remark 6, it follows that

$$(1) \quad v - 2 \mid d(k - 1)(k - 2).$$

Combining this with [18, Thm. 3.3 (a)] gives

$$(2) \quad \Phi_{d-1}^*(2) \mid 2^{d-1} - 1 \mid d(2^a - 1)(2^{a-1} - 1).$$

Clearly, $a < d - 1$ (otherwise, $k = 2^{d-1}$, a contradiction to Corollary 5). If $\Phi_{d-1}^*(2) = 1$, then, by [18, Thm. 3.5], there exists no non-trivial 2-primitive prime divisor of $2^{d-1} - 1$, and hence $d = 7$ in view of Zsigmondy’s theorem (see [33, p. 283]). By using [11, Lemma 3 (d) and Corollary 4] we can easily check the very small number of possibilities for $k$. It turns out that only $k = 4$ can occur. Thus, we may assume that $d > 3$. As $\Phi_{d-1}^*(2) = 1$ has already been considered, we may suppose that $\Phi_{d-1}^*(2) = \Phi_{d-1}^*(2)$. Now [18, Thm. 3.9 (b)] yields $d \leq 19$. The small number of cases can easily be checked by hand as above. Again, it turns out that only $k = 4$ can occur.
Let us suppose now that $k$ is no power of 2. We distinguish two cases according as some non-trivial translation preserves a block $B \in \mathcal{B}$ or not. Let $T_B \neq 1$. Then $B$ is a disjoint union of affine subspaces $X_i$ of $AG(d, 2)$, $i \geq 1$ (namely the point-orbits $X_i$ of $T_B$ contained in $B$). As $k$ is no power of 2, we may assume that $i \geq 2$. Let $x_i \in X_i$. Then the translation $t$ mapping $x_1$ onto $x_i$ maps $B$ onto some other block $B_i$ (because $t \notin T_B$).

Since $X_i \subseteq B \cap B_i$ and $|X_i| \geq p = 2$, it follows from the definition of Steiner 3-designs that $|X_i| = 2$ for each $i$. Therefore, $|G_B \cap T| = |T_B| = 2$. Without restriction, we may assume that $T_B = \langle x \mapsto x + 1 \rangle$. Thus

$$G_B \leq \mathcal{C}_{AGL(1, v)}(T_B) = T \cdot \langle \alpha \rangle,$$

where $\mathcal{C}_{AGL(1, v)}(T_B)$ denotes the centralizer of $T_B$ in $AGL(1, v)$ and $\alpha$ the Frobenius automorphism $GF(v) \to GF(v)$, $x \mapsto x^2$. Hence

$$G_B/T_B \cong G_B : T/T$$

is isomorphic to a subgroup of

$$\mathcal{C}_{AGL(1, v)}(T_B)/T \cong \langle \alpha \rangle.$$

Because of the transitivity of $G_B$ on the points of $B$, we conclude that $k \mid |G_B| \mid 2d$. Therefore, $v - 2 < 4d^3$ by (1), and the small number of possibilities for $k$ can easily be eliminated by hand using (1) and Lemma 3 (d). Now, let $T_B = 1$. We first show that $G_B \leq G_y$ for some $y \notin B$. Let $G^* = G_B \cap AGL(1, v)$. Then $G^*$ is conjugated to a subgroup of $G_0$ by Hall’s theorem. If $G^* = 1$, then $G_B$ is isomorphic to a subgroup of $\langle \alpha \rangle$, hence cyclic and $|G_B| \mid d$. As $G_B$ acts transitively on the points of $B$, we obtain $k \mid d$, and thus $v - 2 < d^3$ by (1). The very few possibilities for $k$ can easily be ruled out by hand as before. Therefore, $G^* \neq 1$. By construction, $G^*$ has only the point 0 as fixed point. Since $G^* \leq G_B$, obviously $G_B$ fixes the set of fixed points of $G^*$, i.e. the point 0. Hence $G_B \leq G_0$, and $0 \notin B$ by the flag-transitivity of $G$.

As $G$ is point 2-transitive, we have $|G| = v(v-1)a$ with $a \mid d$. Then Remark 5 yields

$$v - 2 = (k - 1)(k - 2)\frac{a}{|G_{xB}|} \quad \text{if } x \in B.$$  

(3)

As $G_B$ fixes some $y \notin B$, it follows that $|G_{xB}| \mid |G_{xy}| = a$.

If $G_{0x}$ fixes three or more distinct points, then $G_{0x}$ would fix some block $\overline{B} \in \mathcal{B}$. Thus, we have $a \mid |G_{xB}|$, and therefore $v - 2 = (k - 1)(k - 2)$. However, as $d > 3$, it follows from Proposition 4 (b) that $v - 2 > (k - 1)(k - 2)$, a contradiction. Hence, $G_{0x}$ fixes only 0 and $x$. Then $G_{0x}$ must contain a field automorphism of order $d$, and we conclude that $G = AGL(1, 2^d)$.

Let $p$ be a prime divisor of $d$, say $d = ps$. Then $(G_{0x})^p$ fixes at least three distinct points, and hence we have $s \mid |G_{xB}|$. If there exists a further prime divisor $p$ of $d$ with $p \neq p$, then the quotients $d/p$ and $d/p$ both divide the order of $G_{xB}$ by the flag-transitivity of $G$. Therefore, we obtain $d \mid |G_{xB}|$, which gives the contradiction $a = d$ as above.
Thus, we have $d = p^n$ for some $n \in \mathbb{N}$, and therefore $p^{n-1} = s \mid |G_xB|$. Now, it follows that $|G_xB| = p^{n-1}$, and hence $|G_B| = kp^{n-1} \mid (v-1)p^n$. This shows that $k \mid (v-1)p$. If we set $c = (k, p)$, then $c = 1$ or $p$, and we obtain $\frac{k}{c} \mid v - 1$. Comparing this with equation (3) yields

$$v - 2 = (k - 1)(k - 2)\frac{p^n}{p^n - 1},$$

and hence

$$-1 \equiv 2p \left( \mod \frac{k}{c} \right).$$

Therefore, we have

$$\frac{k}{c} \leq 2p + 1,$$

and finally

$$2^{p^n} - 2 = v - 2 = (k - 1)(k - 2)p \leq (2p^2 + p - 1)(2p^2 + p - 2)p.$$

This leaves only a small number of cases to check. As $k \mid (2^{p^n} - 1)p$, and $k \geq \left\lceil \sqrt{\frac{2^{p^n} - 2}{p^n} + \frac{3}{2}} \right\rceil$ by (11), these can again easily be eliminated by hand using Lemma 3 (c) and (d), and Corollary 5.

**Case (2):** $G_0 \geq SL(\frac{d}{a}, p^a)$, $d \geq 2a$.

In the following, let $e_i$ denote the $i$-th unit vector of the vector space $V = V(\frac{d}{a}, p^a)$, and $\langle e_i \rangle$ the 1-dimensional vector subspace spanned by $e_i$. We will show that only the flag-transitive designs described in part (1) of the Main Theorem with $d \geq 3$ and $G \cong AGL(d, 2)$ can occur.

First, let $p^a \neq 2$. For $d = 2a$, let $U = U(\langle e_1 \rangle) \leq G_0$ denote the subgroup of all transvections with axis $\langle e_1 \rangle$. Then $U$ consists of all elements of the form

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \quad c \in GF(p^a) \text{ arbitrary.}$$

Clearly, $U$ fixes as points only the elements of $\langle e_1 \rangle$. Hence, $G_0$ has point-orbits of length at least $p^a$ outside $\langle e_1 \rangle$. Now, let $x \in \langle e_1 \rangle$ be distinct from 0 and $e_1$. Obviously, $U$ fixes the unique block $B \in \mathcal{B}$ which is incident with the 3-subset $\{0, e_1, x\}$. Thus, if $B$ contains at least one point outside $\langle e_1 \rangle$, then we would obtain $k \geq p^a + 3$. But, according to Corollary 5, we have $k \leq p^a + 1$, a contradiction. Therefore, $B$ is contained completely in $\langle e_1 \rangle$. Hence, as $G$ is flag-transitive, we may conclude that each block lies in an affine line. But, by the definition of Steiner 3-designs, any three distinct non-collinear points must also be incident with a unique block, a contradiction.
For \( d \geq 3a \), we consider \((\frac{d}{a} \times \frac{d}{a})\)-matrices of the form

\[
A_i = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 \\
x_1 & B_i & & & \\
0 & & \ddots & & \\
\vdots & & & \ddots & \\
0 & & & & 1
\end{pmatrix}, \ 1 \leq i \leq \frac{d}{a} - 1, \ x_1 \in GF(p^a) \text{ arbitrary},
\]

where

\[
B_1 = \begin{pmatrix}
x_2 & x_3 & x_4 & \cdots & x_{\frac{d}{a}} \\
0 & x_2^{-1} & 1 & \ast & \\
0 & 0 & 1 & \ddots & \\
\vdots & 0 & \ddots & \ddots & \\
0 & 0 & \ddots & \ddots & 1
\end{pmatrix}, \ x_2 \neq 0,
\]

\[
B_2 = \begin{pmatrix}
x_3^{-1} & 0 & & & \\
0 & x_3^{-1} & \ast & & \\
0 & 0 & 1 & \ddots & \\
\vdots & 0 & \ddots & \ddots & \\
0 & 0 & \ddots & \ddots & 1
\end{pmatrix}, \ x_3 \neq 0,
\]

\[
B_i = \begin{pmatrix}
x_{i+1} & x_{i+2} & \cdots & x_{\frac{d}{a}} \\
0 & 0 & \cdots & 0 & x_{i+1} \\
0 & 1 & \ddots & \ddots & \ddots \\
\vdots & \ddots & \ddots & \ddots & 0 \\
x_{i+1}^{-1} & 0 & \cdots & 0 & 1 \\
\vdots & 0 & \ddots & \ddots & \ddots \\
0 & 0 & \cdots & 1 & 1
\end{pmatrix}, \ x_{i+1} \neq 0, \ 3 \leq i \leq \frac{d}{a} - 1.
\]

Obviously, \( B_i \in SL(\frac{d}{a} - 1, p^a) \) for \( 1 \leq i \leq \frac{d}{a} - 1 \), and hence \( A_i \in SL(\frac{d}{a}, p^a) \epsilon_1 \) by Laplace’s expansion theorem. By multiplying \( e_2 \) with the matrices \( A_i \) (\( 1 \leq i \leq \frac{d}{a} - 1 \)), we obtain as images exactly the vectors of \( V \setminus \langle e_1 \rangle \). Thus \( SL(\frac{d}{a}, p^a) \epsilon_1 \), and hence also \( G_{0, e_1} \), acts point-transitively outside \( \langle e_1 \rangle \). Again, let \( x \in \langle e_1 \rangle \) be distinct from 0 and \( e_1 \). If the unique block \( B \in B \) which is incident with the 3-subset \( \{0, e_1, x\} \) contains some point outside \( \langle e_1 \rangle \), then it would already contain all points outside, thus at least \( p^{d - p^a} + 3 \) many, which obviously contradicts Corollary 5. Therefore, \( B \) lies completely in \( \langle e_1 \rangle \), and by the same argument as above, we obtain that here \( G \leq Aut(D) \) cannot act flag-transitively on any non-trivial Steiner 3-design \( D \).
Now, let \( p^a = 2 \). To obtain non-trivial Steiner 3-designs, let \( v = 2^d > 4 \). For \( v = 8 \), necessarily \( k = 4 \) must hold in view of Lemma 3 (c). For \( v > 8 \), we will show that also only Steiner quadruple systems can occur. Thus, applying [20] yields the claim. We remark that clearly any three distinct points are non-collinear in \( \text{AG}(d, 2) \) and hence define an affine plane. Let \( E = \langle e_1, e_2 \rangle \) denote the 2-dimensional vector subspace spanned by \( e_1 \) and \( e_2 \). We consider \((d \times d)\)-matrices of the form

\[
A_i = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 \\
0 & 1 & 0 & \cdots & 0 \\
x_1 & x_2 & B_i & \cdots & 0 \\
0 & 0 & \cdots & \cdots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & \cdots & 0 \\
\end{pmatrix}, \quad 1 \leq i \leq d - 2; \ x_1, x_2 \in GF(2) \text{ arbitrary}
\]

with

\[
B_1 = \begin{pmatrix}
x_3 & x_4 & x_5 & \cdots & x_d \\
0 & x_3^{-1} & 1 & \cdots & 0 \\
0 & 1 & \cdots & \cdots & 0 \\
\vdots & 0 & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 1 & 1 \\
\end{pmatrix}, \quad x_3 \neq 0,
\]

\[
B_2 = \begin{pmatrix}
0 & x_4 & x_5 & \cdots & x_d \\
x_4^{-1} & 0 & -1 & \cdots & 0 \\
0 & 1 & \cdots & \cdots & 0 \\
\vdots & 0 & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 1 & 1 \\
\end{pmatrix}, \quad x_4 \neq 0,
\]

and

\[
B_i = \begin{pmatrix}
0 & 0 & \cdots & 0 & x_{i+2} & x_{i+3} & \cdots & x_d \\
0 & 0 & \cdots & 0 & 1 & \cdots & \cdots & \cdots \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \cdots & 0 & 1 & \cdots & \cdots & \cdots \\
0 & 0 & \cdots & 0 & 1 & \cdots & \cdots & \cdots \\
\end{pmatrix}, \quad x_{i+2} \neq 0, \ 3 \leq i \leq d - 2.
\]

Analogously as above, \( B_i \in SL(d-2, 2) \) for \( 1 \leq i \leq d-2 \) and \( A_i \in SL(d, 2)E \). By multiplying \( e_3 \) with the matrices \( A_i \) (\( 1 \leq i \leq d - 2 \)), we obtain as images exactly the vectors of \( V \setminus E \). Hence \( SL(d, 2)E \), and therefore also \( G_0E \), acts point-transitively on \( V \setminus E \). If the unique block \( B \in B \) which is incident with the 3-subset \( \{0, e_1, e_2\} \) contains some point outside \( E \), then
it would already contain all points of $V \setminus \mathcal{E}$. But then, we would have $k \geq 2^d - 4 + 3 = 2^d - 1$, a contradiction to Corollary $\S$. Hence, $B$ lies completely in $\mathcal{E}$, and by the flag-transitivity of $G$, it follows that each block must be contained in an affine plane. Thus $k \leq 4$, and finally $k = 4$ as we exclude trivial Steiner 3-designs.

**Case (3):** $G_0 \geq Sp\left(\frac{2d}{a}, p^a\right)$, $d \geq 2a$.

We will prove by contradiction that $G \leq Aut(D)$ cannot act flag-transitively on any non-trivial Steiner 3-design $D$. First, let $p^a \neq 2$. The permutation group $PSp\left(\frac{2d}{a}, p^a\right)$ on the points of the associated projective space is a rank 3 group, and the orbits of the one-point stabilizer are known (e.g. [23, Ch. II, Thm. 9.15 (b)]). Thus, $G_0 \geq Sp\left(\frac{2d}{a}, p^a\right)$ has exactly two orbits on $V \setminus \langle x \rangle$ ($0 \neq x \in V$) of length at least

$$\frac{p^a(p^{2d-2a} - 1)}{p^a - 1} = \sum_{i=1}^{2d-2} p^{ia} > p^d.$$ 

Let $y \in \langle x \rangle$ be distinct from 0 and $x$. If the unique block which is incident with the 3-subset $\{0, x, y\}$ contains at least one point of $V \setminus \langle x \rangle$, then we would have $k > p^d + 3$. But, on the other hand, we have $k \leq p^d + 1$ by Corollary $\S$, a contradiction. Therefore, we can argue as in Case (2) to obtain the desired contradiction.

Now, let $p^a = 2$. To exclude trivial Steiner 3-designs, let $v = 2^{2d} > 4$. For $d = 2$ (here $Sp(4, 2) \cong S_6$ as well-known), Corollary $\S$ yields $k \leq 5$. As $k = 2 \nmid v - 2$ for $k = 5$, it is sufficient by Lemma $\S$ (d) to consider the case when $k = 4$. For $d > 2$, we will show that we can also restrict ourselves to Steiner quadruple systems. Hence, the claim follows from [23] again. It is easily seen that there are $2^{2d-1}(2^{2d} - 1)$ hyperbolic pairs in the non-degenerate symplectic space $V = V(2d, 2)$, and by Witt’s theorem, $Sp(2d, 2)$ is transitive on these hyperbolic pairs. Let $\{x, y\}$ denote a hyperbolic pair, and $\mathcal{E} = \langle x, y \rangle$ the hyperbolic plane spanned by $\{x, y\}$. As $\mathcal{E}$ is non-degenerate, we have the orthogonal decomposition

$$V = \mathcal{E} \perp \mathcal{E}^\perp.$$ 

Clearly, $Sp(2d, 2)_{\{x, y\}}$ stabilizes $\mathcal{E}^\perp$ as a subspace, which implies that $Sp(2d, 2)_{\{x, y\}} \cong Sp(2d - 2, 2)$. As $|Out(Sp(2d, 2))| = 1$, we have therefore

$$Sp(2d - 2, 2) \cong Sp(2d, 2)_{\{x, y\}} \leq Sp(2d, 2)_\mathcal{E} = G_0, \mathcal{E}.$$ 

Since $Sp(2d - 2, 2)$ acts transitively on the non-zero vectors of the $(2d - 2)$-dimensional symplectic subspace, it is easy to see that the smallest orbit on $V \setminus \mathcal{E}$ under $G_0, \mathcal{E}$ has length at least $2^{2d-2} - 1$. If the unique block $B \in B$ which is incident with the 3-subset $\{0, x, y\}$ contains some point in $V \setminus \mathcal{E}$, then we would have $k \geq 2^{2d-2} + 2$, a contradiction to Corollary $\S$. Thus, $B$ lies completely in $\mathcal{E}$, and with regard to the flag-transitivity of $G$, we conclude that each block must be contained in an affine plane. Therefore,
we have \( k \leq 4 \), and in particular \( k = 4 \) as trivial Steiner 3-designs are excluded.

**Case (4):** \( G_0 \supseteq G_2(2^a)' \), \( d = 6a \).

We will also show by contradiction that \( G \leq \text{Aut}(\mathcal{D}) \) cannot act flag-transitively on any non-trivial Steiner 3-design \( \mathcal{D} \). First, let \( a = 1 \). Then we have \( v = 2^6 = 64 \), and by Corollary \( 5 \) it follows that \( k \leq 9 \). But, on the other hand, we have \( |G_2(2)'| = 2^5 \cdot 3^3 \cdot 7 \) and \( |\text{Out}(G_2(2)')| = 2 \). Thus, in view of Lemma \( 2 \), we obtain

\[
r = \frac{63 \cdot 62}{(k-1)(k-2)} \quad |G_0| \quad 2^6 \cdot 3^3 \cdot 7.
\]

But this implies that \( k - 1 \) or \( k - 2 \) is a multiple of 31, a contradiction.

Now, let \( a > 1 \). As here \( G_2(2^a) \) is simple non-Abelian, it is sufficient to consider \( G_0 \supseteq G_2(2^a) \). The permutation group \( G_2(2^a) \) is of rank 4, and for \( 0 \neq x \in V \), the one-point stabilizer \( G_2(2^a)_x \) has exactly three orbits \( O_i \) \((i = 1, 2, 3)\) on \( V \setminus \langle x \rangle \) of length \( 2^a - 2^a, 2^a - 2^a, 2^a - 2^a \) (see, e.g., \( 1 \) or \( 8, \text{Thm. 3.1} \)). Thus, \( G_0 \) has exactly three orbits on \( V \setminus \langle x \rangle \) of length at least \( |O_i| \). Let \( y \in \langle x \rangle \) be distinct from 0 and \( x \). Again, we will show that the unique block \( B \in \mathcal{B} \) which is incident with the 3-subset \( \{0, x, y\} \) lies completely in \( \langle x \rangle \). If \( B \) contains at least one point of \( V \setminus \langle x \rangle \) in \( O_2 \) or \( O_3 \), then we would obtain as above a contradiction to Corollary \( 5 \). Thus, we only have to consider the case when \( B \) contains points of \( V \setminus \langle x \rangle \) which all lie in \( O_1 \). By \( 11 \), the orbit \( O_1 \) is exactly known, and we have

\[
O_1 = x\Delta \setminus \langle x \rangle,
\]

where \( x\Delta = \{ y \in V \mid f(x, y, z) = 0 \text{ for all } z \in V \} \) with an alternating trilinear form \( f \) on \( V \). Then \( B \) consists, apart from elements of \( \langle x \rangle \), exactly of \( O_1 \). Since \( |O_1| \neq 1 \), we can choose \( \langle \overline{x} \rangle \in x\Delta \) with \( \langle \overline{x} \rangle \neq \langle x \rangle \). Let \( \overline{y} \in \langle \overline{x} \rangle \) be distinct from 0 and \( \overline{x} \). Then, for symmetric reasons, the 3-subset \( \{0, \overline{x}, \overline{y}\} \) is also incident with the unique block \( B \). But, on the other hand, we have \( \overline{x}\Delta \neq x\Delta \) for \( \langle \overline{x} \rangle \neq \langle x \rangle \), a contradiction. Thus, \( B \) is contained completely in \( \langle x \rangle \), and we may argue as in the cases above.

**Case (5):** \( G_0 \cong A_6 \) or \( A_7 \), \( v = 2^4 \).

As \( v = 2^4 \), we have \( k \leq 5 \) by Corollary \( 5 \). If \( k = 4 \), then applying \( 20 \) yields the flag-transitive design described in part (1) of the Main Theorem with assertion (iii). For \( k = 5 \), we obtain with Lemma \( 3(d) \) a contradiction.

**Cases (6)-(8).**

For the existence of non-trivial Steiner 3-designs, we have in these cases only a small number of possibilities for \( k \) to check, which can easily be ruled out by hand using Lemma \( 3(b) \) and \( (d) \), and Corollary \( 5 \).
4. Cases with a Group of Automorphisms of Almost Simple Type

Maintaining the same notation, let $D = (X, B, I)$ be a non-trivial Steiner 3-design with $G \leq \text{Aut}(D)$ acting flag-transitively on $D$. We will examine in this section successively those cases where $G$ is of almost simple type.

Case (1): $N = A_v$, $v \geq 5$. Here, $G$ is 3-transitive and does not act on any non-trivial Steiner 3-design by [24, Thm. 3].

Case (2): $N = \text{PSL}(d, q)$, $d \geq 2$, $v = \frac{q^d - 1}{q - 1}$, where $(d, q) \neq (2, 2), (2, 3)$.

We distinguish two subcases:

(i) $N = \text{PSL}(2, q)$, $v = q + 1$.

Let $\bar{q} = q^e$, $e \geq 1$. Without restriction, we have here $q^e \geq 5$ as $\text{PSL}(2, 4) \cong \text{PSL}(2, 5)$, and $\text{Aut}(N) = \text{PGL}(2, q^e)$. First, we suppose that $G$ is 3-transitive. In view of [24, Thm. 3], we have then only the 3-$(q^e + 1, q + 1, 1)$ design described in part (2) of the Main Theorem (without the subcase in brackets) with $\text{PSL}(2, q^e) \leq G \leq \text{PGL}(2, q^e)$, $q \geq 3$, $e \geq 2$. Conversely, flag-transitivity holds as the 3-transitivity of $G$ implies that $G_x$ acts block-transitively on the derived Steiner 2-design $D_x$ for any $x \in X$. Since $\text{PGL}(2, q^e)$ is a transitive extension of $\text{AGL}(1, q^e)$, it is easily seen that the derived design at any given point of $G\Gamma \{q^e\} \cup \{\infty\}$ is isomorphic to the 2-$(q^e, q, 1)$ design consisting of the points and lines of $AG(e, q)$.

Now, we suppose that $G$ is 3-homogeneous but not 3-transitive. Since here $\text{PSL}(2, q^e)$ is a transitive extension of $AG^2L(1, q^e)$ (which is the group of all permutations of $G\Gamma \{q^e\}$ of the form $x \mapsto a^{i}x + c$ with $a, c \in G\Gamma \{q^e\}$, $a \neq 0$), we can deduce from [14] that the derived design at any given point is either $AG(e, q)$ with the lines as blocks or the Netto triple system $\tilde{N}(\Gamma)$.

Thus, part (2) of the Main Theorem holds with the subcase in brackets or part (3) with $\text{PSL}(2, q^e) \leq G \leq \text{PGL}(2, q^e)$ (where, for an odd prime $p$, we define $\text{PGL}(2, p^a) = \text{PSL}(2, p^a) \rtimes \langle \tau_a \rangle$ with $\tau_a \in \text{Sym}(G\Gamma \{p^a\} \cup \{\infty\}) \cong S_a$ of order $a$ induced by the Frobenius automorphism $\alpha : G\Gamma \{p^a\} \rightarrow G\Gamma \{p^a\}$, $x \mapsto x^p$). Conversely, in view of its 3-homogeneity, $G$ is also block-transitive. By the orbit-stabilizer property, we obtain $|\text{PSL}(2, q^e)_B| = |\text{PSL}(2, q)|$ and in view of [16, Ch. 12, p. 286] actually

$$\text{PSL}(2, q^e)_B \cong \text{PSL}(2, q)$$

for any $B \in B$. Since $\text{PSL}(2, q)$ acts 2-transitively on $k = q + 1$ points, it follows that in both cases flag-transitivity holds.

Finally, we assume that $G$ is not 3-homogeneous. As $\text{PGL}(2, q^e)$ is 3-homogeneous, the unique orbit under $\text{PGL}(2, q^e)$ on the 3-subsets of $X$ splits under $\text{PSL}(2, q^e)$ in exactly two orbits of equal length. Thus, $G$ has here exactly two orbits of equal length on the 3-subsets of $X$, and by the definition of Steiner 3-designs, it follows that $G$ has exactly two orbits (possibly}
of different length) on the blocks. Hence, \( G \leq \text{Aut}(\mathcal{D}) \) cannot act block-transitively, and therefore not flag-transitively, on any non-trivial Steiner 3-design \( \mathcal{D} \).

(ii) \( N = \text{PSL}(d, \tilde{q}), \ d \geq 3 \).

We have here \( \text{Aut}(N) = \text{PGL}(d, \tilde{q}) \times \langle \iota_{\beta} \rangle \), where \( \iota_{\beta} \) denotes the graph automorphism induced by the inverse-transpose map \( \beta : \text{GL}(d, \tilde{q}) \rightarrow \text{GL}(d, \tilde{q}), \ x \mapsto t(x^{-1}) \). We will prove by contradiction that \( G \leq \text{Aut}(\mathcal{D}) \) cannot act on any non-trivial Steiner 3-design \( \mathcal{D} \).

Let us first assume that \( d = 3 \). By the definition of Steiner 3-designs, we may choose in the underlying projective plane \( \text{PG}(2, \tilde{q}) \) three distinct non-collinear points \( x, y, z \in X \), which are incident with a unique block \( B \in \mathcal{B} \). We consider two subcases:

(a) \( B \) contains at least one further point of the triangle through \( x, y, z \).

(b) \( B \) does not contain any further point of the triangle.

\( \text{ad} \ (a) \): Let \( \mathcal{G} \) denote a line of \( \text{PG}(2, \tilde{q}) \). It is well-known that the translation group \( T(\mathcal{G}) \) operates regularly on the points of \( \text{PG}(2, \tilde{q}) \setminus \mathcal{G} \) and acts trivially on \( \mathcal{G} \). Thus, \( T(\mathcal{G}) \) fixes a block \( B \in \mathcal{B} \) if three or more distinct points of \( B \) lie on \( \mathcal{G} \). Therefore, the block mentioned in (a) must contain all points of \( \text{PG}(2, \tilde{q}) \setminus \mathcal{G} \), thus at least \( \tilde{q}^2 + 3 \) many. But, these are obviously more than half of the points of \( \text{PG}(2, \tilde{q}) \), a contradiction to \( k \leq \lfloor \frac{v}{4} + 2 \rfloor \) by Proposition 4 (a).

\( \text{ad} \ (b) \): The pointwise stabilizer of three distinct points in \( \text{SL}(3, \tilde{q}) \) consists precisely of the diagonal matrices, and hence has order \( (\tilde{q} - 1)^2 \) (see, e.g., [23, Ch. II, Thm. 7.2 (b)]). To this corresponds in \( \text{PSL}(3, \tilde{q}) \) a subgroup \( U \) of order

\[
\frac{1}{n}(\tilde{q} - 1)^2 \quad \text{with} \quad n = (3, \tilde{q} - 1).
\]

As \( U \) acts semi-regularly outside the triangle, we obtain \( n \) point-orbits of equal length \( \frac{1}{n}(\tilde{q} - 1)^2 \), since if \( U \) fixes some further point outside the triangle, then \( U \) would fix some non-degenerate quadrangle, and so would be the identity, a contradiction. Thus, we get

\[
k \geq 3 + \frac{1}{n}(\tilde{q} - 1)^2.
\]

On the other hand, we know that the block mentioned in (b) is an arc, and therefore contains at most \( \tilde{q} + 1 \) points for \( \tilde{q} \) odd or \( \tilde{q} + 2 \) points for \( \tilde{q} \) even (see, e.g., [15, Ch. 3.2, Thm. 24]). Only for \( \tilde{q} = 2 \) and 4 both conditions are fulfilled. But, with regard to Lemma 3 (d), there exist no non-trivial 3-(7, \( k, 1 \)) designs and 3-(21, \( k, 1 \)) designs. Therefore, for \( d = 3 \) we have shown that \( G \) cannot act on any non-trivial 3-(\( \tilde{q}^2 + \tilde{q} + 1, k, 1 \)) design.

Now, we consider the case when \( d > 3 \). Via induction over \( d \), we will verify that \( G \leq \text{Aut}(\mathcal{D}) \) cannot act on any non-trivial Steiner 3-design \( \mathcal{D} \). For this, let us assume that there is a counter-example with \( d \) minimal. Without restriction, we can choose three distinct points \( x, y, z \) from a hyperplane \( \mathcal{H} \) of \( \text{PG}(d - 1, \tilde{q}) \). First, we show that the unique block \( B \in \mathcal{B} \) which is
incident with the 3-subset \( \{x, y, z\} \) is contained completely in \( \mathcal{H} \). Analogously as above, the translation group \( T(\mathcal{H}) \) acts regularly on the points of \( PG(d - 1, \bar{q}) \setminus \mathcal{H} \), but trivially on \( \mathcal{H} \). If \( B \) contains at least one point outside \( \mathcal{H} \), then it would already contain all points of \( PG(d - 1, \bar{q}) \setminus \mathcal{H} \), thus at least \( \bar{q}^{d-1} + 3 \) many. However, as
\[
v = \frac{\bar{q}^{d-1} - 1}{q - 1} < 2\bar{q}^{d-1} \iff \bar{q}^d - 1 < 2(\bar{q}^d - \bar{q}^{d-1}) \iff 2\bar{q}^{d-1} - 1 < \bar{q}^d,
\]
these are more than half of the points of \( PG(d-1, \bar{q}) \), the same contradiction as above. Thus, \( \mathcal{H} \) induces a
\[3-(\frac{\bar{q}^{d-1} - 1}{q - 1}, k, 1)\] design,
on which \( G \) containing \( PSL(d - 1, \bar{q}) \) as simple normal subgroup operates. Inductively, we obtain the minimal counter-example for \( d = 3 \). But, as we have shown above, \( G \) with \( PSL(3, \bar{q}) \) as simple normal subgroup cannot act on any non-trivial \( 3-(\bar{q}^2 + \bar{q} + 1, k, 1) \) design, and the assertion follows.

**Case (3):** \( N = PSU(3, q^2) \), \( v = q^3 + 1, q = p^e > 2 \).

Here \( Aut(N) = P^I U(3, q^2) \), and \( |G| = (q^3+1)q^3\left(\frac{q^2-1}{n}\right) \) with \( n = (3, q+1) \) and \( a \mid 2ne \). Thus, from Remark 3 we obtain
\[q^2 + q + 1 = (k - 1)(k - 2)\frac{q^2 - 1}{n} = \frac{a}{|G_B|} \text{ if } x \in B.
\]
We will show by contradiction that \( G \leq Aut(D) \) cannot act flag-transitively on any non-trivial Steiner 3-design \( D \).

Let \( \{v_1, v_2, v_3\} \) be a basis of the non-degenerate hermitian vector space \( V = V(3, q^2) \) with
\[(v_2, v_2) = (v_1, v_3) = 1, \quad (v_1, v_1) = (v_3, v_3) = (v_1, v_2) = (v_2, v_3) = 0.
\]
For \( v = \sum_{i=1}^{3} a_i v_i \) and \( w = \sum_{i=1}^{3} b_i v_i \), \( (a_i, b_i) \in GF(q^2) \), we have then
\[(v, w) = a_1b_3^\tau + a_2b_2^\tau + a_3b_1^\tau,
\]
where \( \tau \) denotes the unique involutory automorphism \( GF(q^2) \to GF(q^2) \), \( x \mapsto x^q \). We deduce from the proof of [23, Ch. II, Thm. 10.12] that the cyclic group
\[
\left\{ \begin{pmatrix} c & -2 \\ c^{-2} & c \end{pmatrix} \mid c^{-2} \neq c, c \in GF(q^2)^* \right\}
\]
of linear transformations on \( V \) induces a group \( U \) of dilatations of order \( \frac{q^3+1}{n} \) on the associated projective space \( PG(2, q^2) \) with axis the non-absolute line \( \mathcal{G} \) consisting of the absolute points \( \langle (1, 0, 0) \rangle, \langle (0, 0, 1) \rangle \) and \( \langle (a_1, 0, a_3) \rangle \) with
\[a_1a_3^\tau + a_1^\tau a_3 = \text{Tr}(a_1a_3^\tau) = 0
\]
(where \( \text{Tr} \) denotes the trace map \( GF(q^2) \to GF(q), x \mapsto x + x^q \) and as center the pole of the axis, i.e. the non-absolute point \( \langle (0, 1, 0) \rangle \).
As it is customary (see, e.g., [2, p. 87]), we call in the following non-
absolute lines \( G \) and \( H \) perpendicular if \( G \) passes through the pole of \( H \) and \( H \) passes, therefore, through the pole of \( G \).

By the definition of Steiner 3-designs, we may choose three distinct absolute points on \( G \), which are incident with a unique block \( B \in B \). Let us first assume that \( B \) contains absolute points outside \( G \) which are all on \( H \). It is clear that \( U \) fixes each point of \( G \), and hence in particular \( B \). Furthermore, \( H \) intersects \( G \) in a non-absolute point \( x \) (see, e.g., [2, p. 88]). As \( U \) acts outside \( x \) semi-regularly on \( H \), we conclude that all point-orbits have length \( q + 1 \). If we choose now three distinct absolute points on \( H \), then they are also incident with the unique block \( B \). Thus, by the same arguments, \( U \) fixes each point of \( H \) and acts outside \( x \) semi-regularly on \( G \). Therefore, we have

\[
k = (n_1 + n_2)\frac{q + 1}{n}
\]

with \( n_1, n_2 \in \{1, 2, 3\} \). If \( n = 1 \), then obviously \( k = 2(q + 1) \), which is impossible in view of Lemma 3(d). Thus, \( n \neq 1 \). For \( n_1 + n_2 = 3 \), it follows from equation (4) that \( q^2 + q + 1 \mid (q - 1)^2 - q \), which is clearly not possible. In each of the other cases, polynomial division with remainder gives a contradiction to Lemma 3(d).

Now, we assume that \( B \) contains absolute points outside \( G \) which are not all on \( H \). By applying the same arguments as above, we obtain additionally a lattice of points such that

\[
k = n_1 n_2 \left( \frac{q + 1}{n} \right)^2 + (n_1 + n_2)\frac{q + 1}{n}
\]

with \( n_1, n_2 \) as above, which clearly contradicts Corollary 5.

Hence, we have shown that \( B \) is completely contained in \( G \). Thus, in view of the flag-transitivity of \( G \), each block is contained in a non-absolute line. But, by the definition of Steiner 3-designs, any three non-collinear absolute points must also be incident with a unique block, a contradiction.

Case (4): \( N = Sz(q), v = q^2 + 1, q = 2e + 1 > 2 \).

We have \( \text{Aut}(N) = Sz(q) \rtimes \langle \alpha \rangle \), where \( \alpha \) denotes the Frobenius automorphism \( GF(q) \rightarrow GF(q), x \mapsto x^2 \). Thus, by Dedekind’s law, \( G = Sz(q) \rtimes (G \cap \langle \alpha \rangle) \), and \( |G| = (q^2 + 1)q^2(q - 1)a \) with \( a \mid 2e + 1 \). It follows from Remark 4 that

\[
q + 1 = (k - 1)(k - 2)\frac{a}{|G_xB|} \quad \text{if} \ x \in B
\]

We will prove by contradiction that \( G \leq \text{Aut}(D) \) cannot act flag-transitively on any non-trivial Steiner 3-design \( D \).

Let us first remark that we only have one class of involutions in \( G \). Hence, every involution has exactly one fixed point, which lies in an appropriate block. Therefore, by the flag-transitivity of \( G \), there exists for every \( B \in B \)
always an involution \( \tau \in G_x \cap Sz(q) \) with \( x \in B \), and \( B \) can be regarded as the orbit of fixed points of involutions in \( G_B \cap Sz(q) \).

Since \( G \) is flag-transitive, we can restrict ourselves to consider the unique block \( B \in \mathcal{B} \) which is incident with the 3-subset \( \{0, 1, \infty\} \) of \( X \). As every non-identity element of \( Sz(q) \) fixes at most two distinct points, we have \( \text{Aut}(\langle \alpha \rangle) \) of subgroups of \( Sz(q) \) non-identity element of \( Sz(q) \) divisor \( G \) as the orbit of fixed points of involutions in \( G \) yields for \( q > 8 \), Zsigmondy’s theorem yields the existence of a 2-primitive prime divisor \( \ell \) with \( \ell \parallel q \pm 1 \). Then

\[
q + 1 = q^2 (q^2 - 1) \frac{a}{|G_{0B}|}.
\]

As \( q > 8 \), Zsigmondy’s theorem yields the existence of a 2-primitive prime divisor \( \ell \) with \( \ell \parallel q \pm 1 \). Then

\[
\ell \mid q + 1 = q^2 (q^2 - 1) \frac{a}{|G_{0B}|}.
\]

But now \( [15] \) Thm. 3.5 (ii)] yields \( (\ell, q) = 1 \) and \( \ell > a \) since \( \ell \equiv 1 \pmod{(2e + 1)} \). Therefore, we conclude that \( q = q \), a contradiction.

Let \( G_B \cap Sz(q) \) be conjugated to a subgroup of \( Sz(q) \) by the remark above, contrary to the fact that \( x \notin B \) by the flag-transitivity of \( G \). Thus, \( x \in B \) by the remark above. Hence \( (G_B \cap Sz(q)) \cap O_{\ell^2}(U) = 1 \), and therefore \( |G_{0B} \cap Sz(q)| \leq 4 \).

Let \( G_B \cap Sz(q) \) be conjugated to a subgroup of \( U \) with \( |U| = 4(q \pm 1) \), where \( \ell^2 = 2q \). Then \( |O_{\ell^2}(U)| = q \pm l + 1 \), and \( O_{\ell^2}(U) \) operates fixed-point-freely on \( X \) since \( (q \pm l + 1, q) = 1 \) and \( (q \pm l + 1, q^2 - 1) = 1 \). Thus \( (G_{0B} \cap Sz(q)) \cap O_{\ell^2}(U) = 1 \), and therefore \( |G_{0B} \cap Sz(q)| \leq 4 \).

Let \( G_B \cap Sz(q) \) be conjugated to a subgroup of \( U \) with \( |U| = 2(q - 1) \). Then \( |O_{\ell^2}(U)| = q - 1 \), and \( O_{\ell^2}(U) \) has two distinct fixed points in \( X \). As \( O_{\ell^2}(U) \) contains no involutions, these fixed points cannot lie in \( B \) by the remark above. Hence \( (G_B \cap Sz(q)) \cap O_{\ell^2}(U) = 1 \), and thus \( |G_{0B} \cap Sz(q)| \leq 2 \).

Since \( |G_{0B} \cap Sz(q)| \equiv 0 \pmod{2} \), we have therefore

\[
|G_{0B} \cap Sz(q)| = 2 \text{ or } 4.
\]

As \( G \cap \langle \alpha \rangle \leq G_{0B} \), and clearly \( (G_B \cap Sz(q)) \cap (G \cap \langle \alpha \rangle) = 1 \), we conclude that \( u = 2 \) or 4.

Finally, our equation

\[
u(q + 1) = (k - 1)(k - 2)
\]
yields for \( u = 2 \) that

\[
2^{2e+2} = k(k - 3),
\]
which is clearly impossible since \( e \geq 1 \). For \( u = 4 \), we obtain
\[
2^{2e+3} = k^2 - 3k - 2.
\]
By setting \( x = 2k-3 \) and \( n = 2e+5 \) this becomes the well-known generalized Ramanujan-Nagell equation
\[
x^2 - 17 = 2^n,
\]
which has exactly the four solutions \((x, n) = (5, 3), (7, 5), (9, 6), (23, 9)\) (see, e.g., [3] Thm. 3). As we have \( e \geq 1 \), it follows that \((e, k) = (2, 13)\) is the only solution of equation (5). But, by Lemma 3(b), this is impossible, which verifies the claim.

**Case (5):** \( N = \text{Re}(q), \ v = q^3 + 1, \ q = 3^{2e+1} > 3. \)

Here \( \text{Aut}(N) = \text{Re}(q) \rtimes \langle \alpha \rangle \), where \( \alpha \) denotes the Frobenius automorphism \( GF(q) \rightarrow GF(q), \ x \mapsto x^3 \). Thus, by Dedekind’s law, \( G = \text{Re}(q) \rtimes (G \cap \langle \alpha \rangle) \), and \( G = (q^3 + 1)q^3(q - 1)a \) with \( a \mid 2e + 1. \) From Remark 6 we hence obtain
\[
q^2 + q + 1 = (k - 1)(k - 2)|G|^{x_B} \text{ if } x \in B.
\]
We will also prove by contradiction that \( G \leq \text{Aut}(D) \) cannot act flag-transitively on any non-trivial Steiner 3-design \( D \).

We remark that we only have one class of involutions in \( G \). Thus, every involution fixes at least three distinct points, each of which lies in an appropriate block. Therefore, by the flag-transitivity of \( G \), there exists for every \( B \in \mathcal{B} \) always an involution \( \tau \in G_{x_B} \cap \text{Re}(q) \) with \( x \in B \).

We show furthermore that \( 9 \mid |G_{x_B} \cap \text{Re}(q)| \). Let \( P \) be a Sylow 3-subgroup of \( \text{Re}(q) \). According to [32], \( P \) contains a normal elementary Abelian subgroup \( \overline{P} \) of order \( q^2 \) containing \( Z(P) \). Thus, there exist subgroups \( U_1, U_2 \) of \( \overline{P} \) of order 3 with \( U_1 \leq Z(P), \ U_2 \nleq Z(P) \). As the stabilizer of three distinct points in \( \text{Re}(q) \) has order 2, we have \( \text{Fix}_X(U_1) = \text{Fix}_X(U_2) = \{x\} \) for some \( x \in X \). Hence, if \( U_1 \) and \( U_2 \) are conjugated in \( \text{Re}(q) \), then they are already conjugated in \( \text{Re}(q)_x \). But, as \( Z(P) \) is a characteristic subgroup of \( \text{Re}(q)_x \), this is impossible. Therefore, we have at least two distinct classes of subgroups of order 3 in \( \text{Re}(q) \), and the assertion follows by the definition of Steiner 3-designs.

Because of the block-transitivity of \( G \), we can restrict ourselves to consider the unique block \( B \in \mathcal{B} \) which is incident with the 3-subset \( \{0, 1, \infty\} \) of \( X \). Clearly, \( \langle \alpha \rangle \leq \text{Aut}(N)_{0, 1, \infty} \), and hence \( G \cap \langle \alpha \rangle \leq G_{0B} \) by the definition of Steiner 3-designs. Furthermore, obviously \( (G_{B} \cap \text{Re}(q)) \cap (G \cap \langle \alpha \rangle) = 1 \). Therefore, as \( G_{B} \) acts transitively on the points of \( B \), Dedekind’s law yields
\[
k = |0^G_B| = [G_{B} : G_{0B}] = [G_{B} \cap \text{Re}(q) : G_{0B} \cap \text{Re}(q)].
\]
Thus, \( G_{B} \cap \text{Re}(q) \) acts also transitively on the points of \( B \).
In the following, we will examine the list of subgroups of $Re(q)$ (cf. \cite{32}). As 9 divides the order of $G_B \cap Re(q)$, clearly $G_B \cap Re(q)$ cannot be conjugated to a subgroup of the normalizer of a Sylow 2-subgroup of $Re(q)$ of order $8 \cdot 7 \cdot 3$. By the same argument, $G_B \cap Re(q)$ cannot be conjugated to a subgroup of $U$ with $|U| = 6(q + 1 \pm 3l)$, where $l = 3^e$.

Let $G_B \cap Re(q)$ be isomorphic to $Re(\overline{q})$ for some $\overline{q} \geq 27$ such that $\overline{q}^n = q$, $m \geq 1$. Let $\overline{X} \subseteq X$ with $|\overline{X}| = \overline{q}^3 + 1$. We first show that only involutions may have fixed points in $X \setminus \overline{X}$. Let $g \in G$ with $o(g) = s$, where $s \neq 2$ is a prime. If $s \mid \overline{q} - 1$, then $g$ has two distinct fixed points in $\overline{X}$, and none in $X \setminus \overline{X}$ since the stabilizer of three distinct points in $Re(q)$ has order 2. For $s = 3$, clearly $g$ has exactly one fixed point, which lies in $\overline{X}$. If $s \mid \overline{q} + 1$, we show that $g$ has no fixed point in $X$. Obviously, $g$ has no fixed point in $\overline{X}$.

As $3 \nmid \overline{q} + 1$, we assume that $g$ has two distinct fixed points in $X \setminus \overline{X}$. But, as

$$q^3 - \overline{q}^3 = \left(\sum_{i=0}^{3n-1} (-1)^i \frac{q^3}{\overline{q}^{1+i}} - \overline{q}^2 + \overline{q} - 1\right)\overline{q} + 1,$$

and hence $(q^3 - \overline{q}^3 - 2, q^2 - \overline{q} + 1) = (2, \overline{q} + 1) = 2$, this is impossible. If $s \mid \overline{q} + 1 \pm 3\overline{q}$, we show again that $g$ has no fixed point in $X$. As $\overline{q}^3 + 1 = (\overline{q} + 1 + 3\overline{q})(\overline{q} + 1 - 3\overline{q})(\overline{q} + 1)$, it is obvious that $g$ has no fixed point in $\overline{X}$.

Since $3 \nmid \overline{q} + 1 \pm 3\overline{q}$, we assume in both cases that $g$ has two distinct fixed points in $X \setminus \overline{X}$. But, as $(\overline{q} + 1 + 3\overline{q})(\overline{q} + 1 - 3\overline{q}) = \overline{q}^2 - \overline{q} + 1$, and

$$q^3 - \overline{q}^3 = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{1} (-1)^{2+3i} \frac{q^3}{\overline{q}^{2+3i+j}} - \overline{q} - 1\right)\overline{q}^2 - \overline{q} + 1,$$

we have $(q^3 - \overline{q}^3 - 2, \overline{q}^2 - \overline{q} + 1) = (2, \overline{q}^2 - \overline{q} + 1) = 2$, a contradiction.

As $G_B \cap Re(q)$ acts transitively on the points of $B$, we have $B \subseteq \overline{X}$ or $B \subseteq X \setminus \overline{X}$. In the first case, equation (7) yields

$$k = \overline{q}^3 + 1,$$

while in the second

$$k = \frac{(\overline{q}^3 + 1)\overline{q}^3(\overline{q} - 1)}{n},$$

where $n$ is a power of 2, and $n \leq 8$ as the order of $Re(q)$ is divisible by 8 but not by 16.

We will prove now that none of these values of $k$ is possible. We assume first that $k = \overline{q}^3 + 1$. Clearly, $m > 1$ (otherwise, $k = q^3 + 1$, a contradiction to Corollary 5). Thus, we have

$$q^2 + q + 1 = \overline{q}^3(\overline{q} - 1)\frac{a}{|G_{0B}|}.$$

Zsigmondy’s theorem yields the existence of a 3-primitive prime divisor $\overline{q}$ with $\overline{q} \nmid 3^{3(2e+1)} - 1$. Then

$$\overline{q} \mid q^2 + q + 1 = \overline{q}^3(\overline{q} - 1)\frac{a}{|G_{0B}|}.$$
But now \[18\text{, Thm. 3.5 (ii)}\] yields \((r, q) = 1\) and \(r > a\) since \(r \equiv 1 \pmod{2e + 1}\). Therefore, we have \(\overline{q} = q\), a contradiction.

Now, we assume that \(k = \frac{(q^3 + 1)q^3(q - 1)}{n}\). Then

\[|G_{0B}| = \frac{|G_B \cap Re(q)|}{k} = n\overline{a},\]

where \(\overline{a} | a\). Here, \(n < 4\) since otherwise \((k - 1)(k - 2) \equiv 0 \pmod{4}\) by equation (6) and, by applying Lemma 3 (c), this would imply that \(q^3 - 1\) is divisible by 4, which is impossible since \(q - 1 \equiv 2 \pmod{8}\) in \(Re(q)\).

Thus, we may assume that \(n = 2\). Polynomial division with remainder gives

\[q^3 - 1 = \left(\sum_{i=0}^{m} \frac{2^{2i+1}q^3}{((q^3 + 1)q^3(q - 1))^{i+1}}\right)\left(\frac{(q^3 + 1)q^3(q - 1)}{2} - 2\right) + \frac{2^{2m+2}q^3}{(q^3 + 1)q^3(q - 1)^{m+1}} - 1\]

for a suitable \(m \in \mathbb{N}\) (such that

\[\deg\left(\frac{2^{2m+2}q^3}{(q^3 + 1)q^3(q - 1)^{m+1}} - 1\right) < \deg\left(\frac{(q^3 + 1)q^3(q - 1)}{2} - 2\right)\]

as is well-known). As \(8 | |Re(q)|\), clearly \((\frac{(q^3 + 1)q^3(q - 1)}{2})^{m+1}\) is divisible by \(2^{3(m+1)}\). Thus \(\frac{2^{2m+2}q^3}{(q^3 + 1)q^3(q - 1)^{m+1}} \neq 1\), yielding a contradiction to Lemma 3 (d).

Let \(G_B \cap Re(q)\) be conjugated to a subgroup of \(Re(q)_x\) \((x \in X)\). By the transitivity of \(G\), we can choose \(x\) as fixed point of an involution. Thus, \(x \in B\) for an appropriate block \(B \in \mathcal{B}\) by the remark above, contrary to the fact that \(x \notin B\) by the flag-transitivity of \(G\).

Let \(G_B \cap Re(q)\) be conjugated to a subgroup of \(PSL(2, q) \times \langle \tau \rangle\), where \(\tau\) denotes any involution in \(Re(q)\). By the remark above, we can choose \(\tau\) such that 0 is a fixed point under \(\tau\). As 9 must be a divisor of the order of \(G_B \cap Re(q)\), we can restrict ourselves to the examination of the following cases (cf. [10] Ch. 12, p. 285f.] or [28] Ch. II, Thm. 8.27):

(i) \(G_B \cap Re(q)\) is conjugated to \(PSL(2, \overline{q})\) or \(PSL(2, \overline{q}) \times \langle \tau \rangle\) for some \(\overline{q} \geq 2\tau\) such that \(\overline{q}^m = q, m \geq 1\).

Let \(X \subseteq X\) with \(|X| = \overline{q} + 1\). First, we show again that only involutions may have fixed points in \(X \setminus X\). Let \(g \in G\) with \(o(g) = s\), where \(s \neq 2\) is a prime. If \(s | \overline{q} - 1\), then \(g\) has two distinct fixed points in \(X\) and none in \(X \setminus X\). For \(s = 3\), clearly \(g\) has exactly one fixed point, which lies in \(X\). If \(s | \overline{q} + 1\), we show that \(g\) has no fixed point in \(X\). Obviously, \(g\) has no fixed point in \(X\). As \(3 \nmid \overline{q} + 1\), we
assume that \( g \) has two distinct fixed points in \( X \setminus X \). But, as
\[
q^3 - \overline{q} = \left( \sum_{i=0}^{\overline{m} - 1} (-1)^i \frac{q^3}{\overline{q} + 1} \right) \left( \overline{q} + 1 \right),
\]
and hence \((q^3 - \overline{q} - 2, \overline{q} + 1) = (2, \overline{q} + 1) = 2\), this is impossible.

Again, we have \( B \subseteq X \) or \( B \subseteq X \setminus X \). With equation (7), we obtain
\[
k = \overline{q} + 1,
\]
in the first case, while in the second
\[
k = \frac{\overline{q}(\overline{q}^2 - 1)}{n},
\]
where \( n \) is a power of 2, and \( n \leq 8 \) again.

We will prove now that none of the values of \( k \) is possible. We assume first that \( k = \overline{q} + 1 \). Then
\[
q^2 + q + 1 \mid \overline{q}(\overline{q} - 1) \alpha
\]
by equation (5). Since \((q^2 + q + 1, \overline{q}) = 1\) and \((q^2 + q + 1, \overline{q} - 1) = (3, \overline{q} - 1) = 1\), this is equivalent to
\[
q^2 + q + 1 \mid a,
\]
which is impossible as clearly \( a \leq q \). Now, we assume that \( k = \frac{\overline{q}(\overline{q}^2 - 1)}{n} \). Then
\[
|G_{0B}| = \frac{|G_B \cap Re(q)|}{k} = \frac{n\overline{\pi}}{2} \text{ or } n\overline{\alpha},
\]
where \( \overline{\pi} \mid a \). Considering the first yields
\[
\frac{(q^2 + q + 1)n}{2} = (k - 1)(k - 2)\frac{\alpha}{n}
\]
by equation (5). Clearly, \( n = 2 \) is impossible. If \( n = 4 \), then \( k = \frac{\overline{q}(\overline{q}^2 - 1)}{4} \) is divisible by 2 but not by 4. Thus, 4 is a divisor of \( k - 2 \), but not of the left side. For \( n = 8 \), we have \((k - 1)(k - 2) \equiv 0 \pmod{4}\), which is not possible as we have seen above.

Now, we assume that \(|G_{0B}| = n\overline{\alpha} \). Here, \( n < 4 \) again. For \( n = 2 \), we have \( k = \frac{\overline{q} - 1}{2} \). Then, polynomial division with remainder gives
\[
q^3 - 1 = \left( \sum_{i=0}^{\overline{m}} \frac{2^{2i+1}q^3}{(q^3 - \overline{q})^{i+1}} \right) \left( \frac{\overline{q}^3}{2} - \overline{q} \right) + \frac{2^{2\overline{m}+2}q^3}{(q^3 - \overline{q})^{\overline{m} + 1}} - \frac{\overline{q}^3}{2}
\]
for a suitable \( \overline{m} \in \mathbb{N} \). As \((q^2 - 1)^{\overline{m} + 1} \) is divisible by \( 2^{3(\overline{m} + 1)} \), clearly \( \frac{2^{2\overline{m}+2}q^3}{(q^3 - \overline{q})^{\overline{m} + 1}} \neq 1 \), yielding a contradiction to Lemma 3 (d).

(ii) \( G_B \cap Re(q) \) is conjugated to \( U \) or \( U \times \langle \tau \rangle \), where \( U \) is an elementary Abelian subgroup of order \( \overline{q} \mid q \) of \( PSL(2,q) \).

Let \( X \subseteq X \) with \( |X| = q + 1 \). Clearly, \( U \) operates regularly on \( \overline{q} \) points, and each non-identity element of \( U \) has \( \infty \) as only fixed point.
in $\overline{X}$ and none in $X \setminus \overline{X}$.

As $2 \nmid |U|$, it follows that $k = \overline{q}$ in both of the cases $B \subseteq \overline{X}$ and $B \subseteq X \setminus \overline{X}$. But, polynomial division with remainder gives

$$q^3 - 1 = \left( \sum_{i=0}^{m} \frac{2^i q^3}{\overline{q}^{i+1}} \right) (\overline{q} - 2) + \frac{2^{m+1} q^3}{\overline{q}^{m+1}} - 1$$

for a suitable $m \in \mathbb{N}$. As clearly $\frac{2^{m+1} q^3}{\overline{q}^{m+1}} \neq 1$, this leads to a contradiction to Lemma 3 (d) again.

(iii) $G_B \cap Re(q)$ is conjugated to $U$ or $U \times \langle \tau \rangle$, where $U$ is a semi-direct product of an elementary Abelian subgroup of order $\overline{q}$ with a cyclic subgroup of order $c$ of $PSL(2,q)$ with $c \mid \overline{q} - 1$ and $c \mid q - 1$.

Let $\overline{X} \subseteq X$ with $|X| = q + 1$. Again, we show that only involutions may have fixed points in $X \setminus \overline{X}$. Let $g \in G$ with $o(g) = s$, where $s \neq 2$ is a prime. If $s = 3$, then $g$ has exactly one fixed point, which lies in $\overline{X}$. If $s \mid c$, then $g$ has exactly two distinct fixed points, which lie in $\overline{X}$.

For $B \subseteq \overline{X}$, we deduce that $k = \overline{q}$ or $\overline{q} c$, and for $B \subseteq X \setminus \overline{X}$ that $k = \overline{q} c$ with $n \leq 2$ since $q - 1 \equiv 2 \pmod{8}$. Again, we will prove that none of the values of $k$ is possible. For $k = \overline{q}$, we have already shown that this is impossible. We assume next that $k = \overline{q} c$. If $2 \mid c$, then $k$ is divisible by 2 but not by 4. Therefore, $k - 2 \equiv 0 \pmod{4}$, and hence $q^3 - 1 \equiv 0 \pmod{4}$ by Lemma 3 (d), which is impossible as we have already seen. For $2 \nmid c$, polynomial division with remainder gives

$$q^3 - 1 = \left( \sum_{i=0}^{m} \frac{2^i q^3}{(qc)^{i+1}} \right) (\overline{q} c - 2) + \frac{2^{m+1} q^3}{(qc)^{m+1}} - 1$$

for a suitable $m \in \mathbb{N}$. But obviously $\frac{2^{m+1} q^3}{(qc)^{m+1}} \neq 1$, which leads to the same contradiction as before.

Now, we assume that $k = \overline{q} c$. Then

$$|G_{0B}| = \frac{|G_B \cap Re(q)\bar{a}|}{k} = n\overline{a} \text{ or } 2n\overline{a},$$

where $\overline{a} = a$. When considering the first possibility, clearly equation 3 rules out the case $n = 1$. So, we assume that $n = 2$. Hence $k = \overline{q} c$, but polynomial division with remainder yields

$$q^3 - 1 = \left( \sum_{i=0}^{m} \frac{2^{2i+1} q^3}{(qc)^{i+1}} \right) \left( \frac{\overline{q} c}{2} - 2 \right) + \frac{2^{m+2} q^3}{(qc)^{m+1}} - 1$$

for a suitable $m \in \mathbb{N}$. But since $c \mid q - 1$, the largest possible power of 2 that is contained in $c^{m+1}$ is $2^{m+1}$. Thus $\frac{2^{m+2} q^3}{(qc)^{m+1}} \neq 1$, the same contradiction as above.
Now, we assume that $|G_{0B}| = 2n\alpha$. For $n = 1$, we get $k = \overline{7c}$, which
is not possible as shown above. The case $n = 2$ is ruled out by
equation (5) since $(k - 1)(k - 2)$ is not divisible by 4 as we already
know.

This completes the list of subgroups that we have to examine, and the claim
is established.

Case (6): $N = Sp(2d, 2)$, $d \geq 3$, $v = 2^{2d-1} \pm 2^{d-1}$.

As here $|\text{Out}(N)| = 1$, we have $N = G$. Let $X^+$ (respectively $X^-$) denote
the set of points on which $G$ operates. It is well-known that $G_x$ acts on
$X^+ \setminus \{x\}$ as $O^\pm(2d, 2)$ does in its usual rank 3 representation on singular
points of the underlying orthogonal space. Thus, $G_{xy}$ has two orbits on
$X^+ \setminus \{x, y\}$ of length $2(2^{d-1} \mp 1)(2^{d-2} \pm 1)$ and $2^{2d-2}$ (see, e.g., [24, p. 69]).

We will show by contradiction that $G \leq \text{Aut}(D)$ cannot act flag-transitively
on any non-trivial Steiner 3-design $D$.

Let $z \in X^+ \setminus \{x, y\}$. Then, in both cases, the 3-subset $\{x, y, z\}$ is incident
with a unique block $B \in B$. By Remark [9] we have therefore

$$(v - 2) |G_{xB}| = (k - 1)(k - 2) |G_{xy}|,$$

where

$$|G_{xB}| = n |G_{xy}|,$$

for some $n \in \mathbb{N}$. This is equivalent to

$$2(2^{2d-2} \pm 2^{d-2} - 1)n = (k - 1)(k - 2) |z^{G_{xy}}|$$

with

$$|z^{G_{xy}}| = \begin{cases} 2(2^{d-1} \mp 1)(2^{d-2} \pm 1), & \text{or} \\ 2^{2d-2}, & \text{or} \end{cases}$$

Clearly, $2^{2d-2} \pm 2^{d-2} - 1 \equiv 1 \pmod{2}$ and $(k - 1)(k - 2) \equiv 0 \pmod{2}$. As
$(2^{2d-2} \pm 2^{d-2} - 1, 2^{d-1} \mp 1) = (2^{d-2}, 2^{d-1} \mp 1) = 1$ and $(2^{2d-2} \pm 2^{d-2} - 1,
2^{d-2} \pm 1) = (2, 2^{d-2} \pm 1) = 1$, it follows that $|z^{G_{xy}}|$ always divides $n$. Thus
$|G_{xy}| \mid |G_{xB}|$, and equation (8) yields

$$v - 2 \mid (k - 1)(k - 2).$$

But, on the other hand, we have $v - 2 \geq (k - 1)(k - 2)$ by Proposition [4] (b),
and it is immediately seen that $v$ cannot take the values where equality
holds.

Cases (7)-(8).

For the existence of non-trivial flag-transitive Steiner 3-designs, we have
in these cases only a small number of possibilities for $k$ to check, which can
easily be ruled out by hand using Lemma [2], Lemma [3] (d), and Corollary [5]
Case (9): $N = M_v$, $v = 11, 12, 22, 23, 24$.

Here $G$ is always 3-transitive, and thus [23] Thm. 3] yields the design described in part (iv) of the Main Theorem. Obviously, flag-transitivity holds as the 3-transitivity of $G$ implies that $G_x$ acts block-transitively on the derived Steiner 2-design $D_x$ for any $x \in X$.

Cases (10)-(13).

Again, the few possibilities for $k$ can easily be ruled out by hand using Lemma 2, Lemma 3 (c) and (d), and Corollary 5.

This completes the proof of the Main Theorem.

Acknowledgment. I am grateful to C. Hering and W. M. Kantor for helpful suggestions.

References

1. M. Aschbacher, Chevalley groups of type $G_2$ as the group of a trilinear form, J. Algebra 109 (1987), 193–259.
2. R. Baer, Polarities in finite projective planes, Bull. Amer. Math. Soc. 52 (1946), 77–93.
3. F. Beukers, On the generalized Ramanujan-Nagell equation, I, Acta Arith. 38 (1981), 389–410.
4. R. E. Block, Transitive groups of collineations on certain designs, Pacific J. Math. 15 (1965), 13–18.
5. F. Buekenhout, A. Delandtsheer, and J. Doyen, Finite linear spaces with flag-transitive groups, J. Combin. Theory, Series A 49 (1988), 268–293.
6. F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck, and J. Saxl, Linear spaces with flag-transitive automorphism groups, Geom. Dedicata 36 (1990), 89–94.
7. P. J. Cameron, Parallelisms of Complete Designs, London Math. Soc. Lecture Note Series 23, Cambridge Univ. Press, Cambridge, 1976.
8. P. J. Cameron and W. M. Kantor, 2-transitive and antiflag transitive collineation groups of finite projective and polar spaces, J. Algebra 60 (1979), 384–422.
9. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
10. C. W. Curtis, G. M. Seitz, and W. M. Kantor, The 2-transitive permutation representations of the finite Chevalley groups, Trans. Amer. Math. Soc. 218 (1976), 1–59.
11. A. Delandtsheer, Finite (line, plane)-flag-transitive planar spaces, Geom. Dedicata 41 (1992), 145–153.
12. ____, Dimensional linear spaces, in: Handbook of Incidence Geometry, ed. by F. Buekenhout, Elsevier Science, Amsterdam, 1995, 193-294.
13. ____, Finite flag-transitive linear spaces with alternating socle, in: Algebraic Combinatorics and Applications, Proc. Euroconf. (Gößweinstein 1999), ed. by A. Betten et al., Springer, Berlin, 2001, 79-88.
14. A. Delandtsheer, J. Doyen, J. Siemons, and C. Tamburini, Doubly homogeneous 2-(v, k, 1) designs, J. Combin. Theory, Series A 43 (1986), 140–145.
15. P. Dembowski, Finite Geometries, Springer, Berlin, Heidelberg, New York, 1968; Reprint: Springer, 1997.
16. L. E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, Teubner, Leipzig, 1901; Reprint: Dover Publications, New York, 1958.
17. D. Gorenstein, Finite Simple Groups. An Introduction to Their Classification, Plenum Press, New York, London, 1982.
18. C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, Geom. Dedicata 2 (1974), 425–460.
19. C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II, J. Algebra 93 (1985), 151–164.
20. M. Huber, Classification of flag-transitive Steiner quadruple systems, J. Combin. Theory, Series A 94 (2001), 180–190.
21. M. Huber, Klassifikationen fahnentransitiver Steiner Designs, Dissertation, Univ. Tübingen, Tübingen, 2001, (URL: http://w210.ub.uni-tuebingen.de/dbt/volltexte/2001/275).
22. B. Huppert, Zweifach transitive, auflösbare Permutationsgruppen, Math. Z. 68 (1957), 126–150.
23. B. Huppert, Endliche Gruppen I, Springer, Berlin, Heidelberg, New York, 1967.
24. W. M. Kantor, Homogeneous designs and geometric lattices, J. Combin. Theory, Series A 38 (1985), 66–74.
25. P. B. Kleidman and M. W. Liebeck, The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Note Series 129, Cambridge Univ. Press, Cambridge, 1990.
26. M. W. Liebeck, The classification of finite linear spaces with flag-transitive automorphism groups of affine type, J. Combin. Theory, Series A 84 (1998), 196–235.
27. H. Lüneburg, Fahnenhomogene Quadrupelsysteme, Math. Z. 89 (1965), 82–90.
28. E. Maillet, Sur les isomorphes holoédriques et transitifs des groupes symétriques ou alternés, J. Math. Pures Appl. (5) 1 (1895), 5–34.
29. J. Saxl, On finite linear spaces with almost simple flag-transitive automorphism groups, J. Combin. Theory, Series A 100 (2002), 322–348.
30. M. Suzuki, On a class of doubly transitive groups, Ann. Math. 75 (1962), 105–145.
31. H. N. Ward, On Ree’s series of simple groups, Trans. Amer. Math. Soc. 121 (1966), 62–89.
32. K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. für Math. u. Phys. 3 (1892), 265–284.