

On Highly Symmetric Combinatorial Designs

HABILITATIONSSCHRIFT

zur Erlangung der Venia legendi
der Fakultät für Mathematik und Physik
der Eberhard-Karls-Universität Tübingen

vorgelegt von
DR. MICHAEL HUBER

2005

Contents

Zusammenfassung (Summary)	3
1 Introduction	7
2 A Census of Highly Symmetric Combinatorial Designs	9
3 Definitions and Preliminary Results	17
4 The Classification of all Flag-transitive Steiner 3-Designs	25
4.1 Groups of Automorphisms of Affine Type	26
4.2 Groups of Automorphisms of Almost Simple Type	35
5 The Classification of all Flag-transitive Steiner 4-Designs	49
5.1 Groups of Automorphisms of Affine Type	49
5.2 Groups of Automorphisms of Almost Simple Type	54
6 The Classification of all Flag-transitive Steiner 5-Designs	83
6.1 Groups of Automorphisms of Affine Type	83
6.2 Groups of Automorphisms of Almost Simple Type	85
7 The Non-Existence of Flag-transitive Steiner 6-Designs	103
7.1 Groups of Automorphisms of Affine Type	103
7.2 Groups of Automorphisms of Almost Simple Type	105
Bibliography	109

Zusammenfassung (Summary)

Für natürliche Zahlen $t \leq k \leq v$ und λ definieren wir ein t - (v, k, λ) *Design* als eine endliche Inzidenzstruktur $\mathcal{D} = (X, \mathcal{B}, I)$, wobei X eine Menge von *Punkten*, $|X| = v$, und \mathcal{B} eine Menge von *Blöcken*, $|\mathcal{B}| = b$, bezeichnet, mit den Eigenschaften, dass jeder Block $B \in \mathcal{B}$ mit k Punkten inzidiert und jede t -elementige Teilmenge von X mit λ Blöcken inzidiert (dabei inzidiert eine Teilmenge von X mit einem Block B , falls jedes ihrer Elemente mit B inzidiert). Eine *Fahne* von \mathcal{D} ist ein inzidentes Punkt-Block Paar $(x, B) \in I$ mit $x \in X$ und $B \in \mathcal{B}$. Wir betrachten Automorphismen von \mathcal{D} als Paare von Permutationen auf X und \mathcal{B} , welche die Inzidenz erhalten, und nennen eine Automorphismengruppe $G \leq \text{Aut}(\mathcal{D})$ von \mathcal{D} *fahnentransitiv* (resp. *blocktransitiv*, *t -fach punkttransitiv*, *t -fach punkthomogen*), falls G transitiv auf den Fahnen (resp. transitiv auf den Blöcken, t -fach transitiv auf den Punkten, t -fach homogen auf den Punkten) von \mathcal{D} operiert. Abkürzend heißt \mathcal{D} beispielsweise fahnentransitiv, falls \mathcal{D} eine fahnentransitive Automorphismengruppe zulässt.

Aus historischen Gründen wird ein t - (v, k, λ) Design mit $\lambda = 1$ als *Steiner t -Design* (manchmal auch als *Steinersystem*) bezeichnet. Wir bemerken, dass in diesem Falle jeder Block eindeutig bestimmt ist durch die Menge der Punkte, mit denen er inzidiert, und daher mit einer k -elementigen Teilmenge von X identifiziert werden kann. Falls $t < k < v$ gilt, dann sprechen wir von einem *nicht-trivialen* Steiner t -Design.

Infolge der Klassifikation der endlichen einfachen Gruppen gelang es in den letzten Jahrzehnten Steiner t -Designs, in der Hauptsache für $t = 2$, zu charakterisieren, die Automorphismengruppen mit genügend starken Symmetrieeigenschaften zuzulassen. Vermutlich als eines der ersten der weitreichendsten Resultate für Steiner 2-Designs wurden 1985 alle 2-fach punkttransitiven Steiner 2-Designs

von W. M. Kantor [35, Thm. 1] klassifiziert unter Verwendung der Klassifikation der endlichen 2-fach transitiven Permutationsgruppen. Bedeutend schwieriger erwies sich die Bestimmung im Falle von fahnentransitiven Steiner 2-Designs: Unter den hoch-symmetrischen Eigenschaften von Inzidenzstrukturen gilt die der Fahnentransitivität sicherlich als eine besonders wichtige und natürliche. Bereits lange vor der angekündigten Klassifikation der endlichen einfachen Gruppen wurde durch D. G. Higman und J. E. McLaughlin [28] eine allgemeine Untersuchung von fahnentransitiven Steiner 2-Designs initiiert, indem sie bewiesen, dass eine fahnentransitive Automorphismengruppe $G \leq \text{Aut}(\mathcal{D})$ eines Steiner 2-Designs \mathcal{D} primitiv auf den Punkten von \mathcal{D} operiert. Sie stellten die Frage nach der Klassifikation aller endlichen fahnentransitiven projektiven Ebenen und zeigten, dass solche Ebenen desarguessch sind, falls ihre Ordnungen geeignet beschränkt sind. Wesentlich später bestimmte W. M. Kantor [37] alle diese Ebenen mit Ausnahme des noch immer offenen Falles, wenn die Automorphismengruppe eine Frobeniusgruppe von Primzahlgrad ist. Sein Beweis basiert auf der Klassifikation der endlichen einfachen Gruppen und setzt genaue Kenntnis von primitiven Permutationsgruppen von ungeradem Grad voraus. In einer großen gemeinschaftlichen Arbeit charakterisierten schließlich F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck und J. Saxl [8, 19, 39, 42, 47] nahezu vollständig alle endlichen fahnentransitiven linearen Räume, das sind fahnentransitive Steiner 2-Designs. Ihr Resultat wurde 1990 angekündigt und beruht auf der Klassifikation der endlichen einfachen Gruppen. Als Ausgangspunkt dient dabei der obige Satz von Higman und McLaughlin, ferner wird der Satz von O’Nan-Scott über endliche primitive Permutationsgruppen verwendet. Für den noch offenen Fall mit einer 1-dimensionalen affinen Automorphismengruppe verweisen wir auf [8, Sect. 4] und [38, Sect. 3].

Jedoch blieben bislang, trotz der Klassifikation der endlichen einfachen Gruppen, für Steiner t -Designs mit $t > 2$ die meisten dieser Charakterisierungen mit einer hoch-symmetrischen Automorphismengruppe lange Zeit ungelöste und schwierige Probleme. Durch Untersuchung von t -Designs mit beliebigem λ , aber großem t , zeigten P. J. Cameron und C. E. Praeger [13, Thm. 1.1], dass es weder nicht-triviale fahnentransitive t -Designs für $t \geq 7$ noch blocktransitive t -Designs für $t \geq 8$ geben kann. Insbesondere gilt die Bestimmung aller fahnentransitiven Steiner t -Designs mit $3 \leq t \leq 6$ als von besonderem Interesse und ist

seit ungefähr 40 Jahren offen. Selbst die Klassifikation aller fahnen transitiven Steiner 3-Designs ist bekannt als "long-standing and still open problem" (cf. [17, p. 147] und [18, p. 273]). Vermutlich beschäftigte sich H. Lüneburg [44] im Jahr 1965 als erster mit einem Teil dieses Problems, indem er fahnen transitiv Steiner 3-Designs mit der Blockgröße 4 (sog. *Steinerquadrupelsysteme*) charakterisierte unter der zusätzlichen starken Voraussetzung, dass jedes von der Identität verschiedene Element der Automorphismengruppe höchstens zwei Fixpunkte hat. Dieses Resultat wurde 2001 vom Autor [29] verallgemeinert ohne die zusätzliche Voraussetzung über die Fixpunktanzahl.

In der vorliegenden Arbeit führen wir die vollständige Klassifikation aller fahnen transitiven Steiner 3-Designs in Kapitel 4 an. Wir geben ferner die vollständige Klassifikation aller fahnen transitiven Steiner 4-Designs in Kapitel 5. Beide Resultate beruhen auf der Klassifikation der endlichen 2-fach transitiven Permutationsgruppen. Die Charakterisierung im Falle der fahnen transitiven Steiner 3-Designs ist 2005 erschienen in [30], die der fahnen transitiven Steiner 4-Designs ist eingereicht [31]. In den Kapiteln 6 und 7 bestimmen wir vollständig alle fahnen transitiven Steiner 5-Designs und zeigen, dass es keine nicht-trivialen fahnen transitiven Steiner 6-Designs geben kann. Für beide Resultate benötigen wir die Klassifikation der endlichen 3-fach homogenen Permutationsgruppen. Darüber hinaus geben wir in Kapitel 2 einen Überblick über die weitreichendsten Resultate über hoch-symmetrische Steiner t -Designs. Die Inhalte dieser Kapitel sind ebenfalls eingereicht [32].

Unsere Ergebnisse zusammenfassend lautet die vollständige Bestimmung aller nicht-trivialen Steiner t -Designs mit $t \geq 3$, die eine fahnen transitive Automorphismengruppe zulassen, wie folgt:

Main Theorem. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales Steiner t -Design mit $t \geq 3$. Genau dann operiert $G \leq \text{Aut}(\mathcal{D})$ fahnen transitiv auf \mathcal{D} , wenn einer der folgenden Fälle auftritt:*

- (1) \mathcal{D} ist isomorph zum 3 - $(2^d, 4, 1)$ Design, bestehend aus den Punkten und Ebenen des affinen Raumes $AG(d, 2)$, und es gilt eine der folgenden Aussagen:
 - (i) $d \geq 3$, und $G \cong AGL(d, 2)$,
 - (ii) $d = 3$, und $G \cong AGL(1, 8)$ oder $A\Gamma L(1, 8)$,

- (iii) $d = 4$, und $G_0 \cong A_7$,
 - (iv) $d = 5$, und $G \cong AFL(1, 32)$,
- (2) \mathcal{D} ist isomorph zu einem $3-(q^e + 1, q + 1, 1)$ Design, dessen Punkte die Elemente von $GF(q^e) \cup \{\infty\}$ und dessen Blöcke die Bilder von $GF(q) \cup \{\infty\}$ unter $PGL(2, q^e)$ (resp. $PSL(2, q^e)$, e ungerade) sind mit einer Primzahlpotenz $q \geq 3$, $e \geq 2$, und das abgeleitete Design in einem beliebigen Punkt ist isomorph zum $2-(q^e, q, 1)$ Design, bestehend aus den Punkten und Geraden von $AG(e, q)$, und $PSL(2, q^e) \leq G \leq P\Gamma L(2, q^e)$,
- (3) \mathcal{D} ist isomorph zu einem $3-(q + 1, 4, 1)$ Design, dessen Punkte die Elemente von $GF(q) \cup \{\infty\}$ mit einer Primzahlpotenz $q \equiv 7 \pmod{12}$ und dessen Blöcke die Bilder von $\{0, 1, \varepsilon, \infty\}$ unter $PSL(2, q)$ sind, wobei ε eine primitive sechste Einheitswurzel in $GF(q)$ ist, und das abgeleitete Design in einem beliebigen Punkt ist isomorph zum Nettotripelsystem $N(q)$, und $PSL(2, q) \leq G \leq P\Sigma L(2, q)$,
- (4) \mathcal{D} ist isomorph zu einem der folgenden Witt Designs:
- (i) das $3-(22, 6, 1)$ Design, und $G \supseteq M_{22}$,
 - (ii) das $4-(11, 5, 1)$ Design, und $G \cong M_{11}$,
 - (iii) das $4-(23, 7, 1)$ Design, und $G \cong M_{23}$,
 - (iv) das $5-(12, 6, 1)$ Design, und $G \cong M_{12}$,
 - (v) das $5-(24, 8, 1)$ Design, und $G \cong PSL(2, 23)$ oder $G \cong M_{24}$.

Wir bemerken, dass die Steiner 3-Designs in Teil (1) (ii) mit $G \cong AGL(1, 8)$ und (iv) mit $G \cong AFL(1, 32)$ sowie das Steiner 5-Design in Teil (4) mit $G \cong PSL(2, 23)$ scharf fahnen transitiv sind. Ferner enthält in Teil (4) (v) M_{24} als die volle Automorphismengruppe von \mathcal{D} nur eine Konjugiertenklasse von zu $PSL(2, 23)$ isomorphen Untergruppen.

Eine genaue Beschreibung des Nettotripelsystems $N(q)$ wird in [7, Sect. 2] gegeben. Für eine ausführliche Darstellung der Witt $t-(v, k, 1)$ Designs mit ihren zugehörigen Mathieugruppen M_v vom Grad v verweisen wir beispielsweise auf [50].

Chapter 1

Introduction

For positive integers $t \leq k \leq v$ and λ , we define a t - (v, k, λ) *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 λ 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*, *point t -homogeneous*) if G acts transitively on the flags (respectively transitively on the blocks, t -transitively on the points, t -homogeneously 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.

For historical reasons, a t - (v, k, λ) design with $\lambda = 1$ is called 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 $t < k < v$ 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 $t = 2$, admitting groups of automorphisms with sufficiently strong symmetry properties. For Steiner 2-designs, probably the most general results have been the classification of all point 2-transitive Steiner 2-designs in 1985 by W. M. Kantor [35, 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 [8, 19, 42, 47].

However, despite the classification of the finite simple groups, for Steiner t -designs with $t > 2$ most of these characterizations have remained long-standing challenging problems. Investigating t -designs for arbitrary λ , but large t , P. J. Cameron and C. E. Praeger [13, Thm. 1.1] showed that there cannot exist any non-trivial flag-transitive t -designs for $t \geq 7$ nor any block-transitive t -designs for $t \geq 8$. Especially, the determination of all flag-transitive Steiner t -designs with $3 \leq t \leq 6$ is of particular interest and has been open for about 40 years (cf. [17, p. 147] and [18, p. 273], but presumably dating back to 1965).

In the present work, we state the complete classification of all flag-transitive Steiner 3-designs in Chapter 4. We give furthermore the complete classification of all flag-transitive Steiner 4-designs in Chapter 5. Both results rely on the classification of the finite 2-transitive permutation groups. The characterization in the case of flag-transitive Steiner 3-designs has been published 2005 in [30], that of flag-transitive Steiner 4-designs is submitted [31].

In Chapters 6 and 7, we completely determine all flag-transitive Steiner 5-designs and prove that there are no non-trivial flag-transitive Steiner 6-designs. Both results depend on the classification of the finite 3-homogeneous permutation groups. Summarizing our work, we state the complete determination of all flag-transitive Steiner t -designs with $t \geq 3$ in Chapter 2. Moreover, we give in this context a survey on some of the most general results on highly symmetric Steiner t -designs. The content of these chapters is also submitted [32].

Chapter 2

A Census of Highly Symmetric Combinatorial Designs

In the sequel, we present the complete determination of all flag-transitive Steiner t -designs with $t \geq 3$ and survey some of the most general results on highly symmetric Steiner t -designs. For detailed descriptions of the respective designs and their groups of automorphisms as well as for further surveys concerning particularly highly symmetric Steiner 2-designs, we refer to [7, Sect. 1, 2], [21, Ch. 2.3, 2.4, 4.4], [36], [38] and [50].

As probably one of the first most general results, all point 2-transitive Steiner 2-designs were classified by W. M. Kantor [35, Thm. 1], using the classification of the finite 2-transitive permutation groups.

Theorem 1. (Kantor 1985). *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 2-design, and let $G \leq \text{Aut}(\mathcal{D})$ act point 2-transitively on \mathcal{D} . Then one of the following holds:*

- (1) \mathcal{D} is isomorphic to the $2\text{-}(\frac{q^d-1}{q-1}, q+1, 1)$ design whose points and blocks are the points and lines of the projective space $PG(d-1, q)$, and $PSL(d, q) \leq G \leq P\Gamma L(d, q)$, or $(d-1, q) = (3, 2)$ and $G \cong A_7$,
- (2) \mathcal{D} is isomorphic to a Hermitian unital $U_H(q)$ of order q , and $PSU(3, q^2) \leq G \leq P\Gamma U(3, q^2)$,
- (3) \mathcal{D} is isomorphic to a Ree unital $U_R(q)$ of order q with $q = 3^{2e+1} > 3$, and $Re(q) \leq G \leq \text{Aut}(Re(q))$,

- (4) \mathcal{D} is isomorphic to the 2 - $(q^d, q, 1)$ design whose points and blocks are the points and lines of the affine space $AG(d, q)$, and one of the following holds:
- (i) $G \leq A\Gamma L(1, q^d)$,
 - (ii) $G_0 \supseteq SL(\frac{d}{a}, q^a)$, $d \geq 2a$,
 - (iii) $G_0 \supseteq Sp(\frac{2d}{a}, q^a)$, $d \geq 2a$,
 - (iv) $G_0 \supseteq G_2(q^a)'$, q even, $d = 6a$,
 - (v) $G_0 \supseteq SL(2, 3)$ or $SL(2, 5)$, $v = q^2$, $q = 5, 7, 9, 11, 19, 23, 29$ or 59 ,
 - (vi) $G_0 \supseteq SL(2, 5)$, or G_0 contains a normal extraspecial subgroup E of order 2^5 and G_0/E is isomorphic to a subgroup of S_5 , $v = 3^4$,
 - (vii) $G_0 \cong SL(2, 13)$, $v = 3^6$,
- (5) \mathcal{D} is isomorphic to the affine nearfield plane A_9 of order 9, and G_0 as in (4)(vi),
- (6) \mathcal{D} is isomorphic to the affine Hering plane A_{27} of order 27, and G_0 as in (4)(vii),
- (7) \mathcal{D} is isomorphic to one of the two Hering spaces 2 - $(9^3, 9, 1)$, and G_0 as in (4)(vii).

Moreover, for point t -transitive Steiner t -designs with $t > 2$, W. M. Kantor [35, Thm. 3] showed that the classification of the finite 2-transitive permutation groups and Theorem 1 easily imply the following classification:

Theorem 2. (Kantor 1985). *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner t -design with $t \geq 3$, and let $G \leq \text{Aut}(\mathcal{D})$ act point t -transitively on \mathcal{D} . Then one of the following holds:*

- (1) \mathcal{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
- (i) $d \geq 3$, and $G \cong AGL(d, 2)$, or
 - (ii) $d = 4$, and $G_0 \cong A_7$,

- (2) \mathcal{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 $PSL(2, q^e) \leq G \leq P\Gamma L(2, q^e)$,
- (3) \mathcal{D} is isomorphic to one of the following Witt designs:
- (i) the $3-(22, 6, 1)$ design, and $G \supseteq M_{22}$,
 - (ii) the $4-(11, 5, 1)$ design, and $G \cong M_{11}$,
 - (iii) the $4-(23, 7, 1)$ design, and $G \cong M_{23}$,
 - (iv) the $5-(12, 6, 1)$ design, and $G \cong M_{12}$,
 - (v) the $5-(24, 8, 1)$ design, and $G \cong M_{24}$.

Certainly, among the highly symmetric properties of incidence structures, flag-transitivity is a particularly important and natural one. Even long before the aforementioned classification of the finite simple groups, a general study of flag-transitive Steiner 2-designs was introduced by D. G. Higman and J. E. McLaughlin [28] proving that a flag-transitive group $G \leq \text{Aut}(\mathcal{D})$ of automorphisms of a Steiner 2-design \mathcal{D} is necessarily primitive on the points of \mathcal{D} . They posed the problem of classifying all finite flag-transitive projective planes, and showed that such planes are desarguesian if its orders are suitably restricted. Much later W. M. Kantor [37] determined all such planes apart from the still open case when the group of automorphisms is a Frobenius group of prime degree. His proof involves detailed knowledge of primitive permutation groups of odd degree based on the classification of the finite simple groups. In a big common effort, F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck, and J. Saxl [8, 19, 39, 42, 47] essentially characterized all finite flag-transitive linear spaces, that is flag-transitive Steiner 2-designs. Their result, which also relies on the classification of the finite simple groups, starts with the result of Higman and McLaughlin and uses the O’Nan-Scott Theorem for finite primitive permutation groups. For the incomplete case with a 1-dimensional affine group of automorphisms, we refer to [8, Sect. 4] and [38, Sect. 3].

Theorem 3. (Buekenhout et al. 1990). *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a Steiner 2-design, and let $G \leq \text{Aut}(\mathcal{D})$ act flag-transitively on \mathcal{D} . Then one of the following occurs:*

- (1) \mathcal{D} is isomorphic to the $2\text{-}(q^d, q, 1)$ design whose points and blocks are the points and lines of the affine space $AG(d, q)$, and one of the following holds:
 - (i) G is 2-transitive (hence as in Theorem 1 (4)),
 - (ii) $d = 2$, $q = 11$ or 23 , and G is one of the three solvable flag-transitive groups given in [23, Table II],
 - (iii) $d = 2$, $q = 9, 11, 19, 29$ or 59 , $G_0^{(\infty)} \cong SL(2, 5)$ (where $G_0^{(\infty)}$ denotes the last term in the derived series of G_0), and G is given in [23, Table II],
 - (iv) $d = 4$, $q = 3$, and $G_0 \cong SL(2, 5)$,
- (2) \mathcal{D} is isomorphic to a non-Desargues affine translation plane. More precisely, one of the following holds:
 - (i) \mathcal{D} is isomorphic to a Lüneburg-Tits plane $\text{Lue}(q^2)$ of order q^2 with $q = 2^{2e+1} > 2$, and $Sz(q) \leq G_0 \leq \text{Aut}(Sz(q))$,
 - (ii) \mathcal{D} is isomorphic to the affine Hering plane A_{27} of order 27, and $G_0 \cong SL(2, 13)$,
 - (iii) \mathcal{D} is isomorphic to the affine nearfield plane A_9 of order 9, and G is one of the seven flag-transitive subgroups of $\text{Aut}(A_9)$, described in [24, §5],
- (3) \mathcal{D} is isomorphic to one of the two Hering spaces $2\text{-}(9^3, 9, 1)$, and $G_0 \cong SL(2, 13)$,
- (4) \mathcal{D} is isomorphic to the $2\text{-}(\frac{q^d-1}{q-1}, q+1, 1)$ design whose points and blocks are the points and lines of the projective space $PG(d-1, q)$, and $PSL(d, q) \leq G \leq P\Gamma L(d, q)$, or $(d-1, q) = (3, 2)$ and $G \cong A_7$,
- (5) \mathcal{D} is isomorphic to a Hermitian unital $U_H(q)$ of order q , and $PSU(3, q^2) \leq G \leq P\Gamma U(3, q^2)$,
- (6) \mathcal{D} is isomorphic to a Ree unital $U_R(q)$ of order q with $q = 3^{2e+1} > 3$, and $Re(q) \leq G \leq \text{Aut}(Re(q))$,

- (7) \mathcal{D} is isomorphic to a Witt-Bose-Shrikhande space $W(q)$ with $q = 2^d \geq 8$,
and $PSL(2, q) \leq G \leq P\Gamma L(2, q)$,
- (8) $G \leq A\Gamma L(1, q)$.

Investigating t -designs \mathcal{D} for arbitrary λ , but large t , P. J. Cameron and C. E. Praeger [13, Thm. 1.1 and 2.1] showed that for $t \geq 7$ the flag-transitivity, respectively for $t \geq 8$ the block-transitivity of $G \leq \text{Aut}(\mathcal{D})$ implies at least its point 4-homogeneity and proved the following result:

Theorem 4. (Cameron and Praeger 1993). *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a t - (v, k, λ) design. If $G \leq \text{Aut}(\mathcal{D})$ acts block-transitively on \mathcal{D} , then $t \leq 7$, while if $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on \mathcal{D} , then $t \leq 6$.*

Especially, the determination of all flag-transitive Steiner t -designs with $3 \leq t \leq 6$ is of particular interest, but even the classification of all flag-transitive Steiner 3-designs has been known as "a long-standing and still open problem" (cf. [17, p. 147] and [18, p. 273]). Presumably, H. Lüneburg [44] in 1965 has been the first dealing with part of this problem characterizing flag-transitive Steiner 3-designs with block size $k = 4$ (so-called *Steiner quadruple systems*) under the additional strong assumption that every non-identity element of the group of automorphisms fixes at most two distinct points. This result has been generalized in 2001 by the author [29], omitting the additional assumption concerning the number of fixed points.

In the present work, we state the complete classification of all flag-transitive Steiner 3-designs in Chapter 4. We give furthermore the complete classification of all flag-transitive Steiner 4-designs in Chapter 5. Both results rely on the classification of the finite 2-transitive permutation groups. The characterization in the case of flag-transitive Steiner 3-designs has been published 2005 in [30], that of flag-transitive Steiner 4-designs is submitted [31].

In Chapters 6 and 7, we completely determine all flag-transitive Steiner 5-designs and prove that there are no non-trivial flag-transitive Steiner 6-designs. Both results depend on the classification of the finite 3-homogeneous permutation groups, and are also submitted [32].

Summarizing our results, the complete determination of all non-trivial Steiner t -designs with $t \geq 3$ admitting a flag-transitive group of automorphisms can be stated as follows.

Theorem 5. (Huber 2005). *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner t -design with $t \geq 3$. Then $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on \mathcal{D} if and only if one of the following occurs:*

- (1) \mathcal{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) \mathcal{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 $PSL(2, q^e) \leq G \leq P\Gamma L(2, q^e)$,
- (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 ε 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 one of the following Witt designs:
 - (i) the 3 - $(22, 6, 1)$ design, and $G \supseteq M_{22}$,
 - (ii) the 4 - $(11, 5, 1)$ design, and $G \cong M_{11}$,
 - (iii) the 4 - $(23, 7, 1)$ design, and $G \cong M_{23}$,

(iv) *the 5-(12, 6, 1) design, and $G \cong M_{12}$,*

(v) *the 5-(24, 8, 1) design, and $G \cong PSL(2, 23)$ or $G \cong M_{24}$.*

We remark that the Steiner 3-designs in Part (1) (ii) with $G \cong AGL(1, 8)$ and (iv) with $G \cong A\Gamma L(1, 32)$ as well as the Steiner 5-design in Part (4) with $G \cong PSL(2, 23)$ are sharply flag-transitive, and furthermore, concerning Part (4) (v), that M_{24} as the full group of automorphisms of \mathcal{D} contains only one conjugacy class of subgroups isomorphic to $PSL(2, 23)$.

Chapter 3

Definitions and Preliminary Results

If $\mathcal{D} = (X, \mathcal{B}, I)$ is a t - (v, k, λ) 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 $\text{Fix}_X(g)$ denote the set of fixed points of g in X . We call G *semi-regular* if the identity is the only element that fixes any point of X . If additionally G is transitive, then it is said to be *regular*. Furthermore, for $x \in X$, the orbit x^G containing x is called *regular* if it has length $|G|$. If $\{x_1, \dots, x_m\} \subseteq X$, let $G_{\{x_1, \dots, x_m\}}$ be its setwise stabilizer and G_{x_1, \dots, x_m} its pointwise stabilizer (for short, we often write $G_{x_1 \dots x_m}$ 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 (throughout this work, $0 \notin \mathbb{N}$). 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. [26, 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 $\bar{r} \perp q^n - 1$ that \bar{r} 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.

For Steiner t -designs \mathcal{D} with $t = 2$, it is elementary that the point 2-transitivity of $G \leq \text{Aut}(\mathcal{D})$ implies its flag-transitivity. However, for $t \geq 3$, it can be deduced from a result of R. E. Block that the converse holds:

Proposition 6. *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 [6, Thm. 2], G_x also acts point-transitively on \mathcal{D}_x , and the claim follows. \square

The above result is our starting point for the determination of all flag-transitive Steiner t -designs with $t = 3$ and $t = 4$, allowing 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. [16, 25, 26, 27, 33, 35, 45]).

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) $G \leq A\Gamma L(1, p^d)$
- (2) $G_0 \supseteq SL(\frac{d}{a}, p^a)$, $d \geq 2a$
- (3) $G_0 \supseteq Sp(\frac{2d}{a}, p^a)$, $d \geq 2a$
- (4) $G_0 \supseteq G_2(2^a)'$, $d = 6a$
- (5) $G_0 \cong A_6$ or A_7 , $v = 2^4$
- (6) $G_0 \supseteq SL(2, 3)$ 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) $PSL(d, q)$, $d \geq 2$, $v = \frac{q^d - 1}{q - 1}$, 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) $Sp(2d, 2)$, $d \geq 3$, $v = 2^{2d-1} \pm 2^{d-1}$
- (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 required basic properties of the listed groups, we refer, e.g., to [15], [34], [40, Ch. 2, 5], [48], and [49].

For Steiner t -designs with larger values of t , the flag-transitivity of $G \leq \text{Aut}(\mathcal{D})$ has an even stronger implication due to the following assertion, which follows from Block's theorem and a combinatorial result of D. K. Ray-Chaudhuri and R. M. Wilson [46, Thm. 1].

Proposition 7. (Cameron and Praeger [13]). *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a Steiner t -design with $t \geq 2$. Then, the following holds:*

- (a) *If $G \leq \text{Aut}(\mathcal{D})$ acts block-transitively on \mathcal{D} , then G also acts point $\lfloor t/2 \rfloor$ -homogeneously on \mathcal{D} .*
- (b) *If $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on \mathcal{D} , then G also acts point $\lfloor (t+1)/2 \rfloor$ -homogeneously on \mathcal{D} .*

We note that Propositions 6 and 7 hold also for arbitrary λ , whereas for 2 - (v, k, λ) designs \mathcal{D} the implication that the point 2-transitivity of $G \leq \text{Aut}(\mathcal{D})$ yields its flag-transitivity is only true if $(r, \lambda) = 1$.

In order to investigate all flag-transitive Steiner t -designs with $t = 5$ and $t = 6$, we can as a consequence of Proposition 7 (b) make use of the classification of all finite 3-homogeneous permutation groups, which itself relies on the classification of all finite simple groups (cf. [10, 25, 41, 43]).

The list of groups is as follows.

Let G be a finite 3-homogeneous 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 $v = 2^d$. If we identify G with a group of affine transformations

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

of $V = V(d, 2)$, where $g \in G_0$ and $u \in V$, then particularly one of the following occurs:

- (1) $G \cong AGL(1, 8)$, $AFL(1, 8)$ or $AFL(1, 32)$
- (2) $G_0 \cong SL(d, 2)$, $d \geq 2$
- (3) $G_0 \cong A_7$, $v = 2^4$

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) $PSL(2, q)$, $q > 3$, $v = q + 1$
- (3) M_v , $v = 11, 12, 22, 23, 24$
- (4) M_{11} , $v = 12$

We note that if q is odd, then $PSL(2, q)$ is 3-homogeneous for $q \equiv 3 \pmod{4}$, but not for $q \equiv 1 \pmod{4}$, and hence not every group G of almost simple type satisfying (2) is 3-homogeneous on X .

We will now indicate some helpful combinatorial tools on which we rely in the sequel. Let r (respectively λ_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 Chapter 1.

Obvious is the subsequent fact.

Lemma 8. *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a Steiner t -design. If $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on \mathcal{D} , then, for any $x \in X$, the division property*

$$r \mid |G_x|$$

holds.

Elementary counting arguments give the following standard assertions.

Lemma 9. *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a t -(v, k, λ) design. Then the following holds:*

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

For non-trivial Steiner t -designs lower bounds for v in terms of k and t can be indicated.

Proposition 10. (Cameron [9]). *If $\mathcal{D} = (X, \mathcal{B}, I)$ is 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) is stronger for $k > 2(t-1)$. For $k = 2(t-1)$ both assert that $v \geq t^2 - 1$.

As we are in particular interested in the case when $3 \leq t \leq 6$, we deduce from (b) the following upper bound for the positive integer k .

Corollary 11. *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner t -design with $t = 3 + i$, where $i = 0, 1, 2, 3$. Then the block size k can be estimated by*

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

Remark 12. If $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on any Steiner t -design \mathcal{D} with $t \geq 3$, then applying Proposition 6 and Lemma 9 (b) yields the equation

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

where x and y are two distinct points in X and B is a block in \mathcal{B} , and thus

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

Chapter 4

The Classification of all Flag-transitive Steiner 3-Designs

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

Main Theorem 1. *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 3-design. Then $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on \mathcal{D} if and only if one of the following occurs:*

- (1) \mathcal{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 $A\Gamma L(1, 8)$,
 - (iii) $d = 4$, and $G_0 \cong A_7$,
 - (iv) $d = 5$, and $G \cong A\Gamma L(1, 32)$,
- (2) \mathcal{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 $PSL(2, q^e) \leq G \leq P\Gamma L(2, q^e)$,

- (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 ε 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 $G \supseteq M_{22}$.

A detailed description of the Netto triple system $N(q)$ can be found in [7, Sect. 2].

4.1 Groups of Automorphisms of Affine Type

In the following, we begin with the proof of Main Theorem 1. Using the notation as before, let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 3-design with $G \leq \text{Aut}(\mathcal{D})$ acting flag-transitively on \mathcal{D} . Let us recall that in view of Proposition 6, we can restrict ourselves to the inspection of the finite 2-transitive permutation groups listed in Chapter 3. 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 13. *Let $q = p^d$ with $p \neq 2$ a prime. Furthermore, let $2^m \parallel p-1$, $2^{\bar{m}} \parallel p+1$ and $2^n \parallel d$ for some integers m, \bar{m} and n . Then $2^{m+n} \parallel q-1$, unless $p \equiv 3 \pmod{4}$ and $d \equiv 0 \pmod{2}$, in which case $2^{\bar{m}+n} \parallel q-1$.*

Proof. This follows from [26, Lemma 3.2] using induction over n . □

Maintaining the same parameters, we obtain

Lemma 14. *Let $G \leq AGL(1, q)$ 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 $|P \cap AGL(1, q)| \geq 2^m$. Moreover, if $p \equiv 3 \pmod{4}$ and $d \equiv 0 \pmod{2}$, then $|P \cap AGL(1, q)| \geq 2^{\bar{m}}$.*

Proof. Clearly,

$$P/P \cap AGL(1, q) \cong P \cdot AGL(1, q)/AGL(1, q) \leq A\Gamma L(1, q)/AGL(1, q).$$

Thus, we obtain

$$|P| \mid |P \cap AGL(1, q)| \cdot d.$$

As $q(q-1) \mid |G|$ by the 2-transitivity of G , Lemma 13 yields

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

and therefore

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

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

Lemma 15. *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 14. \square

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 15, we know that G contains an involution τ 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 τ . 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 τ_x having only x as fixed point. Hence

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

whereas for the latter we use that τ_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 α . Therefore, we have $\tau_x \in AGL(1, v) \trianglelefteq A\Gamma L(1, v)$. 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 \mathcal{G} be a line in $AG(d, p)$ with distinct points $x, y \in \mathcal{G}$. Let B and \bar{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 $\mathcal{G} \subseteq B \cap \bar{B}$ with $|\mathcal{G}| > 2$, 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 [29], which gives the designs described in Part (1) of Main Theorem 1 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 12, it follows that

$$v - 2 \mid d(k - 1)(k - 2). \quad (4.1)$$

Combining this with [26, Thm. 3.3 (a)] gives

$$\Phi_{d-1}^*(2) \mid 2^{d-1} - 1 \mid d(2^a - 1)(2^{a-1} - 1). \quad (4.2)$$

Clearly, $a < d - 1$ (otherwise, $k = 2^{d-1}$, a contradiction to Corollary 11.) If $\Phi_{d-1}^*(2) = 1$, then, by [26, 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 [52, p. 283]). By using property (4.1), Lemma 9 (c) and Corollary 11, 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 there exists a prime divisor \bar{r} of $\Phi_{d-1}^*(2)$. Then $\bar{r} \mid d$ by [26, Thm. 3.5 (vi)]. As $\bar{r} \equiv 1 \pmod{(d-1)}$ (which follows from [26, Thm. 3.5 (ii)]), we conclude that $\bar{r} = d$. If there exists a further prime divisor \hat{r} of $\Phi_{d-1}^*(2)$ with $\hat{r} \neq \bar{r}$, then again $\hat{r} \mid d$ and $\hat{r} = d$ by the same arguments. Thus $\hat{r} = \bar{r}$, a contradiction. Hence, we have

$$\Phi_{d-1}^*(2) = \bar{r}^n$$

for some $n \in \mathbb{N}$. But then, by dividing property (4.2) by \bar{r} and using [26, Thm. 3.5 (vi)] again, we obtain

$$\frac{\Phi_{d-1}^*(2)}{\bar{r}} \leq 1.$$

Therefore, $\Phi_{d-1}^*(2) \leq \bar{r} = d$. As $\Phi_{d-1}^*(2) = 1$ has already been considered, we may suppose that $\Phi_{d-1}^*(2) = d$. Now [26, 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 not a 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 not a 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 α the Frobenius automorphism $GF(v) \rightarrow GF(v)$, $x \mapsto x^2$. Hence

$$G_B/T_B \cong G_B \cdot T/T$$

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 property (4.1), and the small number of possibilities for k can easily be eliminated by hand using property (4.1) and Lemma 9 (c).

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 conjugate 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 property (4.1). 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 $G^* \trianglelefteq G_B$, 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 2-transitive on points, we have $|G| = v(v-1)a$ with $a \mid d$. Then Remark 12 yields

$$v - 2 = (k - 1)(k - 2) \frac{a}{|G_{xB}|} \quad \text{if } x \in B. \quad (4.3)$$

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 $\bar{B} \in \mathcal{B}$. Thus, we have $a \mid |G_{xB}|$, and therefore $v - 2 = (k - 1)(k - 2)$. However, as $d > 3$, it follows from Proposition 10 (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 $G = A\Gamma L(1, 2^d)$.

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 \bar{p} of d with $\bar{p} \neq p$, then the quotients d/\bar{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 (4.3) yields

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

and hence

$$-1 \equiv 2p \pmod{\frac{k}{c}}.$$

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 property (4.1), these can again easily be eliminated by hand using Lemma 9 (c), and Corollary 11.

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

In the following, let e_i denote the i -th standard basis 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 Main Theorem 1 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 11, 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 obtain via linear algebra that $SL(\frac{d}{a}, p^a)_{e_1}$, and hence also G_{0, e_1} , acts point-transitively on $V \setminus \langle e_1 \rangle$. Again, let $x \in \langle e_1 \rangle$ be distinct from 0 and e_1 . If the unique block $B \in \mathcal{B}$ 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 11. Therefore, B lies completely in $\langle e_1 \rangle$, and by

the same argument as above, we obtain that here $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 3-design \mathcal{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 9 (c). For $v > 8$, we will show that also only Steiner quadruple systems can occur. Thus, applying [29] yields the claim. We remark that clearly any three distinct points are non-collinear in $AG(d, 2)$ and hence define an affine plane. Let $\mathcal{E} = \langle e_1, e_2 \rangle$ denote the 2-dimensional vector subspace spanned by e_1 and e_2 . Again by linear algebra $SL(d, 2)_{\mathcal{E}}$, and therefore also $G_{0, \mathcal{E}}$, acts point-transitively on $V \setminus \mathcal{E}$. If the unique block $B \in \mathcal{B}$ which is incident with the 3-subset $\{0, e_1, e_2\}$ contains some point outside \mathcal{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 11. 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): $G_0 \supseteq Sp(\frac{2d}{a}, p^a)$, $d \geq 2a$.

We will prove by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 3-design \mathcal{D} . First, let $p^a \neq 2$. The permutation group $PSp(\frac{2d}{a}, p^a)$ 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. [34, Ch. II, Thm. 9.15 (b)]). Thus, $G_0 \supseteq Sp(\frac{2d}{a}, p^a)$ has exactly two orbits on $V \setminus \langle x \rangle$ ($0 \neq x \in V$) of length at least

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

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 11, 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 11 yields $k \leq 5$. As $k - 2 \nmid v - 2$ for $k = 5$, it is sufficient by Lemma 9 (c) 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 [29] 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 $|\text{Out}(Sp(2d, 2))| = 1$, we have therefore

$$Sp(2d - 2, 2) \cong Sp(2d, 2)_{\{x, y\}} \trianglelefteq Sp(2d, 2)_{\mathcal{E}} = G_{0, \mathcal{E}}.$$

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 $B \in \mathcal{B}$ 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 11. 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 11, 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 8, we obtain

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

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 \mathcal{O}_i ($i = 1, 2, 3$) on $V \setminus \langle x \rangle$ of length $2^{3a} - 2^a, 2^{5a} - 2^{3a}, 2^{6a} - 2^{5a}$ (see, e.g., [2] or [11, Thm. 3.1]). Thus, G_0 has exactly three orbits on $V \setminus \langle x \rangle$ of length at least $|\mathcal{O}_i|$. 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 \mathcal{O}_2 or \mathcal{O}_3 , then we would obtain as above a contradiction to Corollary 11. Thus, we only have to consider the case when B contains points of $V \setminus \langle x \rangle$ which all lie in \mathcal{O}_1 . By [2], the orbit \mathcal{O}_1 is exactly known, and we have

$$\mathcal{O}_1 = x\Delta \setminus \langle x \rangle,$$

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 \mathcal{O}_1 . Since $|\mathcal{O}_1| \neq 1$, we can choose $\langle \bar{x} \rangle \in x\Delta$ with $\langle \bar{x} \rangle \neq \langle x \rangle$. Let $\bar{y} \in \langle \bar{x} \rangle$ be distinct from 0 and \bar{x} . Then, for symmetric reasons, the 3-subset $\{0, \bar{x}, \bar{y}\}$ is also incident with the unique block B . But, on the other hand, we have $\bar{x}\Delta \neq x\Delta$ for $\langle \bar{x} \rangle \neq \langle x \rangle$, 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 11. If $k = 4$, then applying [29] yields the flag-transitive design described in Part (1) of Main Theorem 1 with assertion (iii). For $k = 5$, we obtain with Lemma 9 (c) 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 9 (b) and (c), and Corollary 11.

4.2 Groups of Automorphisms of Almost Simple Type

Maintaining the same notation, let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 3-design with $G \leq \text{Aut}(\mathcal{D})$ acting flag-transitively on \mathcal{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 [35, Thm. 3].

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

We distinguish two subcases:

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

Let $\tilde{q} = q^e$, $e \geq 1$. Without restriction, we have here $q^e \geq 5$ as $PSL(2, 4) \cong PSL(2, 5)$, and $\text{Aut}(N) = P\Gamma L(2, q^e)$. First, we suppose that G is 3-transitive. In view of [35, Thm. 3], we have then only the 3- $(q^e + 1, q + 1, 1)$ design described in Part (2) of Main Theorem 1 (without the subcase in brackets) with $PSL(2, q^e) \leq G \leq P\Gamma L(2, q^e)$, $q \geq 3$, $e \geq 2$. Conversely, flag-transitivity holds as the 3-transitivity of G implies that G_x acts block-transitively on the derived Steiner 2-design \mathcal{D}_x for any $x \in X$. Since $PGL(2, q^e)$ is a transitive extension of $AGL(1, q^e)$, it is easily seen that the derived design at any given point of $GF(q^e) \cup \{\infty\}$ 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 $PSL(2, q^e)$ is a transitive extension of $AG^2L(1, q^e)$ (which is the group of all permutations of $GF(q^e)$ of the form $x \mapsto a^2x + c$ with $a, c \in GF(q^e)$, $a \neq 0$), we can deduce from [20] that the derived design at any given point is either $AG(e, q)$ with the lines as blocks or the Netto triple system $N(q^e)$. Thus, Part (2) of Main Theorem 1 holds with the subcase in brackets or Part (3) with $PSL(2, q^e) \leq G \leq P\Sigma L(2, q^e)$ (where, for an odd prime p , we define $P\Sigma L(2, p^a) = PSL(2, p^a) \rtimes \langle \tau_\alpha \rangle$ with $\tau_\alpha \in \text{Sym}(GF(p^a) \cup \{\infty\}) \cong S_v$ of order

a induced by the Frobenius automorphism $\alpha : GF(p^a) \longrightarrow GF(p^a)$, $x \mapsto x^p$. Conversely, in view of its 3-homogeneity, G is also block-transitive. By the orbit-stabilizer property, we obtain $|PSL(2, q^e)_B| = |PSL(2, q)|$ and in view of [22, Ch. 12, p. 286] actually

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

for any $B \in \mathcal{B}$. Since $PSL(2, q)$ 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 $PGL(2, q^e)$ is 3-homogeneous, the unique orbit under $PGL(2, q^e)$ on the 3-subsets of X splits under $PSL(2, q^e)$ 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) $N = PSL(d, \tilde{q})$, $d \geq 3$.

We have here $\text{Aut}(N) = P\Gamma L(d, \tilde{q}) \rtimes \langle \iota_\beta \rangle$, where ι_β denotes the graph automorphism induced by the inverse-transpose map $\beta : GL(d, \tilde{q}) \longrightarrow GL(d, \tilde{q})$, $x \mapsto {}^t(x^{-1})$. 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 $PG(2, \tilde{q})$ 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.

ad (a): Let \mathcal{G} denote a line of $PG(2, \tilde{q})$. It is well-known that the translation group $T(\mathcal{G})$ operates regularly on the points of $PG(2, \tilde{q}) \setminus \mathcal{G}$ 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 $PG(2, \tilde{q}) \setminus \mathcal{G}$, thus at least $\tilde{q}^2 + 3$ many. But, these are obviously more than half of the points of $PG(2, \tilde{q})$, a contradiction to $k \leq \lfloor \frac{v}{4} + 2 \rfloor$ by Proposition 10 (a).

ad (b): The pointwise stabilizer of three distinct points in $SL(3, \tilde{q})$ consists precisely of the diagonal matrices, and hence has order $(\tilde{q} - 1)^2$ (see, e.g., [34, Ch. II, Thm. 7.2 (b)]). To this corresponds in $PSL(3, \tilde{q})$ 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., [21, Ch. 3.2, Thm. 24]). Only for $\tilde{q} = 2$ and 4 both conditions are fulfilled. But, with regard to Lemma 9 (c), 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 $PG(d - 1, \tilde{q})$. 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 $PG(d - 1, \tilde{q}) \setminus \mathcal{H}$, but trivially on \mathcal{H} . If B contains at least one point outside \mathcal{H} , then it would already contain all points of $PG(d - 1, \tilde{q}) \setminus \mathcal{H}$, thus at least $\tilde{q}^{d-1} + 3$ many. However, as

$$v = \frac{\tilde{q}^d - 1}{\tilde{q} - 1} < 2\tilde{q}^{d-1} \iff \tilde{q}^d - 1 < 2(\tilde{q}^d - \tilde{q}^{d-1}) \iff 2\tilde{q}^{d-1} - 1 < \tilde{q}^d,$$

these are more than half of the points of $PG(d - 1, \tilde{q})$, the same contradiction as above. Thus, \mathcal{H} induces a 3-($\frac{\tilde{q}^d - 1}{\tilde{q} - 1}, k, 1$) design, on which G containing $PSL(d - 1, \tilde{q})$ as simple normal subgroup operates. Inductively, we obtain the minimal counter-example for $d = 3$. But, as we have shown above, G with $PSL(3, \tilde{q})$ as simple normal subgroup cannot act on any non-trivial 3-($\tilde{q}^2 + \tilde{q} + 1, k, 1$) design, and the assertion follows.

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

Here $\text{Aut}(N) = P\Gamma U(3, q^2)$, and $|G| = (q^3 + 1)q^3 \frac{(q^2-1)}{n} a$ with $n = (3, q + 1)$ and $a \mid 2ne$. Thus, from Remark 12, we obtain

$$q^2 + q + 1 = (k - 1)(k - 2) \frac{q + 1}{n} \frac{a}{|G_{xB}|} \quad \text{if } x \in B. \quad (4.4)$$

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

$$(v, w) = a_1 b_3^\tau + a_2 b_2^\tau + a_3 b_1^\tau,$$

where τ denotes the unique involutory automorphism $GF(q^2) \longrightarrow GF(q^2)$, $x \mapsto x^q$. We deduce from the proof of [34, Ch. II, Thm. 10.12] that the cyclic group

$$\left\{ \left(\begin{array}{c} c \\ c^{-2} \\ c \end{array} \right) \mid c \in GF(q^2)^*, c^{\tau+1} = 1 \right\}$$

of linear transformations on V induces a group U of dilatations of order $\frac{q+1}{n}$ 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

$$a_1 a_3^\tau + a_1^\tau a_3 = \text{Tr}(a_1 a_3^\tau) = 0$$

(where Tr denotes the trace map $GF(q^2) \longrightarrow GF(q)$, $x \mapsto x + x^q$) 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., [3, p. 87]), we call in the following non-absolute lines \mathcal{G} and \mathcal{H} *perpendicular* if \mathcal{G} passes through the pole of \mathcal{H} and \mathcal{H} passes, therefore, through the pole of \mathcal{G} .

By the definition of Steiner 3-designs, we may choose three distinct absolute points on \mathcal{G} , which are incident with a unique block $B \in \mathcal{B}$. Let us first assume

that B contains absolute points outside \mathcal{G} which are all on \mathcal{H} . It is clear that U fixes each point of \mathcal{G} , and hence in particular B . Furthermore, \mathcal{H} intersects \mathcal{G} in a non-absolute point x (see, e.g., [3, p. 88]). As U acts outside x semi-regularly on \mathcal{H} , we conclude that all point-orbits have length $\frac{q+1}{n}$. If we choose now three distinct absolute points on \mathcal{H} , then they are also incident with the unique block B . Thus, by the same arguments, U fixes each point of \mathcal{H} and acts outside x semi-regularly on \mathcal{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 9 (c). Thus, $n \neq 1$. For $n_1 + n_2 = 3$, it follows from equation (4.4) that $q^2 + q + 1 \mid (q-1)\frac{q}{n} < q^2 - q$, which is clearly not possible. In each of the other cases, polynomial division with remainder gives a contradiction to Lemma 9 (c).

Now, we assume that B contains absolute points outside \mathcal{G} which are not all on \mathcal{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 11.

Hence, we have shown that B is completely contained in \mathcal{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): $N = Sz(q)$, $v = q^2 + 1$, $q = 2^{2e+1} > 2$.

We have $\text{Aut}(N) = Sz(q) \rtimes \langle \alpha \rangle$, where α 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 12 that

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

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

Let us first remark that we only have one conjugacy 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 $B \in \mathcal{B}$ always an involution $\tau \in G_{xB} \cap Sz(q)$ 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 block-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 $\text{Aut}(N)_{0,1,\infty} = \langle \alpha \rangle$, and thus $G \cap \langle \alpha \rangle \leq G_{0B}$ by the definition of Steiner 3-designs. Setting $u = \frac{|G_{0B}|}{a}$, we next show that $u = 2$ or 4 . For the list of subgroups of $Sz(q)$, we refer to [48, Thm. 9]. First, let $G_B \cap Sz(q)$ be isomorphic to $Sz(\bar{q})$ for some $\bar{q} \geq 8$ such that $\bar{q}^m = q$, $m \geq 1$. As B can be regarded as the orbit of fixed points of involutions in $G_B \cap Sz(q)$, it follows that $k = \bar{q}^2 + 1$. Clearly, $m > 1$ (otherwise, $k = q^2 + 1$, a contradiction to Corollary 11). Thus, we have

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

As $q > 8$, Zsigmondy's theorem yields the existence of a 2-primitive prime divisor \bar{r} with $\bar{r} \perp 2^{2(2e+1)} - 1$. Then

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

But now [26, Thm. 3.5 (ii)] yields $(\bar{r}, \bar{q}) = 1$ and $\bar{r} > a$ since $\bar{r} \equiv 1 \pmod{(2e+1)}$. Therefore, we conclude that $\bar{q} = q$, a contradiction.

Let $G_B \cap Sz(q)$ be conjugate to a subgroup of $Sz(q)_x$ ($x \in X$). By the transitivity of G , we can choose x as fixed point of an involution. Thus, $x \in B$ by the remark above, contrary to the fact that $x \notin B$ by the flag-transitivity of G .

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

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

$$u = 2 \text{ or } 4.$$

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

$$2^{2e+3} = k^2 - 3k - 2. \quad (4.5)$$

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., [5, Thm. 3]). As we have $e \geq 1$, it follows that $(e, k) = (2, 13)$ is the only solution of equation (4.5). But, by Lemma 9 (b), this is impossible, which verifies the claim.

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

Here $\text{Aut}(N) = Re(q) \rtimes \langle \alpha \rangle$, where α denotes the Frobenius automorphism $GF(q) \rightarrow GF(q)$, $x \mapsto x^3$. Thus, by Dedekind's law, $G = Re(q) \rtimes (G \cap \langle \alpha \rangle)$, and $|G| = (q^3 + 1)q^3(q-1)a$ with $a \mid 2e + 1$. From Remark 12, we hence obtain

$$q^2 + q + 1 = (k-1)(k-2) \frac{a}{|G_{xB}|} \quad \text{if } x \in B. \quad (4.6)$$

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

We remark that we only have one conjugacy 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 $\tau \in G_{xB} \cap Re(q)$ with $x \in B$.

We show furthermore that $9 \mid |G_B \cap Re(q)|$. Let P be a Sylow 3-subgroup of $Re(q)$. According to [49], P contains a normal elementary Abelian subgroup \bar{P} of order q^2 containing $Z(P)$. Thus, there exist subgroups U_1, U_2 of \bar{P} of order 3 with $U_1 \leq Z(P)$, $U_2 \not\leq Z(P)$. As the stabilizer of three distinct points in $Re(q)$ 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 conjugate in $Re(q)$, then they are already conjugate in $Re(q)_x$. But, as $Z(P)$ is a characteristic subgroup of $Re(q)_x$, this is impossible. Therefore, we have at least two distinct conjugacy classes of subgroups of order 3 in $Re(q)$, 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 $(G_B \cap Re(q)) \cap (G \cap \langle \alpha \rangle) = 1$. Therefore, as G_B acts transitively on the points of B , Dedekind's law yields

$$k = |0^{G_B}| = [G_B : G_{0B}] = [G_B \cap Re(q) : G_{0B} \cap Re(q)]. \quad (4.7)$$

Thus, $G_B \cap Re(q)$ acts also transitively on the points of B .

In the following, we will examine the list of subgroups of $Re(q)$ (cf. [49]). As 9 divides the order of $G_B \cap Re(q)$, clearly $G_B \cap Re(q)$ cannot be conjugate 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 conjugate 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 $Re(\bar{q})$ for some $\bar{q} \geq 27$ such that $\bar{q}^m = q$, $m \geq 1$. Let $\bar{X} \subseteq X$ with $|\bar{X}| = \bar{q}^3 + 1$. We first show that only involutions may have fixed points in $X \setminus \bar{X}$. Let $g \in G$ with $o(g) = s$, where $s \neq 2$ is a prime. If $s \mid \bar{q} - 1$, then g has two distinct fixed points in \bar{X} , and none in $X \setminus \bar{X}$ 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 \bar{X} . If $s \mid \bar{q} + 1$, we show that g has no fixed point in X . Obviously, g has no fixed point in \bar{X} . As $3 \nmid \bar{q} + 1$, we assume that g has two

distinct fixed points in $X \setminus \bar{X}$. But, as

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

and hence $(q^3 - \bar{q}^3 - 2, \bar{q} + 1) = (2, \bar{q} + 1) = 2$, this is impossible. If $s \mid \bar{q} + 1 \pm 3\bar{l}$, we show again that g has no fixed point in X . As $\bar{q}^3 + 1 = (\bar{q} + 1 + 3\bar{l})(\bar{q} + 1 - 3\bar{l})(\bar{q} + 1)$, it is obvious that g has no fixed point in \bar{X} . Since $3 \nmid \bar{q} + 1 \pm 3\bar{l}$, we assume in both cases that g has two distinct fixed points in $X \setminus \bar{X}$. But, as $(\bar{q} + 1 + 3\bar{l})(\bar{q} + 1 - 3\bar{l}) = \bar{q}^2 - \bar{q} + 1$, and

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

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

As $G_B \cap Re(q)$ acts transitively on the points of B , we have $B \subseteq \bar{X}$ or $B \subseteq X \setminus \bar{X}$.

In the first case, equation (4.7) yields

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

while in the second

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

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 $k = \bar{q}^3 + 1$. Clearly, $m > 1$ (otherwise, $k = q^3 + 1$, a contradiction to Corollary 11).

Thus, we have

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

Zsigmondy's theorem yields the existence of a 3-primitive prime divisor \bar{r} with $\bar{r} \perp 3^{3(2e+1)} - 1$. Then

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

But now [26, Thm. 3.5 (ii)] yields $(\bar{r}, \bar{q}) = 1$ and $\bar{r} > a$ since $\bar{r} \equiv 1 \pmod{(2e+1)}$.

Therefore, we have $\bar{q} = q$, a contradiction.

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

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

where $\bar{a} \mid a$. Here, $n < 4$ since otherwise $(k-1)(k-2) \equiv 0 \pmod{4}$ by equation (4.6) and, by applying Lemma 9 (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

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

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

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

as is well-known). As $8 \mid |Re(\bar{q})|$, clearly $((\bar{q}^3 + 1)\bar{q}^3(\bar{q} - 1))^{\bar{m}+1}$ is divisible by $2^{3(\bar{m}+1)}$. Thus $\frac{2^{2\bar{m}+2}q^3}{((\bar{q}^3+1)\bar{q}^3(\bar{q}-1))^{\bar{m}+1}} \neq 1$, yielding a contradiction to Lemma 9 (c).

Let $G_B \cap Re(q)$ be conjugate 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 conjugate to a subgroup of $PSL(2, q) \times \langle \tau \rangle$, where τ denotes any involution in $Re(q)$. By the remark above, we can choose τ such that 0 is a fixed point under τ . 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. [22, Ch. 12, p. 285f.] or [34, Ch. II, Thm. 8.27]):

- (i) $G_B \cap Re(q)$ is conjugate to $PSL(2, \bar{q})$ or $PSL(2, \bar{q}) \times \langle \tau \rangle$ for some $\bar{q} \geq 27$ such that $\bar{q}^m = q$, $m \geq 1$.

Let $\bar{X} \subseteq X$ with $|\bar{X}| = \bar{q} + 1$. First, we show again that only involutions may have fixed points in $X \setminus \bar{X}$. Let $g \in G$ with $o(g) = s$, where $s \neq 2$ is a prime. If $s \mid \bar{q} - 1$, then g has two distinct fixed points in \bar{X} and none in $X \setminus \bar{X}$. For $s = 3$, clearly g has exactly one fixed point, which lies in \bar{X} . If $s \mid \bar{q} + 1$, we show that g has no fixed point in X . Obviously, g has no fixed point in \bar{X} . As $3 \nmid \bar{q} + 1$, we assume that g has two distinct fixed points in

$X \setminus \bar{X}$. But, as

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

and hence $(q^3 - \bar{q} - 2, \bar{q} + 1) = (2, \bar{q} + 1) = 2$, this is impossible.

Again, we have $B \subseteq \bar{X}$ or $B \subseteq X \setminus \bar{X}$. With equation (4.7), we obtain

$$k = \bar{q} + 1,$$

in the first case, while in the second

$$k = \frac{\bar{q}(\bar{q}^2 - 1)}{n},$$

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 $k = \bar{q} + 1$. Then

$$q^2 + q + 1 \mid \bar{q}(\bar{q} - 1)a$$

by equation (4.6). Since $(q^2 + q + 1, \bar{q}) = 1$ and $(q^2 + q + 1, \bar{q} - 1) = (3, \bar{q} - 1) = 1$, this is equivalent to

$$q^2 + q + 1 \mid a,$$

which is impossible as clearly $a \leq q$. Now, we assume that $k = \frac{\bar{q}(\bar{q}^2 - 1)}{n}$. Then

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

where $\bar{a} \mid a$. Considering the first yields

$$(q^2 + q + 1) \frac{n}{2} = (k - 1)(k - 2) \frac{a}{\bar{a}}$$

by equation (4.6). Clearly, $n = 2$ is impossible. If $n = 4$, then $k = \frac{\bar{q}(\bar{q}^2 - 1)}{4}$ is divisible by 2 but not by 4. Thus, 4 is a divisor of $k - 2$, but not of the left hand 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 $|G_{0B}| = n\bar{a}$. Here, $n < 4$ again. For $n = 2$, we have $k = \frac{\bar{q}^3 - \bar{q}}{2}$. Then, polynomial division with remainder gives

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

for a suitable $\bar{m} \in \mathbb{N}$. As $(\bar{q}^2 - 1)^{\bar{m}+1}$ is divisible by $2^{3(\bar{m}+1)}$, clearly $\frac{2^{2\bar{m}+2} q^3}{(\bar{q}^3 - \bar{q})^{\bar{m}+1}} \neq 1$, yielding a contradiction to Lemma 9 (c).

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

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

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

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

for a suitable $\bar{m} \in \mathbb{N}$. As clearly $\frac{2^{\bar{m}+1} q^3}{\bar{q}^{\bar{m}+1}} \neq 1$, this leads to a contradiction to Lemma 9 (c) again.

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

Let $\bar{X} \subseteq X$ with $|\bar{X}| = q + 1$. Again, we show that only involutions may have fixed points in $X \setminus \bar{X}$. 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 \bar{X} . If $s \mid c$, then g has exactly two distinct fixed points, which lie in \bar{X} .

For $B \subseteq \bar{X}$, we deduce that $k = \bar{q}$ or $\bar{q}c$, and for $B \subseteq X \setminus \bar{X}$ that $k = \frac{\bar{q}c}{n}$ 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 $k = \bar{q}$, we have already shown that this is impossible. We assume next that $k = \bar{q}c$. 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 9 (c), which is impossible as we have already seen. For $2 \nmid c$, polynomial division with remainder gives

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

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

Now, we assume that $k = \frac{\bar{q}c}{n}$. Then

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

where $\bar{a} \mid a$. When considering the first possibility, clearly equation (4.6) rules out the case $n = 1$. So, we assume that $n = 2$. Hence $k = \frac{\bar{q}c}{2}$, but polynomial division with remainder yields

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

for a suitable $\bar{m} \in \mathbb{N}$. But since $c \mid q - 1$, the largest possible power of 2 that is contained in $c^{\bar{m}+1}$ is $2^{\bar{m}+1}$. Thus $\frac{2^{2\bar{m}+2}q^3}{(\bar{q}c)^{\bar{m}+1}} \neq 1$, the same contradiction as above.

Now, we assume that $|G_{0B}| = 2n\bar{a}$. For $n = 1$, we get $k = \bar{q}c$, which is not possible as shown above. The case $n = 2$ is ruled out by equation (4.6) since $(k - 1)(k - 2)$ is not divisible by 4 as we already know.

This completes the list of subgroups of $Re(q)$ 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 $X^\pm \setminus \{x\}$ 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 $X^\pm \setminus \{x, y\}$ of length $2(2^{d-1} \mp 1)(2^{d-2} \pm 1)$ and 2^{2d-2} (see, e.g., [35, p. 69]). We will show by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 3-design \mathcal{D} .

Let $z \in X^\pm \setminus \{x, y\}$. Then, in both cases, the 3-subset $\{x, y, z\}$ is incident with a unique block $B \in \mathcal{B}$. By Remark 12, we have therefore

$$(v - 2) |G_{xB}| = (k - 1)(k - 2) |G_{xy}|, \quad (4.8)$$

where

$$|G_{xB}| = n \frac{|G_{xy}|}{|z^{G_{xy}}|}$$

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

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

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 (4.8) yields

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

But, on the other hand, we have $v - 2 \geq (k-1)(k-2)$ by Proposition 10 (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 8, Lemma 9 (c), and Corollary 11.

Case (9): $N = M_v$, $v = 11, 12, 22, 23, 24$.

Here G is always 3-transitive, and thus [35, Thm. 3] yields the design described in Part (iv) of Main Theorem 1. Obviously, flag-transitivity holds as the 3-transitivity of G implies that G_x acts block-transitively on the derived Steiner 2-design \mathcal{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 8, Lemma 9 (c), and Corollary 11.

This completes the proof of Main Theorem 1.

Chapter 5

The Classification of all Flag-transitive Steiner 4-Designs

The classification of all non-trivial Steiner 4-designs admitting a flag-transitive group of automorphisms can be stated as follows.

Main Theorem 2. *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 4-design. Then $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on \mathcal{D} if and only if one of the following occurs:*

- (1) \mathcal{D} is isomorphic to the Witt 4-(11, 5, 1) design, and $G \cong M_{11}$,
- (2) \mathcal{D} is isomorphic to the Witt 4-(23, 7, 1) design, and $G \cong M_{23}$.

For a detailed description of the Witt t -($v, k, 1$) designs with their associated Mathieu groups M_v of degree v , we refer, e.g., to [50].

5.1 Groups of Automorphisms of Affine Type

In the sequel, we start with the proof of Main Theorem 2. Using the notation as before, let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 4-design with $G \leq \text{Aut}(\mathcal{D})$ acting flag-transitively on \mathcal{D} . We recall that due to Proposition 6, we may restrict ourselves to the consideration of the finite 2-transitive permutation groups listed in Chapter 3. Let us assume in this section that G is of affine type.

Case (1): $G \leq AFL(1, v)$, $v = p^d$.

As G is point 2-transitive, we have $|G| = v(v-1)a$ with $a \mid d$. Using Lemma 8, we therefore obtain

$$(p^d - 2)(p^d - 3) \mid a(k-1)(k-2)(k-3) \mid d(k-1)(k-2)(k-3),$$

and hence in particular

$$(p^d - 2)(p^d - 3) \leq d(k-1)(k-2)(k-3).$$

But, Proposition 10 (b) yields

$$p^d - 3 \geq (k-2)(k-3),$$

and thus

$$p^d - 2 \leq d(k-1)$$

must hold. With regard to Corollary 11, this leaves only a very small number of possibilities for k to check, which can easily be ruled out by hand using Lemma 9 (b) and (c). Therefore, $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} .

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

In the following, let e_i denote the i -th standard basis 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 prove by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} .

First, let $p^a > 3$. For $d = 2a$, let $U = U(\langle e_1 \rangle) \leq G_0$ denote the subgroup of all transvections with axis $\langle e_1 \rangle$. Clearly, U fixes as points only the elements of $\langle e_1 \rangle$. Thus, G_0 has point-orbits of length at least p^a outside $\langle e_1 \rangle$. Let $S = \{0, e_1, x, y\}$ be a 4-subset of distinct points with $x, y \in \langle e_1 \rangle$. Obviously, U fixes the unique block $B \in \mathcal{B}$ which is incident with S . Therefore, if B contains at least one point outside $\langle e_1 \rangle$, then we would obtain $k \geq p^a + 4$. But, according to Corollary 11, we have $k \leq p^a + 2$, a contradiction. Hence, B is contained completely in $\langle e_1 \rangle$. Then, as G is flag-transitive, we may conclude that each block lies in an affine line. But, by the definition of Steiner 4-designs, any four distinct non-collinear points

must also be incident with a unique block, a contradiction. Thus, let us assume that $d \geq 3a$. Then again $SL(\frac{d}{a}, p^a)_{e_1}$, and hence also G_{0,e_1} , acts point-transitively on $V \setminus \langle e_1 \rangle$. As above, let $S = \{0, e_1, x, y\}$ be a 4-subset of distinct points with $x, y \in \langle e_1 \rangle$. If the unique block $B \in \mathcal{B}$ which is incident with S contains some point outside $\langle e_1 \rangle$, then it would already contain all points outside, thus at least $p^d - p^a + 4$ many, which obviously contradicts Corollary 11. We conclude that B lies completely in $\langle e_1 \rangle$, and by the same argument as above, we obtain that here $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} .

Now, let $p^a = 2$. To exclude trivial Steiner 4-designs, let $v = 2^d > k > 4$. For $d = 3$, we have $v = 8$ and $k = 5$ by Corollary 11, which is not possible in view of Lemma 9 (c). So, we may assume that $d > 3$. We remark that clearly any three distinct points are non-collinear in $AG(d, 2)$ and hence define an affine plane. Let $\mathcal{E} = \langle e_1, e_2 \rangle$ denote the 2-dimensional vector subspace spanned by e_1 and e_2 . Then again $SL(d, 2)_{\mathcal{E}}$, and hence also $G_{0,\mathcal{E}}$, acts point-transitively on $V \setminus \mathcal{E}$. If the unique block $B \in \mathcal{B}$ which is incident with the 4-subset $\{0, e_1, e_2, e_1 + e_2\}$ contains some point outside \mathcal{E} , then it would already contain all points of $V \setminus \mathcal{E}$. But then, we would have $k \geq 2^d - 4 + 4 = 2^d$, a contradiction to Corollary 11. Therefore, B can be identified with \mathcal{E} , and the flag-transitivity of G implies then that each block must be an affine plane. Thus, we always have $k = 4$, a contradiction. Similar arguments hold for $p^a = 3$.

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

We will show by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} . First, let $p^a \neq 2$. The permutation group $PSp(\frac{2d}{a}, p^a)$ 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. [34, Ch. II, Thm. 9.15 (b)]). Thus, $G_0 \cong Sp(\frac{2d}{a}, p^a)$ has exactly two orbits on $V \setminus \langle x \rangle$ ($0 \neq x \in V$) of length at least

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

Let $S = \{0, x, y, z\}$ be a 4-subset with $y, z \in \langle x \rangle$. If the unique block which is incident with S contains at least one point of $V \setminus \langle x \rangle$, then we would have $k > p^d + 4$. But, on the other hand, we have $k \leq p^d + 2$ by Corollary 11,

a contradiction. Therefore, we can argue as in Case (2) to obtain the desired contradiction in this case.

Now, let $p^a = 2$. As we neglect trivial Steiner 4-designs, $v = 2^{2d} > k > 4$ must hold. For $d = 2$ (here $Sp(4, 2) \cong S_6$ as well-known), Corollary 11 yields $k \leq 6$. But, Lemma 9 (c) rules out the cases when $k = 5$ or 6 . Thus, let $d > 2$. 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

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

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

$$Sp(2d - 2, 2) \cong Sp(2d, 2)_{\{x, y\}} \trianglelefteq Sp(2d, 2)_\mathcal{E} = G_{0, \mathcal{E}}.$$

As $Sp(2d - 2, 2)$ 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 $B \in \mathcal{B}$ which is incident with the 4-subset $\{0, x, y, x + y\}$ contains some point in $V \setminus \mathcal{E}$, then we would have $k \geq 2^{2d-2} + 3$, a contradiction to Corollary 11. Thus, B can be identified with \mathcal{E} . But then, by the flag-transitivity of G , each block is an affine plane. Therefore, always $k = 4$ holds, again a contradiction.

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

We will also prove by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} . First, let $a = 1$. Then we have $v = 2^6 = 64$, and by Corollary 11, it follows that $k \leq 10$. 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 8, we obtain

$$r = \frac{63 \cdot 62 \cdot 61}{(k-1)(k-2)(k-3)} \Big| |G_0| \Big| 2^6 \cdot 3^3 \cdot 7.$$

But this implies that k is at least 63, 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 \mathcal{O}_i ($i = 1, 2, 3$) on $V \setminus \langle x \rangle$ of length $2^{3a} - 2^a, 2^{5a} - 2^{3a}, 2^{6a} - 2^{5a}$ (cf., e.g., [2] or [11, Thm. 3.1]). Thus, G_0 has exactly three orbits on $V \setminus \langle x \rangle$ of length at least $|\mathcal{O}_i|$. Let $S = \{0, x, y, z\}$ be a 4-subset with $y, z \in \langle x \rangle$. Again, we will show that the unique block $B \in \mathcal{B}$ which is incident with S lies completely in $\langle x \rangle$. If B contains at least one point of $V \setminus \langle x \rangle$ in \mathcal{O}_2 or \mathcal{O}_3 , then we would obtain as above a contradiction to Corollary 11. Thus, we only have to consider the case when B contains points of $V \setminus \langle x \rangle$ which all lie in \mathcal{O}_1 . By [2], the orbit \mathcal{O}_1 is exactly known, and we have

$$\mathcal{O}_1 = x\Delta \setminus \langle x \rangle,$$

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 \mathcal{O}_1 . Since $|\mathcal{O}_1| \neq 1$, we can choose $\langle \bar{x} \rangle \in x\Delta$ with $\langle \bar{x} \rangle \neq \langle x \rangle$. But then, for symmetric reasons, the 4-subset $\{0, \bar{x}, \bar{y}, \bar{z}\}$ with $\bar{y}, \bar{z} \in \langle \bar{x} \rangle$ must also be incident with the unique block B , a contradiction to the fact that $\bar{x}\Delta \neq x\Delta$ for $\langle \bar{x} \rangle \neq \langle x \rangle$. Consequently, 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 $k \leq 6$ by Corollary 11. But, Lemma 9 (c) obviously eliminates the cases when $k = 5$ or 6 .

Cases (6)-(8).

For the existence of non-trivial Steiner 4-designs, we have in these cases only finitely many possibilities for k to check, which can easily be ruled out by hand using Lemma 8, Lemma 9 (c), and Corollary 11.

5.2 Groups of Automorphisms of Almost Simple Type

Maintaining the same notation, let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 4-design with $G \leq \text{Aut}(\mathcal{D})$ acting flag-transitively on \mathcal{D} . Before we consider in this section successively those cases where G is of almost simple type, we prove some lemmas which will be required for Case (2).

In the following, let q be a prime power p^e , and U a subgroup of $PSL(2, q)$. Furthermore, let N_l denote the number of orbits of length l and let $n = (2, q - 1)$. We will determine the orbit-lengths from the action of subgroups of $PSL(2, q)$ on the points of the projective line. Thereby, we remark that for subgroups $U_1 \leq U_2 \leq PSL(2, q)$, any orbit of U_2 is a union of orbits of U_1 . For the list of subgroups of $PSL(2, q)$, we refer to [22, Ch. 12, p. 285f.] or [34, Ch. II, Thm. 8.27]. In the special case when $q \equiv 3 \pmod{4}$, the orbit lengths have also been calculated in [12, Sect. 4].

Well-known is the following fact (see, e.g., [34, Ch. II, p. 191f.]).

Lemma 16. *Let g be a non-trivial element in $PSL(2, q)$ of order c with f distinct fixed points. Then $c = p$ and $f = 1$, $c \mid \frac{q+1}{n}$ and $f = 0$, or $c \mid \frac{q-1}{n}$ and $f = 2$.*

Lemma 17. *Let U be the cyclic group of order c with $c \mid \frac{q \pm 1}{n}$. Then, we have*

- (a) *if $c \mid \frac{q+1}{n}$, then $N_c = (q + 1)/c$,*
- (b) *if $c \mid \frac{q-1}{n}$, then $N_1 = 2$ and $N_c = (q - 1)/c$.*

Proof. This is an obvious consequence of Lemma 16. □

Lemma 18. *Let U be the dihedral group of order $2c$ with $c \mid \frac{q \pm 1}{n}$. Then*

- (i) *for $q \equiv 1 \pmod{4}$, we have*
 - (a) *if $c \mid \frac{q+1}{2}$, then $N_c = 2$ and $N_{2c} = (q + 1 - 2c)/(2c)$,*
 - (b) *if $c \mid \frac{q-1}{2}$, then $N_2 = 1$, $N_c = 2$, and $N_{2c} = (q - 1 - 2c)/(2c)$, unless $c = 2$, in which case $N_2 = 3$ and $N_4 = (q - 5)/4$,*

(ii) for $q \equiv 3 \pmod{4}$, we have

(a) if $c \mid \frac{q+1}{2}$, then $N_{2c} = (q+1)/(2c)$,

(b) if $c \mid \frac{q-1}{2}$, then $N_2 = 1$ and $N_{2c} = (q-1)/(2c)$,

(iii) for $q \equiv 0 \pmod{2}$, we have

(a) if $c \mid q+1$, then $N_c = 1$ and $N_{2c} = (q+1-c)/(2c)$,

(b) if $c \mid q-1$, then $N_2 = 1$, $N_c = 1$, and $N_{2c} = (q-1-c)/(2c)$.

Proof. First, let $q \equiv 1 \pmod{4}$. If $c \mid \frac{q+1}{2}$, then U has a cyclic subgroup of order c , and hence by Lemma 17 its orbit-lengths are multiples of c . On the other hand, U has at least c involutions contained in one conjugacy class with two distinct fixed points, and hence we have two orbits of length c and all other orbits are regular. If $c \mid \frac{q-1}{2}$, then U has a cyclic subgroup of order c with two distinct fixed points which are interchanged by an involution, and thus $N_2 \geq 1$. We conclude that $N_2 = 1$, unless $c = 2$, in which case we have exactly three involutions with two distinct fixed points and hence $N_2 = 3$. On the other hand, U has at least c involutions contained in one conjugacy class with two distinct fixed points, and hence we have two orbits of length c if $c > 2$ and all remaining orbits are regular.

For $q \equiv 3 \pmod{4}$, we remark that U has at least c involutions contained in one conjugacy class which are fixed point free, and hence we cannot have orbits of length c .

Now, let $q \equiv 0 \pmod{2}$. If $c \mid q+1$, then U has a cyclic subgroup of order c , and hence by Lemma 17 its orbit-lengths are multiples of c . On the other hand, U has at least c involutions contained in one conjugacy class with one fixed point, and hence we have one orbit of length c and all remaining orbits are regular. If $c \mid q-1$, then U has a cyclic subgroup of order c with two distinct fixed points which are interchanged by an involution, thus $N_2 = 1$. On the other hand, U has at least c involutions contained in one conjugacy class with one fixed point, and hence we have one orbit of length c and all remaining orbits are regular. \square

Lemma 19. *Let U be the elementary Abelian group of order $\bar{q} \mid q$. Then, we have $N_1 = 1$ and $N_{\bar{q}} = q/\bar{q}$.*

Proof. We conclude from the Cauchy-Frobenius Lemma that the number of orbits is $(q/\bar{q}) + 1$. As all orbit-lengths are powers of p , we have therefore just one orbit of length 1 and all other orbits are regular. \square

Lemma 20. *Let U be a semi-direct product of the elementary Abelian group of order $\bar{q} \mid q$ and the cyclic group of order c with $c \mid \bar{q} - 1$ and $c \mid q - 1$. Then, we have $N_1 = 1$, $N_{\bar{q}} = 1$, and $N_{\bar{q}c} = (q - \bar{q})/(\bar{q}c)$.*

Proof. As U has an elementary Abelian subgroup of order $\bar{q} \mid q$, we can apply Lemma 19. Thus, we have one orbit of length 1 and all other orbit-lengths are multiples of \bar{q} . However, U has a cyclic subgroup of order c , and thus Lemma 17 yields for the orbit-lengths $l \equiv 0$ or $1 \pmod{c}$. If $l \equiv 0 \pmod{c}$, then necessarily $l = \bar{q}c$. Otherwise, $l = 1$ or \bar{q} . Since an element of order c has two distinct fixed points, the claim follows. \square

Lemma 21. *Let U be $PSL(2, \bar{q})$ with $\bar{q}^m = q$, $m \geq 1$. Then, we have $N_{\bar{q}+1} = 1$, $N_{\bar{q}(\bar{q}-1)} = 1$ if m is even, and all other orbits are regular.*

Proof. Due to the fact that all subgroups of the form $PSL(2, \bar{q})$ of $PSL(2, q)$ are conjugate (see, e.g., [22, Ch. 12, p. 279]), U can be identified with the group consisting of all linear fractional mappings $GF(\bar{q}) \cup \{\infty\} \rightarrow GF(\bar{q}) \cup \{\infty\}$, $x \mapsto \frac{ax+b}{cx+d}$ (where $a, b, c, d \in GF(\bar{q})$, $ad - bc$ is a nonzero square and the usual conventions for ∞ holds) with $GF(\bar{q})$ the unique subfield of $GF(q)$ of order \bar{q} . As U acts transitively on the points of $GF(\bar{q})$, we have an orbit of length $\bar{q} + 1$. As U has a subgroup of order $\bar{q}(\bar{q} - 1)/n$ which is a semi-direct product of the elementary Abelian group of order $\bar{q} \mid q$ and the cyclic group of order $(\bar{q} - 1)/n$, we deduce from Lemma 20 that all other orbit-lengths are multiples of $\bar{q}(\bar{q} - 1)/n$. On the other hand, U has an element of order $(\bar{q} + 1)/n$ which is fixed point free if m is odd, and in this case, all orbit-lengths are multiples of $(\bar{q} + 1)/n$ and hence all other orbits are regular. If m is even, then the element of order $(\bar{q} + 1)/n$ has two distinct fixed points outside the $\bar{q} + 1$ points, and thus we have one orbit of length $\bar{q}(\bar{q} - 1)$ and all remaining orbits are regular. \square

Lemma 22. *Let U be $PGL(2, \bar{q})$ with $\bar{q}^m = q$, $m > 1$ even. Then, we have $N_{\bar{q}+1} = 1$, $N_{\bar{q}(\bar{q}-1)} = 1$, and all other orbits are regular.*

Proof. The assertion follows immediately from Lemma 21. □

Lemma 23. *Let U be isomorphic to A_4 . Then*

(i) *for $q \equiv 1 \pmod{4}$, we have*

(a) *if $3 \mid \frac{q+1}{2}$, then $N_6 = 1$ and $N_{12} = (q - 5)/12$,*

(b) *if $3 \mid \frac{q-1}{2}$, then $N_4 = 2$, $N_6 = 1$, and $N_{12} = (q - 13)/12$,*

(c) *if $3 \mid q$, then $N_4 = 1$, $N_6 = 1$, and $N_{12} = (q - 9)/12$,*

(ii) *for $q \equiv 3 \pmod{4}$, we have*

(a) *if $3 \mid \frac{q+1}{2}$, then $N_{12} = (q + 1)/12$,*

(b) *if $3 \mid \frac{q-1}{2}$, then $N_4 = 2$ and $N_{12} = (q - 7)/12$,*

(c) *if $3 \mid q$, then $N_4 = 1$ and $N_{12} = (q - 3)/12$,*

(iii) *for $q = 2^e$, $e \equiv 0 \pmod{2}$, we have $N_1 = 1$, $N_4 = 1$, and $N_{12} = (q - 4)/12$.*

Proof. We have $p > 2$, or $p = 2$ and $e \equiv 0 \pmod{2}$. First, let $q \equiv 1 \pmod{4}$. As there are in U three involutions contained in one conjugacy class with two distinct fixed points, we have always one orbit of length 6 in subcases (a) and (b). On the other hand, there are in U four subgroups of order 3 contained in one conjugacy class with two distinct fixed points if $3 \mid \frac{q-1}{2}$, and none if $3 \mid \frac{q+1}{2}$. This implies for (a) that all remaining orbits are regular, and for (b) that U has exactly two orbits of equal length on the set of these fixed points and all other orbits are regular. If $3 \mid q$, then we have more precisely $q = 3^e$ with $e \equiv 0 \pmod{2}$, and since $PSL(2, 3) \cong A_4$, the claim follows by applying Lemma 21.

For $q \equiv 3 \pmod{4}$, we remark that the three involutions contained in one conjugacy class are fixed point free, and hence we cannot have orbits of length 6 in (a) and (b). If $3 \mid q$, then we have more precisely $q = 3^e$ with $e \equiv 1 \pmod{2}$, and the claim follows again by Lemma 21.

Now, let $q = 2^e$ with $e \equiv 0 \pmod{2}$. Since the set of fixed points of some subgroup is left invariant by its normalizer, clearly the normalizer $\mathcal{N}_U(P)$ of a Sylow 2-subgroup P in U has then exactly one fixed point. But as in U there is only one Sylow 2-subgroup, we have clearly $\mathcal{N}_U(P) = U$, and hence U has one orbit of length 1. On the other hand, since always $3 \mid q - 1$ in this case, U has an element of order 3 with two distinct fixed points which implies the existence of one orbit of length 4, and all remaining orbits are regular. \square

Lemma 24. *Let U be isomorphic to S_4 . Then*

- (i) *for $q \equiv 1 \pmod{8}$, we have*
 - (a) *if $3 \mid \frac{q+1}{2}$, then $N_6 = 1$, $N_{12} = 1$, and $N_{24} = (q - 17)/24$,*
 - (b) *if $3 \mid \frac{q-1}{2}$, then $N_6 = 1$, $N_8 = 1$, $N_{12} = 1$, and $N_{24} = (q - 25)/24$,*
 - (c) *if $3 \nmid q$, then $N_4 = 1$, $N_6 = 1$, and $N_{24} = (q - 9)/24$,*
- (ii) *for $q \equiv -1 \pmod{8}$, we have*
 - (a) *if $3 \mid \frac{q+1}{2}$, then $N_{24} = (q + 1)/24$,*
 - (b) *if $3 \mid \frac{q-1}{2}$, then $N_8 = 1$ and $N_{24} = (q - 7)/24$.*

Proof. We have $q \equiv \pm 1 \pmod{8}$. As U has a subgroup isomorphic to A_4 , Lemma 23 yields orbits of length 4, 6, 8, 12, 24. First, let $q \equiv 1 \pmod{8}$. As there are in U three involutions contained in one conjugacy class with two distinct fixed points, we have always one orbit of length 6 in subcases (a) and (b). On the other hand, we have in U four subgroups of order 3 contained in one conjugacy class with two distinct fixed points if $3 \mid \frac{q-1}{2}$, and none if $3 \mid \frac{q+1}{2}$. Thus, for (b) we conclude that U necessarily has one orbit of length 8 on the set of these fixed points. Furthermore, if $N_{12} = 0$, then $N_{24} = (q - 13)/24$ which is not integer. Hence, $N_{12} = 1$ and $N_{24} = (q - 25)/24$. For (a) we deduce again if $N_{12} = 0$, then $N_{24} = (q - 5)/24$ which is not integer. Thus, $N_{12} = 1$ and $N_{24} = (q - 17)/24$. For $3 \nmid q$, the assertion follows obviously from Lemma 23 (ii)(c).

Now, let $q \equiv -1 \pmod{8}$. Then, clearly $3 \nmid q$. We remark that the three involutions contained in one conjugacy class are fixed point free, and hence we cannot have orbits of length 6 in (a) and (b). Furthermore, we cannot have orbits of length 12 since otherwise we would have one-point stabilizers of order 2. \square

Lemma 25. *Let U be isomorphic to A_5 . Then*

(i) *for $q \equiv 1 \pmod{4}$, we have*

- (a) *if $q = 5^e$, $e \equiv 1 \pmod{2}$, then $N_6 = 1$ and $N_{60} = (q - 5)/60$,*
- (b) *if $q = 5^e$, $e \equiv 0 \pmod{2}$, then $N_6 = 1$, $N_{20} = 1$, and $N_{60} = (q - 25)/60$,*
- (c) *if $15 \mid \frac{q+1}{2}$, then $N_{30} = 1$ and $N_{60} = (q - 29)/60$,*
- (d) *if $3 \mid \frac{q+1}{2}$ and $5 \mid \frac{q-1}{2}$, then $N_{12} = 1$, $N_{30} = 1$, and $N_{60} = (q - 41)/60$,*
- (e) *if $3 \mid \frac{q-1}{2}$ and $5 \mid \frac{q+1}{2}$, then $N_{20} = 1$, $N_{30} = 1$, and $N_{60} = (q - 49)/60$,*
- (f) *if $15 \mid \frac{q-1}{2}$, then $N_{12} = 1$, $N_{20} = 1$, $N_{30} = 1$, and $N_{60} = (q - 61)/60$,*
- (g) *if $3 \mid q$ and $5 \mid \frac{q+1}{2}$, then $N_{10} = 1$ and $N_{60} = (q - 9)/60$,*
- (h) *if $3 \mid q$ and $5 \mid \frac{q-1}{2}$, then $N_{10} = 1$, $N_{12} = 1$, and $N_{60} = (q - 21)/60$,*

(ii) *for $q \equiv 3 \pmod{4}$, we have*

- (a) *if $15 \mid \frac{q+1}{2}$, then $N_{60} = (q + 1)/60$,*
- (b) *if $3 \mid \frac{q+1}{2}$ and $5 \mid \frac{q-1}{2}$, then $N_{12} = 1$ and $N_{60} = (q - 11)/60$,*
- (c) *if $3 \mid \frac{q-1}{2}$ and $5 \mid \frac{q+1}{2}$, then $N_{20} = 1$ and $N_{60} = (q - 19)/60$,*
- (d) *if $15 \mid \frac{q-1}{2}$, then $N_{12} = 1$, $N_{20} = 1$, and $N_{60} = (q - 31)/60$.*

Proof. We have $p = 5$ or $q \equiv \pm 1 \pmod{10}$. We note that U has a subgroup isomorphic to A_4 . Let $q \equiv 1 \pmod{4}$. For $p = 5$, we have $PSL(2, 5) \cong A_5$, and thus assertions (a) and (b) follow from Lemma 21. For the remaining subcases we distinguish the cases $3 \mid \frac{q+1}{2}$ or $3 \mid q$, and $5 \mid \frac{q+1}{2}$.

ad (c): By Lemma 23 (ii)(a), all orbit-lengths are multiples of 6 respectively 12. On the other hand, U has a fixed point free element of order 5, which means that all orbit-lengths are multiples of 5. Thus, we have $N_{30} = 1$ and all other orbits are regular.

ad (d): Again, by Lemma 23 (ii)(a), all orbit-lengths are multiples of 6 respectively 12. Furthermore, we cannot have an orbit of length 6 since otherwise we would have a one-point stabilizer of order 10, which is not possible for $p \neq 5$ as in A_5 all subgroups of order 10 are isomorphic to dihedral groups. On the other hand, U has an element of order 5 with two distinct fixed points which implies the existence of one orbit of size 12. Therefore, we have $N_{12} = 1$, $N_{30} = 1$, and all remaining orbits are regular.

ad (e): We deduce from Lemma 23 (ii)(b) that all orbit-lengths are multiples of 4, 6 respectively 12. On the other hand, U has a fixed point free element of order 5, which means that all orbit-lengths are multiples of 5. Hence, we conclude that $N_{20} = 1$, $N_{30} = 1$ and all other orbits are regular.

ad (f): By Lemma 23 (ii)(b) again, all orbit-lengths are multiples of 4, 6 respectively 12. We may conclude as in (d) that $N_6 = 0$. Furthermore, we cannot have an orbit of length 4 since otherwise we would have a one-point stabilizer of order 15, which is impossible as the non-Abelian simple group A_5 has proper subgroups only of index at least 5. On the other hand, U has an element of order 5 with two distinct fixed points which implies the existence of one orbit of size 12. Therefore, we have $N_{12} = 1$, $N_{20} = 1$, $N_{30} = 1$, and all remaining orbits are regular.

Let $3 \mid q$. Since the set of fixed points of some subgroup is left invariant by its normalizer, clearly the normalizer $\mathcal{N}_U(P)$ of a Sylow 3-subgroup P in U has then exactly one fixed point. As we have 10 Sylow 3-subgroups in U contained in one conjugacy class, we conclude that $|\mathcal{N}_U(P)| = 6$. Since $\mathcal{N}_U(P)$ is a maximal subgroup in U , it follows therefore that we have one orbit of length 10. If $5 \mid \frac{q+1}{2}$, then U has a fixed point free element of order 5, and hence it follows that all other orbits are regular. If $5 \mid \frac{q-1}{2}$, then U has an element of order 5 with two distinct fixed points which implies the existence of one orbit of size 12 since $N_6 = 0$ as in (d), and all remaining orbits are regular.

For $q \equiv 3 \pmod{4}$, clearly $p = 5$ is not possible, and hence it follows that $3 \nmid q$ and $5 \mid \frac{q\pm 1}{2}$. Since a subgroup of U which is isomorphic to A_4 cannot have orbits of length 6 due to Lemma 23 (ii), we may proceed, mutatis mutandis, as in subcases (c)-(f) above. \square

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

Case (1): $N = A_v$, $v \geq 5$.

As trivial Steiner 4-designs are excluded, we may assume that $v \geq 6$. But then A_v , and hence also G , is 4-transitive and does not act on any non-trivial Steiner 4-design \mathcal{D} in view of [35, Thm. 3].

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

We distinguish two subcases:

Case (2a): $N = PSL(2, q)$, $v = q + 1$, $q = p^e > 3$.

Without restriction, we have $q \geq 5$ as $PSL(2, 4) \cong PSL(2, 5)$. Here $\text{Aut}(N) = P\Gamma L(2, q)$, and $|G| = (q + 1)q^{\frac{(q-1)}{n}}a$ with $n = (2, q - 1)$ and $a \mid ne$. We will show by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} . In the following, we may assume that $k > 4$ as trivial Steiner 4-designs are excluded.

We will first assume that $N = G$. Then, by Remark 12, we obtain

$$(q - 2) |PSL(2, q)_{0B}| \cdot n = (k - 1)(k - 2)(k - 3) \quad (5.1)$$

which is equivalent to

$$(q - 2) |PSL(2, q)_{0B}| \cdot n + 6 = k(k^2 - 6k + 11). \quad (5.2)$$

Thus, we have in particular

$$k \mid (q - 2) |PSL(2, q)_{0B}| \cdot n + 6. \quad (5.3)$$

Since $PSL(2, q)_B$ acts transitively on the points of B , we have

$$k = |0^{PSL(2, q)_B}| = [PSL(2, q)_B : PSL(2, q)_{0B}]. \quad (5.4)$$

Let us first consider the case when $|PSL(2, q)_{0B}| = 1$. If q is even, then $k \mid q + 4$ by property (5.3). On the other hand, using equation (5.4), we have $k = |PSL(2, q)_B| \mid |PSL(2, q)| = q^3 - q$. But, it can easily be seen that

$$(q^3 - q, q + 4) = (60, q + 4) = 4 \cdot (15, 2^{e-2} + 1) = \begin{cases} 4, & \text{if } e \text{ is even and } 4 \nmid e \\ 4 \cdot 3, & \text{if } e \text{ is odd} \\ 4 \cdot 5, & \text{if } 4 \mid e \end{cases}$$

and the possible values for $k > 4$ can immediately be ruled out by hand using equation (5.1). If q is odd, we have $k = |PSL(2, q)_B| \mid 2(q + 1)$ due to property (5.3) and equation (5.4). Examining the list of subgroups of $PSL(2, q)$ (cf. [22, Ch. 12, p. 285f.] or [34, Ch. II, Thm. 8.27]), we have to consider the following possibilities:

- (i) $PSL(2, q)_B$ is conjugate to a cyclic subgroup of order c with $c \mid \frac{q+1}{2}$ of $PSL(2, q)$, and $k = c$.
- (ii) $PSL(2, q)_B$ is conjugate to a dihedral subgroup of order $2c$ with $c \mid \frac{q+1}{2}$ of $PSL(2, q)$, and $k = 2c$.
- (iii) $PSL(2, q)_B$ is conjugate to A_4 , and $k = 12$.
- (iv) $PSL(2, q)_B$ is conjugate to S_4 , and $k = 24$.
- (v) $PSL(2, q)_B$ is conjugate to A_5 , and $k = 60$.

ad (i): By equation (5.1), we have

$$c \mid \frac{q+1}{2} = \frac{(c-1)(c-2)(c-3) + 6}{4} = \frac{c(c^2 - 6c + 11)}{4}.$$

But, on the other hand, for c even obviously $c(c-6) + 11 \equiv 1 \pmod{2}$ and for c odd it is easy to see that $c(c-6) \equiv 3 \pmod{4}$. Thus, in both cases $c^2 - 6c + 11$ is not divisible by 4, a contradiction.

ad (ii): Using equation (5.1), we obtain

$$c \mid \frac{q+1}{2} = \frac{(2c-1)(c-1)(2c-3) + 3}{2}.$$

But, as $(2c-1)(c-1)(2c-3) + 3 = 4c^3 - 12c^2 + 11c \equiv c \pmod{2c}$, this is impossible.

ad (iii)-(v): For each given value of k , we deduce from equation (5.1) that in each subcase q is not a prime power, a contradiction.

We consider now the case when $|PSL(2, q)_{0B}| = 2$. If q is even, then we have $k = \frac{|PSL(2, q)_B|}{2} \mid 2(q+1)$ due to property (5.3) and equation (5.4). Considering the list of subgroups of $PSL(2, q)$, we have the following possibilities:

- (i) $PSL(2, q)_B$ is conjugate to a cyclic subgroup of order c with $c \mid q+1$ of $PSL(2, q)$, and $k = \frac{c}{2}$.
- (ii) $PSL(2, q)_B$ is conjugate to a dihedral subgroup of order $2c$ with $c \mid q+1$ of $PSL(2, q)$, and $k = c$.
- (iii) $PSL(2, q)_B$ is conjugate to $PSL(2, \bar{q})$ with $\bar{q} \mid 4$, and $k = 30$.
- (iv) $PSL(2, q)_B$ is conjugate to A_4 , and $k = 6$.

ad (i), (iii), (iv): In view of Lemmas 17, 22, respectively 23 (iii), clearly k cannot take the given values.

ad (ii): Considering equation (5.1), we obtain a contradiction as for $k = c > 4$ clearly the right hand side of the equation is divisible by 8, but not the left hand side.

If q is odd, then $k \mid 2(2q-1)$ by property (5.3). On the other hand, using equation (5.4), we have $k = \frac{|PSL(2, q)_B|}{2} \mid \frac{|PSL(2, q)|}{2} = \frac{q^3-q}{4}$. But, for q odd, it can easily be seen that $(\frac{q^3-q}{4}, 2(2q-1)) = 2 \cdot (\frac{q^3-q}{8}, 2q-1) = 2 \cdot (3, q+1)$, and thus only $k = 6$ can occur. It follows from equation (5.1) that then $q = 17$ must hold. However, as it is known there does not exist any 4-(18, 6, 1) design (cf. [51, Thm. 6]).

Finally, let us consider the case when $|PSL(2, q)_{0B}| > 2$. Examining the list of subgroups of $PSL(2, q)$ with their orbits on the projective line (Lemmas 17-25), we have to consider the following subcases:

- (i) $PSL(2, q)_B$ is conjugate to S_4 , and $k = 6$ or 8.
- (ii) $PSL(2, q)_B$ is conjugate to A_5 , and $k = 6, 10, 12$ or 20.

- (iii) $PSL(2, q)_B$ is conjugate to a semi-direct product of an elementary Abelian subgroup of order $\bar{q} \mid q$ with a cyclic subgroup of order c of $PSL(2, q)$ with $c \mid \bar{q} - 1$ and $c \mid q - 1$, and $k = \bar{q}$.
- (iv) $PSL(2, q)_B$ is conjugate to $PSL(2, \bar{q})$ with $\bar{q}^m = q$, $m \geq 1$, and $k = \bar{q} + 1$ or $\bar{q}(\bar{q} - 1)$ if m is even.
- (v) $PSL(2, q)_B$ is conjugate to $PGL(2, \bar{q})$ with $\bar{q}^m = q$, $m > 1$ even, and $k = \bar{q} + 1$ or $\bar{q}(\bar{q} - 1)$.

ad (i): We may assume that q is odd. Applying equations (5.1) and (5.4) yields for $k = 6$ that q is not a prime power, and for $k = 8$ that $q = 37$, in which case $q \equiv \pm 1 \pmod{8}$ (cf. Lemma 24) does not hold.

ad (ii): Again, we may assume that q is odd and consider equations (5.1) and (5.4) for the given values of k . We obtain for $k = 6$ that $q = 5$, which is clearly impossible due to Corollary 11, for $k = 10$ that q is not a prime power, and for $k = 20$ that $q = 971$, in which case Lemma 9 (c) gives a contradiction. If $k = 12$, then we get $q = 101$. Since $|PSL(2, q)_{0B}| = 5$ by equation (5.4), and $5 \mid \frac{q-1}{2}$ in this case, $PSL(2, q)_{0B}$ has two distinct fixed points. If one fixed point lies outside B , then clearly $q \equiv 1 \pmod{5}$ and hence $k = 12$ is not possible. Thus, we may assume that both fixed points are incident with B . But then, as every non-identity element of $PSL(2, q)$ fixes at most two distinct points, $PSL(2, q)_{0B}$ must fix some 2-subset by the definition of Steiner 4-designs, and hence contains an involution, a contradiction.

ad (iii): As it is easily seen, we have $((q - 2) |PSL(2, q)_{0B}| \cdot n + 6, q) = (2 \cdot |PSL(2, q)_{0B}| \cdot n - 6, q)$. Thus, we deduce from property (5.3) that in particular

$$k \mid 2 \cdot |PSL(2, q)_{0B}| \cdot n - 6. \quad (5.5)$$

On the other hand, it follows from equation (5.4) that $|PSL(2, q)_{0B}| \mid k - 1$. Therefore, we have in particular

$$\frac{k - 1}{2n} < \frac{k + 6}{2n} \leq |PSL(2, q)_{0B}| \mid k - 1. \quad (5.6)$$

If q is even, then we deduce that $|PSL(2, q)_{0B}| = k - 1$. Property (5.5) yields then $k \mid 2k - 8$, and, as clearly $(2k - 8, k) = (8, k)$, only $k = 8$ is possible. Thus, we have

$q = 32$ in view of equation (5.1). But now, Lemma 9 (c) gives a contradiction. If q is odd, then by property (5.6), we have to consider the possibilities when $|PSL(2, q)_{0B}| = \frac{k-1}{\bar{n}}$ with $\bar{n} = 1, 2, 3$. If $|PSL(2, q)_{0B}| = k - 1$, then we obtain $k \mid 4k - 10$ by property (5.3). Clearly, $(4k - 10, k) = (10, k)$, but as $k \mid q$, only $k = 5$ is possible. Then, equation (5.1) gives $q = 5$, which leads to a contradiction in view of Corollary 11. For $|PSL(2, q)_{0B}| = \frac{k-1}{2}$, we have $k \mid 2k - 8$ and thus $k = 8$ as above, which is impossible as $k \nmid q$. If $|PSL(2, q)_{0B}| = \frac{k-1}{3}$, then property (5.3) yields $k \mid \frac{4k-22}{3}$. But, as obviously $(4k - 22, 3k) = (22, 3k)$ is not divisible by 3, this is not possible.

ad (iv)-(v): In subcase (iv), we have $|PSL(2, q)_{0B}| = \frac{\bar{q}(\bar{q}-1)}{n}$ if $k = \bar{q} + 1$. Thus, equation (5.1) yields for $k = \bar{q} + 1$ that $q = \bar{q}$ must hold, which is impossible due to Corollary 11. For $m > 1$ even and $k = \bar{q}(\bar{q}-1)$, it follows that $|PSL(2, q)_{0B}| = \frac{\bar{q}+1}{n}$. Hence, by property (5.3), we conclude that

$$\bar{q}(\bar{q} - 1) \mid (q - 2)(\bar{q} + 1) + 6 = \bar{q}^{m+1} + \bar{q}^m - 2\bar{q} + 4.$$

But, as clearly $(\bar{q}^{m+1} + \bar{q}^m - 2\bar{q} + 4, \bar{q}) = (4, \bar{q})$, and we may assume that $k > 4$, only the case when $\bar{q} = 4$ has to be considered. Thus, we have $k = 12$ and applying equation (5.2) immediately gives a contradiction. In subcase (v), clearly n does not appear in equations (5.1) and (5.2) as well as in property (5.3), and we may argue *mutatis mutandis* as in subcase (iv).

Now, let us assume that $N < G \leq \text{Aut}(N)$. We recall that $q = p^e > 3$, and will distinguish in the following the cases $p > 2$ and $p = 2$.

First, let $p > 2$. We define

$$G^* = G \cap (PSL(2, q) \rtimes \langle \tau_\alpha \rangle)$$

with $\tau_\alpha \in \text{Sym}(GF(p^e) \cup \{\infty\}) \cong S_v$ of order e induced by the Frobenius automorphism $\alpha : GF(p^e) \rightarrow GF(p^e)$, $x \mapsto x^p$. Then, by Dedekind's law, we can write

$$G^* = PSL(2, q) \rtimes (G^* \cap \langle \tau_\alpha \rangle). \quad (5.7)$$

Defining $P\Sigma L(2, q) = PSL(2, q) \rtimes \langle \tau_\alpha \rangle$, it can easily be calculated that $P\Sigma L(2, q)_{0,1,\infty} = \langle \tau_\alpha \rangle$, and $\langle \tau_\alpha \rangle$ has precisely $p + 1$ distinct fixed points (cf., e.g., [21, Ch. 6.4, Lemma 2]). As $p > 2$, we conclude therefore that $G^* \cap \langle \tau_\alpha \rangle \leq G_{0B}^*$

for some appropriate, unique block $B \in \mathcal{B}$ by the definition of Steiner 4-designs. Furthermore, clearly $PSL(2, q) \cap (G^* \cap \langle \tau_\alpha \rangle) = 1$. Hence, we have

$$\begin{aligned} |(0, B)^{G^*}| &= [G^* : G_{0B}^*] \\ &= [PSL(2, q) \rtimes (G^* \cap \langle \tau_\alpha \rangle) : PSL(2, q)_{0B} \rtimes (G^* \cap \langle \tau_\alpha \rangle)] \\ &= [PSL(2, q) : PSL(2, q)_{0B}] \\ &= |(0, B)^{PSL(2, q)}|. \end{aligned} \quad (5.8)$$

Thus, if we assume that $G^* \leq \text{Aut}(\mathcal{D})$ acts already flag-transitively on \mathcal{D} , then we obtain $|(0, B)^{G^*}| = |(0, B)^{PSL(2, q)}| = bk$ in view of Remark 12. Hence, $PSL(2, q)$ must also act flag-transitively on \mathcal{D} , and we may proceed as in the case when $N = G$. Therefore, let us assume that $G^* \leq \text{Aut}(\mathcal{D})$ does not act flag-transitively on \mathcal{D} . Then, we conclude that $[G : G^*] = 2$ and G^* has exactly two orbits of equal length on the set of flags. Thus, by equation (5.8), we obtain for the orbit containing the flag $(0, B)$ that $|(0, B)^{G^*}| = |(0, B)^{PSL(2, q)}| = \frac{bk}{2}$. As it is well-known the normalizer of $PSL(2, q)$ in $\text{Sym}(X)$ is $P\Gamma L(2, q)$, and hence in particular $PSL(2, q)$ is normal in G . It follows therefore that we have under $PSL(2, q)$ also precisely one further orbit of equal length on the set of flags. Then, proceeding similarly to the case $N = G$ for each orbit on the set of flags, we obtain (representative for the orbit containing the flag $(0, B)$) that

$$\frac{(q-2) |PSL(2, q)_{0B}| \cdot n}{2} = (k-1)(k-2)(k-3) \quad (5.9)$$

which is equivalent to

$$\frac{(q-2) |PSL(2, q)_{0B}| \cdot n}{2} + 6 = k(k^2 - 6k + 11). \quad (5.10)$$

Hence, we have in particular

$$k \mid \frac{(q-2) |PSL(2, q)_{0B}| \cdot n}{2} + 6. \quad (5.11)$$

Since $PSL(2, q)_B$ can have one or two orbits of equal length on the points of B , we have

$$k \text{ or } \frac{k}{2} = |0^{PSL(2, q)_B}| = [PSL(2, q)_B : PSL(2, q)_{0B}]. \quad (5.12)$$

We will first consider the case when $|PSL(2, q)_{0B}| = 1$. As q is odd, clearly $q-2$ is also odd, and we obtain a contradiction to equation (5.9). Let us now

consider the case when $|PSL(2, q)_{0B}| = 2$. For q odd, we have $k \mid 2(q+1)$ in view of property (5.11), and $k = |PSL(2, q)_B|$ or $\frac{|PSL(2, q)_B|}{2}$ by equation (5.12). For $k = |PSL(2, q)_B|$, clearly equation (5.9) with $|PSL(2, q)_{0B}| = 2$ is equivalent to equation (5.1) with $|PSL(2, q)_{0B}| = 1$, and thus we can argue exactly as in case $N = G$ for $|PSL(2, q)_{0B}| = 1$ and q odd. For $k = \frac{|PSL(2, q)_B|}{2}$, we have to consider the following subgroups of $PSL(2, q)$:

- (i) $PSL(2, q)_B$ is conjugate to a cyclic subgroup of order c with $c \mid \frac{q+1}{2}$ of $PSL(2, q)$, and $k = \frac{c}{2}$.
- (ii) $PSL(2, q)_B$ is conjugate to a dihedral subgroup of order $2c$ with $c \mid \frac{q+1}{2}$ of $PSL(2, q)$, and $k = c$.
- (iii) $PSL(2, q)_B$ is conjugate to A_4 , and $k = 6$.
- (iv) $PSL(2, q)_B$ is conjugate to S_4 , and $k = 12$.
- (v) $PSL(2, q)_B$ is conjugate to A_5 , and $k = 30$.

ad (i): Obviously, k cannot take the given value due to Lemma 17.

ad (ii): It follows from equation (5.9) that

$$c \mid \frac{q+1}{2} = \frac{(c-1)(c-2)(c-3)+6}{4} = \frac{c(c^2-6c+11)}{4}.$$

However, on the other hand, for c even obviously $c(c-6)+11 \equiv 1 \pmod{2}$, and for c odd it is easy to see that $c(c-6) \equiv 3 \pmod{4}$. Therefore, in both cases $c^2-6c+11$ is not divisible by 4, a contradiction.

ad (iii)-(v): In view of equation (5.9), we obtain in subcase (iii) that $q = 32$, which is not possible with regard to Lemma 23 (iii), and in each of the other subcases that q is not a prime power.

We consider finally the case when $|PSL(2, q)_{0B}| > 2$. Combining equations (5.9) and (5.12), we obtain

$$\frac{(q-2)|PSL(2, q)_B| \cdot n}{2} = k(k-1)(k-2)(k-3) \quad (5.13)$$

$$\text{with } k = |0^{PSL(2, q)_B}| = \frac{|PSL(2, q)_B|}{|PSL(2, q)_{0B}|}, \text{ or}$$

$$(q-2) |PSL(2, q)_B| \cdot n = k(k-1)(k-2)(k-3) \quad (5.14)$$

$$\text{with } k = 2 \cdot |0^{PSL(2, q)_B}| = 2 \cdot \frac{|PSL(2, q)_B|}{|PSL(2, q)_{0B}|}.$$

In view of the subgroups of $PSL(2, q)$ with their orbits on the projective line (Lemmas 17-25), we have the following possibilities:

- (i) $PSL(2, q)_B$ is conjugate to A_4 , and $k = 2 \cdot |0^{PSL(2, q)_B}| = 8$.
- (ii) $PSL(2, q)_B$ is conjugate to S_4 , and $k = |0^{PSL(2, q)_B}| = 6$ or 8 , respectively $k = 2 \cdot |0^{PSL(2, q)_B}| = 8, 12$ or 16 .
- (iii) $PSL(2, q)_B$ is conjugate to A_5 , and $k = |0^{PSL(2, q)_B}| = 6, 10, 12$ or 20 , respectively $k = 2 \cdot |0^{PSL(2, q)_B}| = 12, 20, 24$ or 40 .
- (iv) $PSL(2, q)_B$ is conjugate to a semi-direct product of an elementary Abelian subgroup of order $\bar{q} \mid q$ with a cyclic subgroup of order c of $PSL(2, q)$ with $c \mid \bar{q} - 1$ and $c \mid q - 1$, and $k = |0^{PSL(2, q)_B}| = \bar{q}$, respectively $k = 2 \cdot |0^{PSL(2, q)_B}| = 2\bar{q}$.
- (v) $PSL(2, q)_B$ is conjugate to $PSL(2, \bar{q})$ with $\bar{q}^m = q$, $m \geq 1$, and $k = |0^{PSL(2, q)_B}| = \bar{q} + 1$, or $\bar{q}(\bar{q} - 1)$ if m is even, respectively $k = 2 \cdot |0^{PSL(2, q)_B}| = 2(\bar{q} + 1)$, or $2\bar{q}(\bar{q} - 1)$ if m is even.
- (vi) $PSL(2, q)_B$ is conjugate to $PGL(2, \bar{q})$ with $\bar{q}^m = q$, $m > 1$ even, and $k = |0^{PSL(2, q)_B}| = \bar{q} + 1$ or $\bar{q}(\bar{q} - 1)$, respectively $k = 2 \cdot |0^{PSL(2, q)_B}| = 2(\bar{q} + 1)$ or $2\bar{q}(\bar{q} - 1)$.

ad (i): Considering equation (5.14), we immediately deduce for q odd that q is not a prime power.

ad (ii): First, applying equation (5.13) yields for $k = 6$ that $q = 17$, which can be excluded since there does not exist any 4-(18, 6, 1) design as already mentioned, and for $k = 8$ that q is not a prime power. Using equation (5.14) gives for $k = 8$ that $q = 37$, in which case $q \equiv \pm 1 \pmod{8}$ (cf. Lemma 24) does not hold, and for $k = 12$ and 16 that q is not a prime power in each case.

ad(iii): Considering first equation (5.13) yields for each given value of k that q is even, a contradiction. Now, applying equation (5.14) gives for $k = 12$ the

prime $q = 101$, which is impossible as according to Lemma 25 we only have orbits of length 6 when $p = 5$, and for $k = 20$ that $q = 971$, in which case Lemma 9 (c) gives a contradiction. For $k = 24$ and 40, we obtain in each case that q is not a prime power.

ad (iv): Let $k = \bar{q}$. As it is easily seen, we have $(\frac{(q-2)|PSL(2,q)_{0B}| \cdot n}{2} + 6, q) = (|PSL(2, q)_{0B}| \cdot n - 6, q)$, and hence deduce from property (5.11) that

$$k \mid |PSL(2, q)_{0B}| \cdot n - 6. \quad (5.15)$$

On the other hand, as $k = |0^{PSL(2,q)_B}| = [PSL(2, q)_B : PSL(2, q)_{0B}]$ in this case, it follows that $|PSL(2, q)_{0B}| = c \mid k - 1$. Thus, we obtain in particular

$$\frac{k-1}{n} < \frac{k+6}{n} \leq |PSL(2, q)_{0B}| \mid k-1,$$

and as q is odd, we conclude that $|PSL(2, q)_{0B}| = k - 1$. But, property (5.15) gives then $k \mid 2k - 8$, and, as clearly $(2k - 8, k) = (8, k)$, it would follow that $k = 8$, which is impossible for q odd. For $k = 2\bar{q}$, it follows from equation (5.14) that

$$(q-2)n = 4 \cdot \frac{(\bar{q}-1)}{c} (2\bar{q}-1)(2\bar{q}-3),$$

which gives a contradiction as clearly the left hand side of the equation is not divisible by 4 for q odd.

ad (v)-(vi): We first consider subcase (v). For $k = \bar{q} + 1$, it follows from equation (5.13) that $q = 2(\bar{q} - 1)$, which is obviously impossible for $\bar{q} > 2$. If $m > 1$ even and $k = \bar{q}(\bar{q} - 1)$, then we have

$$(q-2)(\bar{q}+1) = 2(\bar{q}^2 - \bar{q} - 1)(\bar{q}^2 - \bar{q} - 2)(\bar{q}^2 - \bar{q} - 3)$$

in view of equation (5.13). As clearly $(\bar{q}^2 - \bar{q} - 1, \bar{q} + 1) = 1$, it follows that $\bar{q}^2 - \bar{q} - 1 \mid q - 2$ must hold. But, polynomial division with remainder gives

$$q - 2 = \left(\sum_{i=1}^{m-1} n_i \frac{q}{\bar{q}^{i+1}} \right) (\bar{q}^2 - \bar{q} - 1) + n_m \bar{q} + n_{m-1} - 2, \quad (5.16)$$

where n_i denote the i -th Fibonacci number recursively defined via

$$n_1 = n_2 = 1, \quad n_i = n_{i-1} + n_{i-2} \quad (i \geq 3).$$

Hence, as clearly $n_m\bar{q} + n_{m-1} - 2 > 0$ for $m > 1$, we obtain a contradiction. If $k = 2(\bar{q} + 1)$, then applying equation (5.14) gives

$$(q - 2)(\bar{q} - 1) = 4(2\bar{q} + 1)(2\bar{q} - 1). \quad (5.17)$$

As clearly $(2\bar{q} - 1, \bar{q} - 1) = 1$, we deduce that $2\bar{q} - 1 \mid q - 2$ must hold. Since polynomial division with remainder yields

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

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

$$\deg\left(\frac{q}{(2\bar{q})^{\bar{m}}} - 2\right) < \deg(2\bar{q} - 1)$$

as is well-known), it follows therefore that \bar{q} , and hence also q , is necessarily a power of 2, a contradiction. For $m > 1$ even and $k = 2\bar{q}(\bar{q} - 1)$, equation (5.14) yields

$$(q - 2)(\bar{q} + 1) = 2(2\bar{q}^2 - 2\bar{q} - 1)2(\bar{q}^2 - \bar{q} - 1)(2\bar{q}^2 - 2\bar{q} - 3).$$

Again, as obviously $(\bar{q}^2 - \bar{q} - 1, \bar{q} + 1) = 1$, we deduce that $\bar{q}^2 - \bar{q} - 1 \mid q - 2$ must hold, and we may proceed exactly as above for $k = \bar{q}(\bar{q} - 1)$. In subcase (vi), clearly n does not appear in equations (5.13) and (5.14), and we may argue *mutatis mutandis* as in subcase (v).

Now, let $p = 2$. Then, clearly $N = PSL(2, q) = PGL(2, q)$, and we have $\text{Aut}(N) = P\Sigma L(2, q)$. If we assume that $\langle \tau_\alpha \rangle \leq P\Sigma L(2, q)_{0B}$ for some appropriate, unique block $B \in \mathcal{B}$, then, using the terminology of (5.7), we have $G^* = G = P\Sigma L(2, q)$ and as clearly $PSL(2, q) \cap \langle \tau_\alpha \rangle = 1$, we can apply equation (5.8). Thus, $PSL(2, q)$ must also be flag-transitive, which has already been considered. Therefore, we may assume that $\langle \tau_\alpha \rangle \not\leq P\Sigma L(2, q)_{0B}$. Let s be a prime divisor of $e = |\langle \tau_\alpha \rangle|$. As the normal subgroup $H := (P\Sigma L(2, q)_{0,1,\infty})^s \leq \langle \tau_\alpha \rangle$ of index s fixes at least four distinct points, we have $G \cap H \leq G_{0B}$ for some appropriate, unique block $B \in \mathcal{B}$ by the definition of Steiner 4-designs. It can then be deduced that $e = s^u$ for some $u \in \mathbb{N}$, since if we assume for $G = P\Sigma L(2, q)$ that there exists a further prime divisor \bar{s} of e with $\bar{s} \neq s$, then $\bar{H} := (P\Sigma L(2, q)_{0,1,\infty})^{\bar{s}} \leq \langle \tau_\alpha \rangle$ and H are both subgroups of $P\Sigma L(2, q)_{0B}$ by the flag-transitivity of $P\Sigma L(2, q)$, and

hence $\langle \tau_\alpha \rangle \leq P\Sigma L(2, q)_{0B}$, a contradiction. Furthermore, as $\langle \tau_\alpha \rangle \not\leq P\Sigma L(2, q)_{0B}$, we may, by applying Dedekind's law, assume that

$$G_{0B} = PSL(2, q)_{0B} \rtimes (G \cap H).$$

Thus, by Remark 12, we obtain

$$(q-2) |PSL(2, q)_{0B}| |G \cap H| = (k-1)(k-2)(k-3) |G \cap \langle \tau_\alpha \rangle|.$$

Using that $k = |0^{G_B}| = [G_B : G_{0B}]$, we have more precisely

(A) if $G = PSL(2, q) \rtimes (G \cap H)$:

$$(q-2) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k}, \text{ or}$$

(B) if $G = P\Sigma L(2, q)$:

$$(q-2) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k} \cdot \begin{cases} s, & \text{if } G_B = PSL(2, q)_B \rtimes \langle \tau_\alpha \rangle \\ 1, & \text{if } G_B = PSL(2, q)_B \rtimes H. \end{cases}$$

As far as condition (A) is concerned, we may argue exactly as in the earlier case $N = G$ for q even. Thus, only condition (B) has to be examined, and we will also show that here $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} . Clearly, for each $B \in \mathcal{B}$, there exists always a Klein four-group $V_4 \leq PSL(2, q)$, which fixes B by the definition of Steiner 4-designs, and some additional point $x \in X$. We will distinguish two cases according as x is incident with B or not and examine for each case the list of possible subgroups of $PSL(2, q)$ with their orbits on the projective line (cf. Lemmas 17-25). Let $x \in B$. Then, clearly $k \equiv 1 \pmod{4}$. It follows that we only have to consider the subcase when $PSL(2, q)_B$ is conjugate to $PSL(2, \bar{q})$ with $\bar{q}^m = q$, $m \geq 1$. In view of Lemma 21, we conclude then that $k = \bar{q} + 1$. By condition (B), we have hence

$$(q-2) |PSL(2, q)_{0B}| = \bar{q}(\bar{q}-1)(\bar{q}-2)s \quad (5.18)$$

$$\text{with } |PSL(2, q)_{0B}| = \bar{q}(\bar{q} - 1) \cdot \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

Since $q = 2^{s^u}$, we can write $\bar{q} = 2^{s^w}$ for some integer $0 \leq w \leq u$, and $q = \bar{q}^m = \bar{q}^{s^{u-w}}$. As we may assume that $k = \bar{q} + 1 = 2^{s^w} + 1 > 4$, it follows in particular that $w \geq 1$, and hence $s < 2^{s^w} = \bar{q}$. Thus, using equation (5.18), we obtain

$$\bar{q}^{s^{u-w}} - 2 = q - 2 \leq (\bar{q} - 2)s < \bar{q}^2 - 2s.$$

But, as clearly $u - w \geq 1$ (otherwise, $k = q + 1$, a contradiction to Corollary 11), this yields a contradiction for every prime s .

Now, let $x \notin B$. Then, clearly $k \equiv 0 \pmod{4}$. We may restrict ourselves to the examination of the following subcases:

- (i) $PSL(2, q)_B$ is conjugate to A_4 for $s = 2$, and $k = 12$ in view of Lemma 23.
- (ii) $PSL(2, q)_B$ is conjugate to an elementary Abelian subgroup of order $\bar{q} \mid q$ of $PSL(2, q)$, and $k = \bar{q}$ due to Lemma 19.
- (iii) $PSL(2, q)_B$ is conjugate to a semi-direct product of an elementary Abelian subgroup of order $\bar{q} \mid q$ with a cyclic subgroup of order c of $PSL(2, q)$ with $c \mid \bar{q} - 1$ and $c \mid q - 1$, and $k = \bar{q}$ or $\bar{q}c$ by Lemma 20.
- (iv) $PSL(2, q)_B$ is conjugate to $PSL(2, \bar{q})$ with $\bar{q}^m = q$, $m \geq 1$, acting outside the $\bar{q} + 1$ points mentioned in the case where x has been incident with B , and Lemma 21 yields $k = \bar{q}(\bar{q} - 1)$ if m is even, or $k = (\bar{q} + 1)\bar{q}(\bar{q} - 1)$.

Again, we can write in the following $\bar{q} = 2^{s^w}$ for some integer $0 \leq w \leq u$, and $q = \bar{q}^m = \bar{q}^{s^{u-w}}$.

ad (i): Applying condition (B) yields

$$(q - 2) |PSL(2, q)_{0B}| = 11 \cdot 10 \cdot 9 \cdot 2$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} 2, \text{ or} \\ 1 \end{cases},$$

which is clearly impossible.

ad (iii): Let $k = \bar{q}$. By condition (B), we have

$$(q - 2) |PSL(2, q)_{0B}| = (\bar{q} - 1)(\bar{q} - 2)(\bar{q} - 3)s \tag{5.19}$$

$$\text{with } |PSL(2, q)_{0B}| = c \cdot \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

As we may assume that $k = \bar{q} = 2^{s^w} > 4$, we have in particular $w \geq 1$, and hence $s < 2^{s^w} = \bar{q}$. Thus, using equation (5.19), we obtain

$$q - 2 = \bar{q}^{s^{u-w}} - 2 < \bar{q}^3 s < \bar{q}^4.$$

But, as clearly $u - w \geq 1$ (otherwise, $k = q$, a contradiction to Corollary 11), this yields a contradiction for $s \geq 5$. If $s = 2$, then $\bar{q}^{2^{u-w}} - 2 < 2\bar{q}^3$ must hold, which cannot be true for $u - w > 1$. For $s = 3$, we may also assume that $u - w = 1$ since otherwise, we would have $q = \bar{q}^{3^{u-w}} \geq \bar{q}^9$, again a contradiction to the inequality above. As $c \mid \bar{q} - 1$, it follows for both cases from equation (5.19) that

$$\bar{q} - 2 \mid q - 2,$$

and hence

$$2^{s^w-1} - 1 \mid 2^{s^u-1} - 1.$$

Thus, clearly

$$s^w - 1 \mid s^u - 1$$

and

$$w \mid u.$$

Therefore, we may conclude that $w = 1$ and $u = 2$. But then, for $s = 2$, it follows that $k = \bar{q} = 4$, which has been excluded. If $s = 3$, then we have $\bar{q} = 8$ and $q = 512$, and equation (5.19) yields

$$510 \cdot |PSL(2, q)_{0B}| = 7 \cdot 6 \cdot 5 \cdot 3$$

$$\text{with } |PSL(2, q)_{0B}| = c \cdot \begin{cases} 3, \text{ or} \\ 1 \end{cases},$$

which is clearly impossible.

Now, let $k = \bar{q}c$. Then, condition (B) yields

$$(q - 2) |PSL(2, q)_{0B}| = (\bar{q}c - 1)(\bar{q}c - 2)(\bar{q}c - 3)s \quad (5.20)$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

But, polynomial division with remainder gives

$$2^{s^u-1} - 1 = \left(\sum_{i=1}^{\bar{m}} \frac{2^{s^u-1}}{(c \cdot 2^{s^w-1})^i} \right) (c \cdot 2^{s^w-1} - 1) + \frac{2^{s^u-1}}{(c \cdot 2^{s^w-1})^{\bar{m}}} - 1$$

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

$$\deg\left(\frac{2^{s^u-1}}{(c \cdot 2^{s^w-1})^{\bar{m}}} - 1\right) < \deg\left(c \cdot 2^{s^w-1} - 1\right)$$

as is well-known). As c is odd, clearly $\left(\frac{2^{s^u-1}}{c \cdot 2^{s^w-1}}\right)^{\bar{m}} \neq 1$, and it follows that $\bar{q}c - 2$ does not divide $q - 2$, yielding a contradiction to equation (5.20).

ad (ii): Let $k = \bar{q}$. By condition (B), we have

$$(q-2) |PSL(2, q)_{0B}| = (\bar{q}-1)(\bar{q}-2)(\bar{q}-3)s$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} s, & \text{or} \\ 1. \end{cases}$$

As it is easily seen, we may argue, *mutatis mutandis*, as in subcase (iii), $k = \bar{q}$.

ad (iv): If $m > 1$ even and $k = \bar{q}(\bar{q}-1)$, then, in view of condition (B), we have

$$(q-2) |PSL(2, q)_{0B}| = (\bar{q}^2 - \bar{q} - 1)(\bar{q}^2 - \bar{q} - 2)(\bar{q}^2 - \bar{q} - 3)s$$

$$\text{with } |PSL(2, q)_{0B}| = (\bar{q}+1) \cdot \begin{cases} s, & \text{or} \\ 1. \end{cases}$$

As obviously $(\bar{q}^2 - \bar{q} - 1, \bar{q} + 1) = 1$, it follows that $\bar{q}^2 - \bar{q} - 1 \mid q - 2$ must hold, which is impossible as we have already seen via polynomial division (5.16) with remainder. For $k = \bar{q}^3 - \bar{q}$, condition (B) yields

$$(q-2) |PSL(2, q)_{0B}| = (\bar{q}^3 - \bar{q} - 1)(\bar{q}^3 - \bar{q} - 2)(\bar{q}^3 - \bar{q} - 3)s \quad (5.21)$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} s, & \text{or} \\ 1. \end{cases}$$

We already know that $k = (\bar{q}+1)\bar{q}(\bar{q}-1) \equiv 0 \pmod{4}$, and thus $\bar{q} > 2$. If $|PSL(2, q)_{0B}| = s$, then

$$q = (\bar{q}^3 - \bar{q} - 1)(\bar{q}^3 - \bar{q} - 2)(\bar{q}^3 - \bar{q} - 3) + 2 = \bar{q}^9 - l$$

$$\text{with } l = 3\bar{q}^7 + 6\bar{q}^6 - 3\bar{q}^5 - 12\bar{q}^4 - 10\bar{q}^3 + 6\bar{q}^2 + 11\bar{q} + 4.$$

As clearly $l > 0$, we have $q < \bar{q}^9$. But, on the other hand, for $\bar{q} > 2$ certainly $l < \bar{q}^8(\bar{q} - 1)$ and hence $q > \bar{q}^8$ must hold, a contradiction to the fact that $q = \bar{q}^m$ for some $m \geq 1$. If $|PSL(2, q)_{0B}| = 1$, then equation (5.21) yields

$$\begin{aligned} q &= ls + 2 \text{ with } l = (\bar{q}^3 - \bar{q} - 1)(\bar{q}^3 - \bar{q} - 2)(\bar{q}^3 - \bar{q} - 3) \\ &= \bar{q}^9 - 3\bar{q}^7 - 6\bar{q}^6 + 3\bar{q}^5 + 12\bar{q}^4 + 10\bar{q}^3 - 6\bar{q}^2 - 11\bar{q} - 6. \end{aligned}$$

Since $\bar{q} = 2^{s^w} > 2$, we conclude that $w \geq 1$ and $s < 2^{s^w} = \bar{q}$. As obviously $l < \bar{q}^9 - 1$, it follows therefore that $q < (\bar{q}^9 - 1)\bar{q} + 2 < \bar{q}^{10}$. On the other hand, for $\bar{q} > 2$ clearly $q = ls + 2 \geq 2(l + 1) > \bar{q}^9$ must hold, the same contradiction.

Case (2b): $N = PSL(d, q)$, $d \geq 3$.

We have here $\text{Aut}(N) = P\Gamma L(d, q) \rtimes \langle \iota_\beta \rangle$, where ι_β denotes the graph automorphism induced by the inverse-transpose map $\beta : GL(d, q) \longrightarrow GL(d, q)$, $x \mapsto {}^t(x^{-1})$. We will prove by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act on any non-trivial Steiner 4-design \mathcal{D} . In the following, let $n = (d, q - 1)$, and we may assume that $k > 4$ as trivial Steiner 4-designs are excluded.

Let us first assume that $d = 3$. We have to show that G with $PSL(3, q)$ as simple normal subgroup cannot act on any non-trivial 4 - $(q^2 + q + 1, k, 1)$ design. First, we will prove that $k \leq q + 1$ as an upper bound for the block size k must hold. It is well-known that, for any line \mathcal{G} in the underlying projective plane $PG(2, q)$, the translation group $T(\mathcal{G})$ operates regularly on the points of $PG(2, q) \setminus \mathcal{G}$ and acts trivially on \mathcal{G} . Thus, $T(\mathcal{G})$ fixes a block $B \in \mathcal{B}$ if four or more distinct points of B lie on \mathcal{G} . By the definition of Steiner 4-designs, we may choose in $PG(2, q)$ four distinct collinear points $x_1, x_2, x_3, x_4 \in X$, which are incident with a unique block $B \in \mathcal{B}$. Let \mathcal{G} denote the line of $PG(2, q)$ through $x_1, x_2, x_3, x_4 \in X$. Consequently, if the block B contains at least one further point of $PG(2, q) \setminus \mathcal{G}$, then it must contain all points of $PG(2, q) \setminus \mathcal{G}$, thus at least $q^2 + 4$ many. But, these are obviously more than half of the points of $PG(2, q)$, a contradiction to $k \leq \lfloor \frac{q}{5} + 3 \rfloor$ by Proposition 10 (a). Therefore, B is completely contained in \mathcal{G} , and hence we have $k \leq q + 1$. As clearly the block size k is constant for all blocks, the claims follows.

Now, by the definition of Steiner 4-designs, we may consider a 4-subset consisting of three distinct collinear points $x_1, x_2, x_3 \in X$ and one non-collinear point

$x_4 \in X$, which is incident with a unique block $B \in \mathcal{B}$. If B contains a fourth point on the line \mathcal{G} of $PG(2, q)$ through $x_1, x_2, x_3 \in X$, then, by the same arguments as above using the translation group $T(\mathcal{G})$, we conclude that B lies completely in \mathcal{G} , which is clearly impossible in this case. Thus, we may assume that B contains only further points which are not on \mathcal{G} . Without restriction, we may identify $x_1 = \langle(1, 0, 0)\rangle$, $x_2 = \langle(0, 0, 1)\rangle$, $x_3 \in \langle x_1, x_2 \rangle$, and $x_4 = \langle(0, 1, 0)\rangle$. As it is known the cyclic group

$$\left\{ \left(\begin{array}{ccc} c & & \\ & c^{-2} & \\ & & c \end{array} \right) \mid c \in GF(q)^* \right\}$$

of linear transformations on the associated vector space $V = V(3, q)$ induces a group U of dilatations of order $\frac{q-1}{n}$ on $PG(2, q)$ with axis the line $\mathcal{G} = \langle x_1, x_2 \rangle$ and as center the point x_4 . It is clear that U fixes each point of its axis as well as its center. Furthermore, U acts semi-regularly on the points of $PG(2, q) \setminus (\mathcal{G} \cup \{x_4\})$, and hence all point-orbits on $PG(2, q) \setminus (\mathcal{G} \cup \{x_4\})$ have length $\frac{q-1}{n}$. Thus, as U fixes each of the points $x_1, x_2, x_3, x_4 \in X$, and hence in particular B , we get

$$k \equiv 4 \pmod{\frac{q-1}{n}}.$$

Due to the fact that $k \leq q + 1$, this is obviously impossible if $3 \nmid q - 1$, and for $3 \mid q - 1$, we conclude that

$$k = \frac{q-1}{3} + 4 \text{ or } k = 2 \cdot \frac{q-1}{3} + 4. \quad (5.22)$$

If we assume that $q > 7$, then indeed $q \geq 13$, and hence we obtain $\frac{q-1}{3} \geq 4$, which means that we have at least four distinct collinear points on some line \mathcal{H} of $PG(2, q)$, and we may argue as above using the translation group $T(\mathcal{H})$ that then B lies completely in \mathcal{H} , which is obviously impossible. Therefore, we only have to consider the cases when $q = 4$ or 7 . For $q = 7$, condition (5.22) yields $k = 6$ or 8 , whereas $k = 6$ can immediately be ruled out using Lemma 9 (c). If any 4 -(57, 8, 1) design exists, then there must also exist a derived 3 -(56, 7, 1) design. But, for $t = 3$, it follows from Lemma 9 (c) that then in particular 54 must be divisible by 5, a contradiction. Now, let us assume that $q = 4$. Since we have $4 < k \leq q + 1$, only $k = 5$ may occur. We have then the situation of two intersecting lines \mathcal{G} and \mathcal{H} , and we will distinguish the two cases according as their intersecting point $x \in \mathcal{G} \cap \mathcal{H}$ is incident with B or not. Let us consider the

first case. Then, \mathcal{G} and \mathcal{H} are precisely the lines which intersects B in exactly three distinct points. We will show that the order of $PSL(3,4)_B$ is at most 8. Let B be fixed under $PSL(3,4)$. Then, the set consisting of the lines \mathcal{G} and \mathcal{H} is also fixed. Hence, $PSL(3,4)_B$ has a normal subgroup U of index at most 2 which fixes both lines. Then, U also fixes their intersecting point x and the remaining 2-subset of B on each line. Thus, U has a normal subgroup U_1 of index at most 2 which fixes pointwise any of the two 2-subsets and furthermore, U_1 has a normal subgroup U_2 of index at most 2 which fixes pointwise both 2-subsets. But, since in $PSL(3,q)$ only the identity fixes pointwise some non-degenerate quadrangle, we conclude that $|PSL(3,4)_B| \leq 8$.

Now, let us suppose that the intersecting point x does not belong to B . Hence, we have exactly one line, namely \mathcal{G} , which intersects B in exactly three distinct points. We will show that the order of $PSL(3,4)_B$ is at most 12. Let B be fixed under $PSL(3,4)$. Then, the lines \mathcal{G} and \mathcal{H} are also fixed, and $PSL(3,4)_B$ has a normal subgroup U of index at most 2 which fixes pointwise the 2-subset consisting of the points of B which are on \mathcal{H} . Again by the argument that in $PSL(3,q)$ only the identity fixes pointwise some non-degenerate quadrangle, U operates faithful on the 3-subset consisting of the points of B which are on \mathcal{G} . Hence, U has a normal subgroup U_1 of index at most $|S_3| = 6$. Therefore, we have $|PSL(3,4)_B| \leq 12$. (Indeed, it can be shown that even $|PSL(3,4)_B| \leq 2$ in this case.)

Since there are as blocks 21 projective lines in $PG(2,4)$, it follows that $[PSL(3,4) : PSL(3,4)_B] \leq b - 21$, and hence

$$|PSL(3,4)_B| \geq \frac{|PSL(3,4)|}{b - 21} = \frac{20160}{1176} > 17,$$

yielding a contradiction in both cases. Thus $PSL(3,q)$, and hence also G with $PSL(3,q)$ as simple normal subgroup, cannot act on any non-trivial $4-(q^2 + q + 1, k, 1)$ 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 4-design \mathcal{D} . For this, let us assume that there is a counter-example with d minimal. Without restriction, we can choose four distinct points x_1, x_2, x_3, x_4 from a hyperplane \mathcal{H} of $PG(d-1, q)$. First, we show that the unique block $B \in \mathcal{B}$ which is incident with the 4-subset

$\{x_1, x_2, x_3, x_4\}$ is contained completely in \mathcal{H} . Analogously as above, the translation group $T(\mathcal{H})$ acts regularly on the points of $PG(d-1, q) \setminus \mathcal{H}$, but trivially on \mathcal{H} . If B contains at least one point outside \mathcal{H} , then it would already contain all points of $PG(d-1, q) \setminus \mathcal{H}$, thus at least $q^{d-1} + 4$ many. However, as

$$v = \frac{q^d - 1}{q - 1} < 2q^{d-1} \iff q^d - 1 < 2(q^d - q^{d-1}) \iff 2q^{d-1} - 1 < q^d,$$

these are more than half of the points of $PG(d-1, q)$, the same contradiction as above. Thus, \mathcal{H} induces a $4\text{-}\left(\frac{q^{d-1}-1}{q-1}, k, 1\right)$ design, on which G containing $PSL(d-1, q)$ as simple normal subgroup operates. Inductively, we obtain the minimal counter-example for $d = 3$. But, as we have shown above, G with $PSL(3, q)$ as simple normal subgroup cannot act on any non-trivial $4\text{-}\left(q^2 + q + 1, k, 1\right)$ design, and the assertion follows.

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

Here $\text{Aut}(N) = P\Gamma U(3, q^2)$, and $|G| = (q^3 + 1)q^3 \frac{(q^2-1)}{n} a$ with $n = (3, q + 1)$ and $a \mid 2ne$. For the existence of flag-transitive Steiner 4-designs, necessarily

$$r = \frac{q^3(q^3 - 1)(q^3 - 2)}{(k - 1)(k - 2)(k - 3)} \mid |G_0| \mid |P\Gamma U(3, q^2)_0| = q^3(q^2 - 1)2e$$

must hold in view of Lemma 8. As obviously $(q^2 + q + 1, q + 1) = 1$ and $(q^3 - 2, q + 1) = (3, q + 1) = n$, we have in particular

$$(q^3 - 2)(q^2 + q + 1) \mid (k - 1)(k - 2)(k - 3)2ne, \text{ where } e \leq \log_2 q. \quad (5.23)$$

But, on the other hand, Corollary 11 yields $k \leq \lfloor \sqrt{q^3 + 1} + \frac{5}{2} \rfloor < q^{\frac{3}{2}} + 3$. Hence, using property (5.23), we have only a small number of possibilities to check, which can easily be eliminated by hand. Therefore, we have shown that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} .

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

We have $\text{Aut}(N) = Sz(q) \rtimes \langle \alpha \rangle$, where α 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 $a \mid 2e + 1$. From Remark 12, we hence obtain

$$(q^2 - 2)(q + 1) = (k - 1)(k - 2)(k - 3) \frac{a}{|G_{xB}|} \text{ if } x \in B.$$

We will prove by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} .

First, we show that every element $g \in G$ that fixes three distinct points must fix at least five distinct points. Let us assume that $g \in G$ with $|\text{Fix}_X(g)| \geq 3$. Let $x \in \text{Fix}_X(g)$, and P the normal Sylow 2-subgroup of $Sz(q)_x$ acting regularly on $X \setminus \{x\}$. Furthermore, let $\mathcal{C}_P(g)$ denote the centralizer of g in P , where clearly $\mathcal{C}_P(g) = P \cap \mathcal{C}_{Sz(q)}(g)$. If $y, z \in \text{Fix}_X(g) \setminus \{x\}$, then $z = y^h$ with $h \in P$. Thus, as $y^{hg} = y^h = y^{gh}$, we conclude that

$$[h^{-1}, g^{-1}] \in G_{xy} \cap [P, G_x] \leq P_y = 1.$$

Then $h \in \mathcal{C}_P(g)$, and hence $\mathcal{C}_P(g)$ acts point-transitively on $\text{Fix}_X(g) \setminus \{x\}$. Therefore, as $|\text{Fix}_X(g)| \geq 3$, it follows that $|\text{Fix}_X(g)| \equiv 1 \pmod{2}$. Clearly, the set $\text{Fix}_X(g)$ is left invariant by $\mathcal{C}_{Sz(q)}(g)$ and $\mathcal{C}_{Sz(q)}(g)$ operates on $\text{Fix}_X(g)$. Since $x \in \text{Fix}_X(g)$ can be chosen arbitrarily, it follows that $\mathcal{C}_{Sz(q)}(g)$ operates point-transitively on $\text{Fix}_X(g)$, and thus $|\text{Fix}_X(g)| \mid |Sz(q)|$. As the order of $Sz(q)$ is not divisible by 3, clearly $|\text{Fix}_X(g)| \neq 3$, and due to the fact that $|\text{Fix}_X(g)| \equiv 1 \pmod{2}$, we have $|\text{Fix}_X(g)| \geq 5$.

Since G is block-transitive, it is sufficient to consider some appropriate, unique block $B \in \mathcal{B}$. As clearly $\langle \alpha \rangle \leq \text{Aut}(N)_{0,1,\infty}$, it follows from above that $\langle \alpha \rangle$ must fix some fourth point, and hence $G \cap \langle \alpha \rangle \leq G_{0B}$ by the definition of Steiner 4-designs. Thus, we have particularly

$$(q^2 - 2)(q + 1) \leq (k - 1)(k - 2)(k - 3),$$

which does obviously not hold for $k \leq q + 2$. But, on the other hand, Corollary 11 yields $k \leq \lfloor \sqrt{q^2 + 1} + \frac{5}{2} \rfloor < q + 3$, a contradiction.

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 α 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 $a \mid 2e + 1$. It follows from Remark 12 that

$$(q^3 - 2)(q^2 + q + 1) = (k - 1)(k - 2)(k - 3) \frac{a}{|G_{xB}|} \text{ if } x \in B.$$

We will also show by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} .

First, we show that every element $g \in G$ that fixes three distinct points must also fix a fourth point. Let us assume that $g \in G$ with $|\text{Fix}_X(g)| \geq 3$. Let $x \in \text{Fix}_X(g)$, and P the normal Sylow 3-subgroup of $\text{Re}(g)_x$ acting regularly on $X \setminus \{x\}$. As in Case (4), it can be shown that then $\mathcal{C}_P(g)$ acts point-transitively on $\text{Fix}_X(g) \setminus \{x\}$. Thus, we have $|\text{Fix}_X(g)| \equiv 0 \pmod{2}$, and the claim follows.

Since G is block-transitive, it is sufficient to consider some appropriate, unique block $B \in \mathcal{B}$. As clearly $\langle \alpha \rangle \leq \text{Aut}(N)_{0,1,\infty}$, we deduce from above that $G \cap \langle \alpha \rangle \leq G_{0B}$ by the definition of Steiner 4-designs. Hence, we have in particular

$$(q^3 - 2)(q^2 + q + 1) \leq (k - 1)(k - 2)(k - 3),$$

which is not possible as Corollary 11 yields $k \leq \lfloor \sqrt{q^3 + 1} + \frac{5}{2} \rfloor < q^{\frac{3}{2}} + 3$.

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

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_z acts on $X^\pm \setminus \{z\}$ as $O^\pm(2d, 2)$ does in its usual rank 3 manner on singular points of the underlying non-degenerate orthogonal space $V^\pm = V^\pm(2d, 2)$. Again, we will prove by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 4-design \mathcal{D} .

It is easily seen that there are $2^{2d-2}(2^d \mp 1)(2^{d-1} \pm 1)$ hyperbolic pairs in V^\pm , and by Witt's theorem, $O^\pm(2d, 2)$ 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

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

Clearly, $O^\pm(2d, 2)_{\{x, y\}}$ stabilizes \mathcal{E}^\perp as a subspace, which implies that $O^\pm(2d, 2)_{\{x, y\}} \cong O^\pm(2d - 2, 2)$. Therefore, we have

$$O^\pm(2d - 2, 2) \cong O^\pm(2d, 2)_{\{x, y\}} \trianglelefteq O^\pm(2d, 2)_\mathcal{E} = G_{z, \mathcal{E}}.$$

Since $O^\pm(2d - 2, 2)$ acts transitively on the singular points of the $(2d - 2)$ -dimensional orthogonal subspace, we conclude that the smallest orbit on $V^\pm \setminus \mathcal{E}$

under $G_{z,\mathcal{E}}$ has length at least $2^{2d-3} \pm 2^{d-2}$. If the unique block $B \in \mathcal{B}$ which is incident with the 4-subset $\{x, y, x + y, z\}$ contains some singular point in $V^\pm \setminus \mathcal{E}$, then we would have $k \geq 2^{2d-3} \pm 2^{d-2} + 4$, a contradiction to Corollary 11. Thus, all points of B apart from z lie completely in \mathcal{E} . By the flag-transitivity of G , it follows then that for each block all points apart from a singleton must be contained in an affine plane. Therefore, we have $k \leq 5$, and in particular $k = 5$ as trivial Steiner 4-designs are excluded. But, on the other hand, Lemma 9 (c) yields $k \equiv 0 \pmod{4}$, a contradiction.

Case (7): $N = PSL(2, 11)$, $v = 11$.

As it is known, this exceptional permutation action occurs inside the Mathieu group M_{24} in its action on 24 points. This set can be partitioned into two sets X_1 and X_2 of 12 points each such that the setwise stabilizer of X_1 is the Mathieu group M_{12} . The stabilizer in this latter group of a point x in X_1 is isomorphic to M_{11} and operates (apart from its natural 4-transitive action on $X_1 \setminus \{x\}$) 3-transitively on the 12 points of X_2 . The one-point stabilizer in this action of degree 12 is $PSL(2, 11)$ acting 2-transitively on 11 points. The geometry preserved by the 3-transitive action of M_{11} is not a Steiner t -design, but a 3-(12, 6, 2) design (e.g. [4, Ch. IV, 5.3]). Thus, the derived design \mathcal{D} on which $G \leq \text{Aut}(\mathcal{D})$ acts cannot be a Steiner design.

Case (8): $N = PSL(2, 8)$, $v = 28$.

As $v = 28$, we have $k \leq 7$ by Corollary 11. But, Lemma 9 (c) clearly eliminates the cases when $k = 5, 6$ or 7 .

Case (9): $N = M_v$, $v = 11, 12, 22, 23, 24$.

If $v = 11, 12, 23$ or 24 , then $G = M_v$ is always 4-transitive, and thus [35, Thm. 3] yields the designs described in Main Theorem 2. Obviously, flag-transitivity holds as the 4-transitivity of G implies that G_x acts block-transitively on the derived Steiner 3-design \mathcal{D}_x for any $x \in X$. For $v = 22$, Corollary 11 gives $k \leq 7$, and again the cases for k can easily be eliminated by Lemma 9 (c).

Case (10): $N = M_{11}$, $v = 12$.

As already illustrated in Case (7), $G \leq \text{Aut}(\mathcal{D})$ cannot act on any Steiner design \mathcal{D} .

Cases (11)-(13).

For the existence of non-trivial flag-transitive Steiner 4-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 8, Lemma 9 (b) and (c), and Corollary 11.

This completes the proof of Main Theorem 2.

Chapter 6

The Classification of all Flag-transitive Steiner 5-Designs

The classification of all non-trivial Steiner 5-designs admitting a flag-transitive group of automorphisms is as follows.

Main Theorem 3. *Let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 5-design. Then $G \leq \text{Aut}(\mathcal{D})$ acts flag-transitively on \mathcal{D} if and only if one of the following occurs:*

- (1) \mathcal{D} is isomorphic to the Witt 5-(12, 6, 1) design, and $G \cong M_{12}$,
- (2) \mathcal{D} is isomorphic to the Witt 5-(24, 8, 1) design, and $G \cong PSL(2, 23)$ or $G \cong M_{24}$.

We remark that in Part (2), $G \cong PSL(2, 23)$ acts sharply flag-transitively on \mathcal{D} , and furthermore that M_{24} as the full group of automorphisms of \mathcal{D} contains only one conjugacy class of subgroups isomorphic to $PSL(2, 23)$ (cf. [15]).

6.1 Groups of Automorphisms of Affine Type

In this section, we start with the proof of Main Theorem 3. Using the notation as before, let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 5-design with $G \leq \text{Aut}(\mathcal{D})$ acting flag-transitively on \mathcal{D} . We recall that due to Proposition 7, we may restrict ourselves to the consideration of the finite 3-homogeneous permutation groups listed in Chapter 3. Let us first assume that G is of affine type.

Case (1): $G \cong AGL(1, 8)$, $AFL(1, 8)$ or $AFL(1, 32)$.

As trivial Steiner 5-designs are excluded, let $k > 5$. For $v = 8$, we obtain $k = 6$ by Corollary 11, which is not possible in view of Lemma 9 (b). If $v = 32$, then $|G| = 5v(v - 1)$, and Lemma 8 immediately yields that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 5-design \mathcal{D} .

Case (2): $G_0 \cong SL(d, 2)$, $d \geq 2$.

Let e_i denote the i -th standard basis vector of the vector space $V = V(d, 2)$, and $\langle e_i \rangle$ the 1-dimensional vector subspace spanned by e_i . We will prove by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 5-design \mathcal{D} .

To exclude trivial Steiner 5-designs, let $v = 2^d > k > 5$. For $d = 3$, we have $v = 8$ and $k = 6$ by Corollary 11, which is not possible in view of Lemma 9 (b) again. So, we may assume that $d > 3$. We remark that clearly any five distinct points are non-coplanar in $AG(d, 2)$ and hence generate an affine subspace of dimension at least 3. Let $\mathcal{E} = \langle e_1, e_2, e_3 \rangle$ denote the 3-dimensional vector subspace spanned by e_1, e_2, e_3 . Then by linear algebra $SL(d, 2)_{\mathcal{E}}$, and therefore also $G_{0, \mathcal{E}}$, acts point-transitively on $V \setminus \mathcal{E}$. If the unique block $B \in \mathcal{B}$ which is incident with the 5-subset $\{0, e_1, e_2, e_3, e_1 + e_2\}$ contains some point outside \mathcal{E} , then it would already contain all points of $V \setminus \mathcal{E}$. But then, we would have $k \geq 2^d - 8 + 5 = 2^d - 3$, a contradiction to Corollary 11. Hence, B lies completely in \mathcal{E} , and by the flag-transitivity of G , it follows that each block must be contained in a 3-dimensional affine subspace. Thus, clearly $k \leq 8$. But, on the other hand, for \mathcal{D} to be a block-transitive 5-design admitting $G \leq \text{Aut}(\mathcal{D})$, we obtain from [1] the necessary (and sufficient) condition that $2^d - 3$ must divide $\binom{k}{4}$, and hence it follows for each respective value of k that $d = 3$, contradicting our assumption.

Case (3): $G_0 \cong A_7$, $v = 2^4$.

Since $v = 2^4$, we obtain from Corollary 11 that $k \leq 7$. But, Lemma 8 easily rules out the cases when $k = 6$ or 7.

6.2 Groups of Automorphisms of Almost Simple Type

Maintaining the same notation, let $\mathcal{D} = (X, \mathcal{B}, I)$ be a non-trivial Steiner 5-design with $G \leq \text{Aut}(\mathcal{D})$ acting flag-transitively on \mathcal{D} . We consider in this section successively those cases where G is of almost simple type. For Case (2) Lemmas 16-25 from Chapter 5 will be required.

Case (1): $N = A_v$, $v \geq 5$.

As trivial Steiner 5-designs are excluded, we may assume that $v \geq 7$. But then A_v , and hence also G , is 5-transitive and does not act on any non-trivial Steiner 5-design \mathcal{D} in view of [35, Thm. 3].

Case (2): $N = PSL(2, q)$, $v = q + 1$, $q = p^e > 3$.

Without restriction, we have $q \geq 5$ as $PSL(2, 4) \cong PSL(2, 5)$, and $\text{Aut}(N) = P\Gamma L(2, q)$. We will show that only the flag-transitive design given in Part (2) of Main Theorem 3 with $G \cong PSL(2, 23)$ can occur. In the following, let $n = (2, q - 1)$, and we may assume that $k > 5$ as trivial Steiner 5-designs are excluded.

We will first assume that $N = G$. Then, by Remark 12, we obtain

$$(q - 2)(q - 3) |PSL(2, q)_{0B}| \cdot n = (k - 1)(k - 2)(k - 3)(k - 4). \quad (6.1)$$

In view of Proposition 10 (b), we have

$$q - 3 \geq (k - 3)(k - 4), \quad (6.2)$$

and thus it follows from equation (6.1) that

$$(q - 2) |PSL(2, q)_{0B}| \cdot n \leq (k - 1)(k - 2). \quad (6.3)$$

If we assume that $k \geq 9$, then clearly

$$(k - 1)(k - 2) < 2(k - 3)(k - 4),$$

and hence we obtain

$$(q - 2) |PSL(2, q)_{0B}| \cdot n < 2(q - 3)$$

due to Proposition 10 (b) again, which is obviously only possible when $|PSL(2, q)_{0B}| \cdot n = 1$. Thus, in particular q has to be even. But then, considering equation (6.1) yields that the left hand side of the equation is not divisible by 4, whereas obviously the right hand side is always divisible by 8, a contradiction. If $k < 9$, then, using equation (6.1) and inequality (6.2), the very few remaining possibilities for k can immediately be ruled out by hand, except for the case when $k = 8$, $q = 23$ and $|PSL(2, q)_{0B}| = 1$. It is well-known that for the parameters $t = 5$, $v = 24$ and $k = 8$ there exists (up to isomorphism) only the unique Witt 5-(24, 8, 1) design \mathcal{D} , which can be constructed from $PSL(2, 23)$ in its natural 3-homogeneous action on the elements of $GF(23) \cup \{\infty\}$. Furthermore, it can be shown that the setwise stabilizer $PSL(2, 23)_B$ of an appropriate, unique block $B \in \mathcal{B}$ is a dihedral group of order 8 (see, e.g., [4, Ch. IV, 1.5], [14, Ch. XIV, 115], and [51, Thm. 5] for a uniqueness proof). Thus, using Lemma 9 (b), we obtain $b = 759 = [PSL(2, 23) : PSL(2, 23)_B]$, and hence $PSL(2, 23)$ acts block-transitively on \mathcal{D} . As for $q = 23$, the dihedral group of order 8 has only orbits of length 8 in view of Lemma 18 (ii)(a), clearly $PSL(2, 23)_B$ acts transitively on the points of B . Since we have $|PSL(2, 23)_{0B}| = 1$, it follows that $PSL(2, 23)$ acts even sharply flag-transitively on \mathcal{D} .

Now, let us assume that $N < G \leq \text{Aut}(N)$. We recall that $q = p^e > 3$, and will distinguish in the following the cases $p > 3$, $p = 2$, and $p = 3$.

First, let $p > 3$. We define

$$G^* = G \cap (PSL(2, q) \rtimes \langle \tau_\alpha \rangle)$$

with $\tau_\alpha \in \text{Sym}(GF(p^e) \cup \{\infty\}) \cong S_v$ of order e induced by the Frobenius automorphism $\alpha : GF(p^e) \rightarrow GF(p^e)$, $x \mapsto x^p$. Then, by Dedekind's law, we can write

$$G^* = PSL(2, q) \rtimes (G^* \cap \langle \tau_\alpha \rangle). \quad (6.4)$$

Defining $P\Sigma L(2, q) = PSL(2, q) \rtimes \langle \tau_\alpha \rangle$, it can easily be calculated that $P\Sigma L(2, q)_{0,1,\infty} = \langle \tau_\alpha \rangle$, and $\langle \tau_\alpha \rangle$ has precisely $p + 1$ distinct fixed points (cf., e.g., [21, Ch. 6.4, Lemma 2]). As $p > 3$, we conclude therefore that $G^* \cap \langle \tau_\alpha \rangle \leq G^*_{0B}$

for some appropriate, unique block $B \in \mathcal{B}$ by the definition of Steiner 5-designs. Furthermore, clearly $PSL(2, q) \cap (G^* \cap \langle \tau_\alpha \rangle) = 1$. Hence, we have

$$\begin{aligned} |(0, B)^{G^*}| &= [G^* : G_{0B}^*] \\ &= [PSL(2, q) \rtimes (G^* \cap \langle \tau_\alpha \rangle) : PSL(2, q)_{0B} \rtimes (G^* \cap \langle \tau_\alpha \rangle)] \\ &= [PSL(2, q) : PSL(2, q)_{0B}] \\ &= |(0, B)^{PSL(2, q)}|. \end{aligned} \quad (6.5)$$

Thus, if we assume that $G^* \leq \text{Aut}(\mathcal{D})$ acts already flag-transitively on \mathcal{D} , then we obtain $|(0, B)^{G^*}| = |(0, B)^{PSL(2, q)}| = bk$ in view of Remark 12. Hence, $PSL(2, q)$ must also act flag-transitively on \mathcal{D} , and we may proceed as in the case when $N = G$. Therefore, let us assume that $G^* \leq \text{Aut}(\mathcal{D})$ does not act flag-transitively on \mathcal{D} . Then, we conclude that $[G : G^*] = 2$ and G^* has exactly two orbits of equal length on the set of flags. Thus, by equation (6.5), we obtain for the orbit containing the flag $(0, B)$ that $|(0, B)^{G^*}| = |(0, B)^{PSL(2, q)}| = \frac{bk}{2}$. As it is well-known the normalizer of $PSL(2, q)$ in $\text{Sym}(X)$ is $P\Gamma L(2, q)$, and hence in particular $PSL(2, q)$ is normal in G . It follows therefore that we have under $PSL(2, q)$ also precisely one further orbit of equal length on the set of flags. Then, proceeding similarly to the case $N = G$ for each orbit on the set of flags, we obtain (representative for the orbit containing the flag $(0, B)$) that

$$\frac{(q-2)(q-3)|PSL(2, q)_{0B}| \cdot n}{2} = (k-1)(k-2)(k-3)(k-4), \quad (6.6)$$

and as here $n = 2$, this is equivalent to

$$\begin{aligned} (q-2)(q-3)|PSL(2, q)_{0B}| &= (k-1)(k-2)(k-3)(k-4) \\ &= k(k^3 - 10k^2 + 35k - 50) + 24. \end{aligned} \quad (6.7)$$

Hence, we have in particular

$$k \mid (q-2)(q-3)|PSL(2, q)_{0B}| - 24. \quad (6.8)$$

Since $PSL(2, q)_B$ can have one or two orbits of equal length on the points of B , we have

$$k \text{ or } \frac{k}{2} = |0^{PSL(2, q)_B}| = [PSL(2, q)_B : PSL(2, q)_{0B}]. \quad (6.9)$$

By the same arguments as in case $N = G$, we deduce from equation (6.7) that

$$(q-2)|PSL(2, q)_{0B}| \leq (k-1)(k-2), \quad (6.10)$$

and assuming that $k \geq 9$, we obtain

$$(q-2) |PSL(2, q)_{0B}| < 2(q-3),$$

which is clearly only possible when $|PSL(2, q)_{0B}| = 1$. Hence, it follows that

$$(q-2)(q-3) = (k-1)(k-2)(k-3)(k-4), \quad (6.11)$$

and $k \mid (q-2)(q-3) - 24$ in view of property (6.8). On the other hand, for $k \geq 9$, we obtain from equation (6.9) that k or $\frac{k}{2} = |PSL(2, q)_B| \mid |PSL(2, q)| = \frac{q^3 - q}{2}$, and thus in particular $k \mid q^3 - q$. But, it can easily be seen that $(q^3 - q, (q-2)(q-3) - 24) \mid 2^3 \cdot 3 \cdot 11$, and thus we have only a small number of possibilities for k to check, which can easily be ruled out by hand using equation (6.11). For $k < 9$, the very few remaining possibilities for k can immediately be ruled out by hand using inequality (6.2) and equation (6.7), except for the case when $k = 8$, $q = 23$ and $|PSL(2, q)_{0B}| = 2$. But, as involutions are fixed point free on the points of the projective line for $q \equiv 3 \pmod{4}$ in view of Lemma 16, this is impossible.

Now, let $p = 2$. Then, clearly $N = PSL(2, q) = PGL(2, q)$, and we have $\text{Aut}(N) = P\Sigma L(2, q)$. If we assume that $\langle \tau_\alpha \rangle \leq P\Sigma L(2, q)_{0B}$ for some appropriate, unique block $B \in \mathcal{B}$, then, using the terminology of (6.4), we have $G^* = G = P\Sigma L(2, q)$ and as clearly $PSL(2, q) \cap \langle \tau_\alpha \rangle = 1$, we can apply equation (6.5). Thus, $PSL(2, q)$ must also be flag-transitive, which has already been considered. Therefore, we may assume that $\langle \tau_\alpha \rangle \not\leq P\Sigma L(2, q)_{0B}$. Let s be a prime divisor of $e = |\langle \tau_\alpha \rangle|$. As the normal subgroup $H := (P\Sigma L(2, q)_{0,1,\infty})^s \leq \langle \tau_\alpha \rangle$ of index s has precisely $p^s + 1$ distinct fixed points (see, e.g., [21, Ch. 6.4, Lemma 2]), we have $G \cap H \leq G_{0B}$ for some appropriate, unique block $B \in \mathcal{B}$ by the definition of Steiner 5-designs. It can then be deduced that $e = s^u$ for some $u \in \mathbb{N}$, since if we assume for $G = P\Sigma L(2, q)$ that there exists a further prime divisor \bar{s} of e with $\bar{s} \neq s$, then $\bar{H} := (P\Sigma L(2, q)_{0,1,\infty})^{\bar{s}} \leq \langle \tau_\alpha \rangle$ and H are both subgroups of $P\Sigma L(2, q)_{0B}$ by the flag-transitivity of $P\Sigma L(2, q)$, and hence $\langle \tau_\alpha \rangle \leq P\Sigma L(2, q)_{0B}$, a contradiction. Furthermore, as $\langle \tau_\alpha \rangle \not\leq P\Sigma L(2, q)_{0B}$, we may, by applying Dedekind's law, assume that

$$G_{0B} = PSL(2, q)_{0B} \rtimes (G \cap H).$$

Thus, by Remark 12, we obtain

$$(q-2)(q-3) |PSL(2, q)_{0B}| |G \cap H| = (k-1)(k-2)(k-3)(k-4) |G \cap \langle \tau_\alpha \rangle|.$$

Using that $k = |0^{G_B}| = [G_B : G_{0B}]$, we have more precisely

(A) if $G = PSL(2, q) \rtimes (G \cap H)$:

$$(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k}, \text{ or}$$

(B) if $G = P\Sigma L(2, q)$:

$$(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k} \cdot \begin{cases} s, & \text{if } G_B = PSL(2, q)_B \rtimes \langle \tau_\alpha \rangle \\ 1, & \text{if } G_B = PSL(2, q)_B \rtimes H. \end{cases}$$

As far as condition (A) is concerned, we may argue exactly as in the earlier case $N = G$. Thus, only condition (B) has to be examined, and we will also show that here $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 5-design \mathcal{D} . Clearly, there exists always a Klein four-group $V_4 \leq PSL(2, q)$, which fixes some 4-subset S of X and some additional point $x \in X$, and hence must fix the unique block $B \in \mathcal{B}$ which is incident with $S \cup \{x\}$ by the definition of Steiner 5-designs. Examining the list of possible subgroups of $PSL(2, q)$ with their orbits on the projective line (cf. Lemmas 17-25), it follows that we only have to consider the possibility when $PSL(2, q)_B$ is conjugate to $PSL(2, \bar{q})$ with $\bar{q}^m = q$, $m \geq 1$, and by Lemma 21, we conclude that $k = \bar{q} + 1$. Applying condition (B) yields then

$$(q-2)(q-3) |PSL(2, q)_{0B}| = \bar{q}(\bar{q}-1)(\bar{q}-2)(\bar{q}-3)s \quad (6.12)$$

$$\text{with } |PSL(2, q)_{0B}| = \bar{q}(\bar{q}-1) \cdot \begin{cases} s, & \text{or} \\ 1. \end{cases}$$

Since $q = 2^{s^u}$, we can write $\bar{q} = 2^{s^w}$ for some integer $0 \leq w \leq u$, and $q = \bar{q}^m = \bar{q}^{s^{u-w}}$. As we may assume that $k = \bar{q} + 1 = 2^{s^w} + 1 > 5$, it follows in particular that $w \geq 1$, and hence $s < 2^{s^w} = \bar{q}$. Thus, using equation (6.12), we obtain

$$(\bar{q}^{s^{u-w}} - 2)(\bar{q}^{s^{u-w}} - 3) = (q-2)(q-3) \leq (\bar{q}-2)(\bar{q}-3)s < (\bar{q}^2 - 2s)(\bar{q}-3).$$

But, as clearly $u - w \geq 1$ (otherwise, $k = q + 1$, a contradiction to Corollary 11), this yields a contradiction for every prime s .

Now, let $p = 3$. We have $\text{Aut}(N) = P\Gamma L(2, q) = PGL(2, q) \rtimes \langle \tau_\alpha \rangle$, and as $PGL(2, q)$ is sharply 3-transitive, it follows that $P\Gamma L(2, q)_{0,1,\infty} = \langle \tau_\alpha \rangle$. Again, we define $G^* = G \cap (PSL(2, q) \rtimes \langle \tau_\alpha \rangle)$ and may write $G^* = PSL(2, q) \rtimes (G^* \cap \langle \tau_\alpha \rangle)$ as in equation (6.4). We will distinguish in the following the cases $G = G^*$ and $[G : G^*] = 2$. First, let $G = G^*$. Then, we have $\text{Aut}(N) = P\Sigma L(2, q)$. If we assume that $\langle \tau_\alpha \rangle \leq P\Sigma L(2, q)_{0B}$ for some appropriate, unique block $B \in \mathcal{B}$, then $G = P\Sigma L(2, q)$, and as clearly $PSL(2, q) \cap \langle \tau_\alpha \rangle = 1$, we can apply equation (6.5). Thus, $PSL(2, q)$ must also be flag-transitive, which has already been considered. Therefore, we may assume that $\langle \tau_\alpha \rangle \not\leq P\Sigma L(2, q)_{0B}$. Let s be a prime divisor of $e = |\langle \tau_\alpha \rangle|$. As already mentioned, the normal subgroup $H := (P\Sigma L(2, q)_{0,1,\infty})^s \leq \langle \tau_\alpha \rangle$ of index s has precisely $p^s + 1$ distinct fixed points, and hence we have $G \cap H \leq G_{0B}$ for some appropriate, unique block $B \in \mathcal{B}$ by the definition of Steiner 5-designs. It can then be deduced exactly as for $p = 2$ that $e = s^u$ for some $u \in \mathbb{N}$. As $\langle \tau_\alpha \rangle \not\leq P\Sigma L(2, q)_{0B}$, we may, by applying Dedekind's law, assume that

$$G_{0B} = PSL(2, q)_{0B} \rtimes (G \cap H).$$

Thus, by Remark 12, we obtain

$$2(q-2)(q-3) |PSL(2, q)_{0B}| |G \cap H| = (k-1)(k-2)(k-3)(k-4) |G \cap \langle \tau_\alpha \rangle|.$$

Using that $k = |0^{G_B}| = [G_B : G_{0B}]$, we have more precisely

(A*) if $G = PSL(2, q) \rtimes (G \cap H)$:

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k}, \text{ or}$$

(B*) if $G = P\Sigma L(2, q)$:

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k} \cdot \begin{cases} s, & \text{if } G_B = PSL(2, q)_B \rtimes \langle \tau_\alpha \rangle \\ 1, & \text{if } G_B = PSL(2, q)_B \rtimes H. \end{cases}$$

Considering condition (A*), we may argue exactly as in the earlier case $N = G$. Thus, only condition (B*) has to be examined, and we will show in the following that here $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 5-design \mathcal{D} . In view of the subgroups of $PSL(2, q)$ with their orbits on the projective line (Lemmas 17-25), we have to examine the following possibilities:

- (i) $PSL(2, q)_B$ is conjugate to a cyclic subgroup of order c with $c \mid \frac{q \pm 1}{2}$ of $PSL(2, q)$, and $k = c$.
- (ii) $PSL(2, q)_B$ is conjugate to a dihedral subgroup of order $2c$ with $c \mid \frac{q \pm 1}{2}$ of $PSL(2, q)$, and $k = c$ or $2c$.
- (iii) $PSL(2, q)_B$ is conjugate to an elementary Abelian subgroup of order $\bar{q} \mid q$ of $PSL(2, q)$, and $k = \bar{q}$.
- (iv) $PSL(2, q)_B$ is conjugate to a semi-direct product of an elementary Abelian subgroup of order $\bar{q} \mid q$ with a cyclic subgroup of order c of $PSL(2, q)$ with $c \mid \bar{q} - 1$ and $c \mid q - 1$, and $k = \bar{q}$ or $c\bar{q}$.
- (v) $PSL(2, q)_B$ is conjugate to $PSL(2, \bar{q})$ with $\bar{q}^m = q$, $m \geq 1$, and $k = \bar{q} + 1$, $\bar{q}(\bar{q} - 1)$ if m is even, or $k = (\bar{q} + 1)\bar{q}(\bar{q} - 1)/2$.
- (vi) $PSL(2, q)_B$ is conjugate to $PGL(2, \bar{q})$ with $\bar{q}^m = q$, $m > 1$ even, and $k = \bar{q} + 1$, $\bar{q}(\bar{q} - 1)$ or $k = (\bar{q} + 1)\bar{q}(\bar{q} - 1)$.
- (vii) $PSL(2, q)_B$ is conjugate to A_4 , and $k = 6$ or 12 .
- (viii) $PSL(2, q)_B$ is conjugate to S_4 , and $k = 6$ or 24 .
- (ix) $PSL(2, q)_B$ is conjugate to A_5 , and $k = 10, 12$ or 60 .

Since $q = 3^{s^u}$, we can write $\bar{q} = 3^{s^w}$ for some integer $0 \leq w \leq u$, and $q = \bar{q}^m = \bar{q}^{s^{u-w}}$.

ad (i): By condition (B*), we have

$$2(q - 2)(q - 3) |PSL(2, q)_{0B}| = (c - 1)(c - 2)(c - 3)(c - 4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} s, & \text{or} \\ 1. & \end{cases}$$

In view of the earlier case $N = G$, it is sufficient to consider the equation

$$(q-2)(q-3) = \frac{(c-1)(c-2)(c-3)(c-4)s}{2}. \quad (6.13)$$

For $c \mid \frac{q+1}{2}$, equation (6.13) yields

$$\begin{aligned} c \mid \frac{(q+1)(q-6)}{2} &= \frac{(q-2)(q-3)}{2} - 6 = \frac{(c-1)(c-2)(c-3)(c-4)s}{4} - 6 \\ &= \frac{cs}{4}(c^3 - 10c^2 + 35c - 50) + 6s - 6, \end{aligned}$$

and thus $c \mid 6s - 6$ must hold. If $c \mid \frac{q-1}{2}$, then, by equation (6.13), we have

$$\begin{aligned} c \mid \frac{(q-1)(q-4)}{2} &= \frac{(q-2)(q-3)}{2} - 1 = \frac{(c-1)(c-2)(c-3)(c-4)s}{4} - 1 \\ &= \frac{cs}{4}(c^3 - 10c^2 + 35c - 50) + 6s - 1, \end{aligned}$$

and hence $c \mid 6s - 1$ must hold. As clearly $c < 6s$ in both cases, it follows from equation (6.13) that in particular

$$(3^{s^u} - 2)(3^{s^u-1} - 1) < \frac{c^4 s}{6} < 6^3 \cdot s^5,$$

which implies that $s^u \leq 7$. As $c \mid 6s - 6$ respectively $c \mid 6s - 1$, this leaves only a very small number of possibilities for k to check, which can easily be ruled out by hand using equation (6.13).

ad (ii): Let $k = c$. Applying condition (B*) yields

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (c-1)(c-2)(c-3)(c-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = 2 \cdot \begin{cases} s, & \text{or} \\ 1. \end{cases}$$

First, let $k = c$. Due to the earlier case $N = G$, it is sufficient to consider the equation

$$(q-2)(q-3) = \frac{(c-1)(c-2)(c-3)(c-4)s}{4}. \quad (6.14)$$

If $c \mid \frac{q+1}{2}$, then, by equation (6.14), we have

$$\begin{aligned} c \mid \frac{(q+1)(q-6)}{2} &= \frac{(q-2)(q-3)}{2} - 6 = \frac{(c-1)(c-2)(c-3)(c-4)s}{8} - 6 \\ &= \frac{cs}{8}(c^3 - 10c^2 + 35c - 50) + 3s - 6, \end{aligned}$$

and hence $c \mid 3s - 6$ must hold. For $c \mid \frac{q-1}{2}$, it follows from equation (6.14) that

$$\begin{aligned} c \mid \frac{(q-1)(q-4)}{2} &= \frac{(q-2)(q-3)}{2} - 1 = \frac{(c-1)(c-2)(c-3)(c-4)s}{8} - 1 \\ &= \frac{cs}{8}(c^3 - 10c^2 + 35c - 50) + 3s - 1, \end{aligned}$$

and thus $c \mid 3s - 1$ must hold. Obviously, we have $c < 3s$ in both cases, and therefore equation (6.14) gives in particular

$$4(3^{s^u} - 2)(3^{s^u-1} - 1) < \frac{c^4 s}{3} < 3^3 \cdot s^5,$$

which implies that $s^u \leq 5$. Due to the fact that $c \mid 3s - 6$ respectively $c \mid 3s - 1$, we have only a very small number of possibilities for k to check, which can easily be ruled out by hand using equation (6.14). Now, let $k = 2c$. Due to condition (B*), we have

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (2c-1)(2c-2)(2c-3)(2c-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} s, & \text{or} \\ 1. \end{cases}$$

Again, it suffices to consider the equation

$$\frac{(q-2)(q-3)}{2} = (2c-1)(c-1)(2c-3)(c-2)s. \quad (6.15)$$

For $c \mid \frac{q+1}{2}$, equation (6.15) yields

$$\begin{aligned} c \mid \frac{(q+1)(q-6)}{2} &= \frac{(q-2)(q-3)}{2} - 6 = (2c-1)(c-1)(2c-3)(c-2)s - 6 \\ &= cs(4c^3 - 20c^2 + 35c - 25) + 6s - 6, \end{aligned}$$

and thus $c \mid 6s - 6$ must hold. If $c \mid \frac{q-1}{2}$, then due to equation (6.15), we have

$$\begin{aligned} c \mid \frac{(q-1)(q-4)}{2} &= \frac{(q-2)(q-3)}{2} - 1 = (2c-1)(c-1)(2c-3)(c-2)s - 1 \\ &= cs(4c^3 - 20c^2 + 35c - 25) + 6s - 1, \end{aligned}$$

and hence $c \mid 6s - 1$ must hold. As clearly $c < 6s$ in both cases, we deduce from equation (6.15) that in particular

$$(3^{s^u} - 2)(3^{s^u-1} - 1) < \frac{(2c)^4 s}{6} < 2^4 \cdot 6^3 \cdot s^5,$$

and hence it follows that $s^u \leq 7$. Since we have $c \mid 6s - 6$ respectively $c \mid 6s - 1$, this leaves only a very small number of possibilities for k to check, which can easily be ruled out by hand using equation (6.15).

ad (iii): In view of condition (B*), we have

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (\bar{q}-1)(\bar{q}-2)(\bar{q}-3)(\bar{q}-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} s, & \text{or} \\ 1. \end{cases}$$

It suffices to consider the equation

$$2(q-2)(q-3) = (\bar{q}-1)(\bar{q}-2)(\bar{q}-3)(\bar{q}-4)s. \quad (6.16)$$

As we may assume that $k = \bar{q} = 3^{s^w} > 5$, we have in particular $w \geq 1$, and hence $s < 3^{s^w} = \bar{q}$. Thus, using equation (6.16), we obtain

$$(\bar{q}^{s^{u-w}} - 2)(\bar{q}^{s^{u-w}} - 3) = (q-2)(q-3) < \bar{q}^4 s < \bar{q}^5.$$

But, as clearly $u - w \geq 1$ (otherwise, $k = q$, a contradiction to Corollary 11), this yields a contradiction for $s \geq 3$. If $s = 2$, then $(\bar{q}^{2^{u-w}} - 2)(\bar{q}^{2^{u-w}} - 3) < 2\bar{q}^4$ must hold, which cannot be true for $u - w > 1$. Thus, let $u - w = 1$. Hence, it follows from equation (6.16) that in particular

$$\bar{q} - 2 \mid (q-2)(q-3) = \bar{q}^4 - 5\bar{q}^2 + 6.$$

But, it is easily seen that $(\bar{q}^4 - 5\bar{q}^2 + 6, \bar{q} - 2) = (2, \bar{q} - 2) = 1$, yielding a contradiction.

ad (iv): Let $k = \bar{q}$. By condition (B*), we have

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (\bar{q}-1)(\bar{q}-2)(\bar{q}-3)(\bar{q}-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = c \cdot \begin{cases} s, & \text{or} \\ 1. \end{cases}$$

As $c \mid \bar{q} - 1$, we may argue, *mutatis mutandis*, as in subcase (iii). For $k = c\bar{q}$, condition (B*) yields

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (c\bar{q}-1)(c\bar{q}-2)(c\bar{q}-3)(c\bar{q}-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} s, & \text{or} \\ 1. & \end{cases}$$

We may consider only the equation

$$2(q-2)(q-3) = (c\bar{q}-1)(c\bar{q}-2)(c\bar{q}-3)(c\bar{q}-4)s. \quad (6.17)$$

Then, surely $(q-2)(q-3) = q^2 - 5q + 6$ must be divisible by $c\bar{q} - 3$. Polynomial division with remainder gives

$$\begin{aligned} q^2 - 5q + 6 &= \left(\sum_{i=1}^m 3^{i-1} \frac{q^2}{(c\bar{q})^i} + \sum_{j=1}^{\bar{m}} 3^{j-1} \frac{\left(\left(\frac{3}{c}\right)^m - 5\right)q}{(c\bar{q})^j} \right) (c\bar{q} - 3) \\ &\quad + \left(\frac{3}{c}\right)^{\bar{m}} \frac{\left(\left(\frac{3}{c}\right)^m - 5\right)q}{\bar{q}^{\bar{m}}} + 6 \end{aligned}$$

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

$$\deg\left(\left(\frac{3}{c}\right)^{\bar{m}} \frac{\left(\left(\frac{3}{c}\right)^m - 5\right)q}{\bar{q}^{\bar{m}}} + 6\right) < \deg(c\bar{q} - 3)$$

as is well-known). As $c \mid q - 1$, clearly c is not divisible by 3. Thus, the remainder can be rewritten as

$$\frac{\left(\left(\frac{3}{c}\right)^m - 5\right)}{c^{\bar{m}}} \cdot 3^{s^u - \bar{m}(s^w - 1)} + 6,$$

and hence in order for the remainder to vanish, necessarily $s^u - \bar{m}(s^w - 1) = 1$ must hold. But then, we obtain $3^m = (-2c^{\bar{m}} + 5)c^m$, a contradiction.

ad (v): Let $k = \bar{q} + 1$. In view of condition (B*), we have

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = \bar{q}(\bar{q}-1)(\bar{q}-2)(\bar{q}-3)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{\bar{q}(\bar{q}-1)}{2} \cdot \begin{cases} s, & \text{or} \\ 1. & \end{cases}$$

Again, it suffices to consider the equation

$$(q-2)(q-3) = (\bar{q}-2)(\bar{q}-3)s. \quad (6.18)$$

As we may assume that $k = \bar{q} + 1 = 3^{s^w} + 1 > 5$, it follows in particular that $w \geq 1$, and hence $s < 3^{s^w} = \bar{q}$. Thus, using equation (6.18), we obtain

$$(\bar{q}^{s^u - w} - 2)(\bar{q}^{s^u - w} - 3) = (q-2)(q-3) = (\bar{q}-2)(\bar{q}-3)s < (\bar{q}^2 - 2s)(\bar{q}-3).$$

But, as clearly $u - w \geq 1$ (otherwise, $k = q + 1$, a contradiction to Corollary 11), this yields a contradiction for every prime s . If $m > 1$ even and $k = \bar{q}(\bar{q} - 1)$, then, in view of condition (B*), we have

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (\bar{q}^2 - \bar{q} - 1)(\bar{q}^2 - \bar{q} - 2)(\bar{q}^2 - \bar{q} - 3)(\bar{q}^2 - \bar{q} - 4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{(\bar{q} + 1)}{2} \cdot \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

We may consider only the equation

$$(q-2)(q-3)(\bar{q}+1) = (\bar{q}^2 - \bar{q} - 1)(\bar{q}^2 - \bar{q} - 2)(\bar{q}^2 - \bar{q} - 3)(\bar{q}^2 - \bar{q} - 4)s.$$

As obviously $(\bar{q}^2 - \bar{q} - 1, \bar{q} + 1) = 1$, it follows that $\bar{q}^2 - \bar{q} - 1 \mid (q-2)(q-3)$ must hold. But, for $m > 1$ even, polynomial division with remainder gives

$$q^2 - 5q + 6 = \left(\sum_{i=1}^{m-1} n_i \frac{q^2}{\bar{q}^{i+1}} + \sum_{j=1}^m (n_j \cdot n_m + n_{j-1}(n_{m-1} - 5)) \frac{q}{\bar{q}^j} \right) (\bar{q}^2 - \bar{q} - 1)$$

$$+ (n_{m+1} \cdot n_m + n_m(n_{m-1} - 5))\bar{q} + n_m^2 + n_{m-1}(n_{m-1} - 5) + 6,$$

where n_i denote the i -th Fibonacci number recursively defined via

$$n_0 = 0, \quad n_1 = n_2 = 1, \quad n_i = n_{i-1} + n_{i-2} \quad (i \geq 3).$$

As it can easily be seen the remainder never vanishes, and hence we obtain a contradiction. For $k = (\bar{q} + 1)\bar{q}(\bar{q} - 1)/2$, condition (B*) yields

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = \left(\frac{\bar{q}^3 - \bar{q}}{2} - 1 \right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 2 \right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 3 \right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 4 \right) s$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

It suffices to consider the equation

$$2(q-2)(q-3) = \left(\frac{\bar{q}^3 - \bar{q}}{2} - 1 \right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 2 \right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 3 \right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 4 \right) s. \quad (6.19)$$

If we assume that $\bar{q} = 3$, then $k = 12$. Thus, we obtain from equation (6.19) that $s^u < 5$. Hence, there are only a very small number of possibilities to check, which can easily be ruled out by hand. Therefore, let us assume that $\bar{q} > 3$. Then, we

have in particular $w \geq 1$, and hence $s < 3^{s^w} = \bar{q}$. Thus, using equation (6.19), we obtain

$$2(q-2)(q-3) < \left(\frac{\bar{q}^3 - \bar{q}}{2}\right)^4 s < \frac{1}{16} \bar{q}^{12} s < \frac{1}{16} \bar{q}^{13}.$$

On the other hand, it follows that

$$\begin{aligned} 2(q-2)(q-3) &= \left(\frac{\bar{q}^3 - \bar{q}}{2} - 1\right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 2\right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 3\right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 4\right) s \\ &\geq 2 \left(\frac{\bar{q}^3 - \bar{q}}{2} - 1\right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 2\right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 3\right) \left(\frac{\bar{q}^3 - \bar{q}}{2} - 4\right) \\ &= \frac{1}{8} \bar{q}^{12} - l \end{aligned}$$

with $l = \frac{1}{2} \bar{q}^{10} + \frac{5}{2} \bar{q}^9 - \frac{3}{4} \bar{q}^8 - \frac{15}{2} \bar{q}^7 - 17 \bar{q}^6 + \frac{15}{2} \bar{q}^5 + \frac{279}{8} \bar{q}^4 + \frac{95}{2} \bar{q}^3 - \frac{35}{2} \bar{q}^2 - 50 \bar{q} - 48$. As for $\bar{q} > 3$, clearly $l < \frac{1}{16} \bar{q}^{12}$ holds, we obtain

$$2(q-2)(q-3) \geq \frac{1}{16} \bar{q}^{12}.$$

But as $2(q-2)(q-3) = 2(\bar{q}^{2m} - 5\bar{q}^m + 6)$, this leaves at most only $m = 6$, which clearly cannot occur since $m = s^{u-w}$.

ad (vi): Let $k = \bar{q} + 1$. Applying condition (B*) yields

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = \bar{q}(\bar{q}-1)(\bar{q}-2)(\bar{q}-3)s$$

$$\text{with } |PSL(2, q)_{0B}| = \bar{q}(\bar{q}-1) \cdot \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

Clearly, we may argue, mutatis mutandis, as for $k = \bar{q} + 1$ in subcase (v). Let $k = \bar{q}(\bar{q}-1)$. Due to condition (B*), we have

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (\bar{q}^2 - \bar{q} - 1)(\bar{q}^2 - \bar{q} - 2)(\bar{q}^2 - \bar{q} - 3)(\bar{q}^2 - \bar{q} - 4)s$$

$$\text{with } |PSL(2, q)_{0B}| = (\bar{q} + 1) \cdot \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

As $\bar{q}^2 - \bar{q} - 1$ is always odd, we may argue, mutatis mutandis, as for $k = \bar{q}(\bar{q}-1)$ in subcase (v). Now, let $k = (\bar{q} + 1)\bar{q}(\bar{q}-1)$. Then, condition (B*) yields

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (\bar{q}^3 - \bar{q} - 1)(\bar{q}^3 - \bar{q} - 2)(\bar{q}^3 - \bar{q} - 3)(\bar{q}^3 - \bar{q} - 4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

We may consider only the equation

$$2(q-2)(q-3) = (\bar{q}^3 - \bar{q} - 1)(\bar{q}^3 - \bar{q} - 2)(\bar{q}^3 - \bar{q} - 3)(\bar{q}^3 - \bar{q} - 4)s. \quad (6.20)$$

If $\bar{q} = 3$, then we have $k = 24$, which implies that $s^u \leq 5$ must hold. Hence, we have only a very small number of possibilities to check, which can easily be ruled out by hand. Thus, let us assume that $\bar{q} > 3$. Then, it follows in particular that $w \geq 1$, and hence $s < 3^{s^w} = \bar{q}$. Using equation (6.20), it follows therefore that

$$2(q-2)(q-3) < (\bar{q}^3 - \bar{q})^4 s < \bar{q}^{12} s < \bar{q}^{13}.$$

On the other hand, we have

$$\begin{aligned} 2(q-2)(q-3) &= (\bar{q}^3 - \bar{q} - 1)(\bar{q}^3 - \bar{q} - 2)(\bar{q}^3 - \bar{q} - 3)(\bar{q}^3 - \bar{q} - 4)s \\ &\geq 2(\bar{q}^3 - \bar{q} - 1)(\bar{q}^3 - \bar{q} - 2)(\bar{q}^3 - \bar{q} - 3)(\bar{q}^3 - \bar{q} - 4) \\ &= 2\bar{q}^{12} - l \end{aligned}$$

with $l = 8\bar{q}^{10} + 20\bar{q}^9 - 12\bar{q}^8 - 60\bar{q}^7 - 62\bar{q}^6 + 60\bar{q}^5 + 138\bar{q}^4 + 80\bar{q}^3 - 70\bar{q}^2 - 100\bar{q} - 48$. As for $\bar{q} > 3$, clearly $l < \bar{q}^{12}$ holds, it follows that

$$2(q-2)(q-3) \geq \bar{q}^{12}.$$

But as $2(q-2)(q-3) = 2(\bar{q}^{2m} - 5\bar{q}^m + 6)$, this leaves only $m = 6$, which obviously cannot occur since $m = s^{u-w}$.

ad (vii): In view of condition (B*), we have

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{12}{k} \cdot \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

It is sufficient to consider the equation

$$(3^{s^u} - 2)(3^{s^u} - 3) = \frac{k(k-1)(k-2)(k-3)(k-4)}{24} \cdot s.$$

Thus, for $k = 6$ respectively $k = 12$, we obtain $s^u \leq 2$ respectively $s^u < 5$, and thus we have only a very small number of possibilities to check, which can easily be ruled out by hand.

ad (viii): Applying condition (B*) yields

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{24}{k} \cdot \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

We may consider only the equation

$$2(3^{s^u} - 2)(3^{s^u} - 3) = \frac{k(k-1)(k-2)(k-3)(k-4)}{24} \cdot s.$$

Thus, for $k = 6$ respectively $k = 24$, we obtain $s^u < 2$ respectively $s^u \leq 5$, and hence we have only a very small number of possibilities to check, which can again easily be ruled out by hand.

ad (ix): Due to condition (B*), we have

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{60}{k} \cdot \begin{cases} s, \text{ or} \\ 1. \end{cases}$$

It is sufficient to consider the equation

$$5(3^{s^u} - 2)(3^{s^u} - 3) = \frac{k(k-1)(k-2)(k-3)(k-4)}{24} \cdot s.$$

Thus, for $k = 10$ and 12 , it follows in both cases that $s^u \leq 3$, and for $k = 60$, we obtain $s^u \leq 7$. Hence, we have again only a very small number of possibilities to check, which can easily be ruled out by hand again, completing the examination of condition (B*).

Now, we consider the case when $[G : G^*] = 2$. We first assume that $\langle \tau_\alpha \rangle \not\leq P\Gamma L(2, q)_{0B}$ for some appropriate, unique block $B \in \mathcal{B}$. Again, let s be a prime divisor of $e = |\langle \tau_\alpha \rangle|$. As the normal subgroup $H := (P\Gamma L(2, q)_{0,1,\infty})^s \leq \langle \tau_\alpha \rangle$ of index s has precisely $p^s + 1$ distinct fixed points, we have $G \cap H \leq G_{0B}$ for some appropriate, unique block $B \in \mathcal{B}$ by the definition of Steiner 5-designs. Mutatis mutandis as in case $p = 2$, it follows then that $e = s^u$ for some $u \in \mathbb{N}$. Since $\langle \tau_\alpha \rangle \not\leq P\Gamma L(2, q)_{0B}$, we may, by applying Dedekind's law, assume that

$$G_{0B} = \begin{cases} PGL(2, q)_{0B} \rtimes (G \cap H), \text{ or} \\ PSL(2, q)_{0B} \rtimes (G \cap H). \end{cases}$$

Thus, by Remark 12, we obtain

$$(q-2)(q-3) \cdot \begin{cases} |PGL(2, q)_{0B}| \\ |PSL(2, q)_{0B}| \end{cases} \cdot |G \cap H| = (k-1)(k-2)(k-3)(k-4) |G \cap \langle \tau_\alpha \rangle|.$$

Using that $k = |0^{G_B}| = [G_B : G_{0B}]$, we have more precisely

(\bar{A}) if $G = PGL(2, q) \rtimes (G \cap H)$:

(i) for $G_{0B} = PGL(2, q)_{0B} \rtimes (G \cap H)$:

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k}, \text{ or}$$

(ii) for $G_{0B} = PSL(2, q)_{0B} \rtimes (G \cap H)$:

$$(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k} \cdot \begin{cases} 2, & \text{if } G_B = PGL(2, q)_B \rtimes (G \cap H) \\ 1, & \text{if } G_B = PSL(2, q)_B \rtimes (G \cap H), \text{ or} \end{cases}$$

(\bar{B}) if $G = PGL(2, q)$:

(i) for $G_{0B} = PGL(2, q)_{0B} \rtimes H$:

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k} \cdot \begin{cases} s, & \text{if } G_B = PGL(2, q)_B \rtimes \langle \tau_\alpha \rangle \\ 1, & \text{if } G_B = PGL(2, q)_B \rtimes H, \text{ or} \end{cases}$$

(ii) for $G_{0B} = PSL(2, q)_{0B} \rtimes H$:

$$(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)s$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k} \cdot \begin{cases} 2s, & \text{if } G_B = PGL(2, q)_B \rtimes \langle \tau_\alpha \rangle \\ s, & \text{if } G_B = PSL(2, q)_B \rtimes \langle \tau_\alpha \rangle \\ 2, & \text{if } G_B = PGL(2, q)_B \rtimes H \\ 1, & \text{if } G_B = PSL(2, q)_B \rtimes H. \end{cases}$$

As far as condition (\bar{A}) is concerned, we may argue exactly as in the earlier case $N = G$. Therefore, only condition (\bar{B}) has to be examined, and we may argue, mutatis mutandis, as for condition (B^*) to prove that here $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 5-design \mathcal{D} . Finally, let us

assume that $\langle \tau_\alpha \rangle \leq P\Gamma L(2, q)_{0B}$. Then, $G = P\Gamma L(2, q)$ and, by Dedekind's law, we can write

$$G_{0B} = \begin{cases} PGL(2, q)_{0B} \rtimes \langle \tau_\alpha \rangle, \text{ or} \\ PSL(2, q)_{0B} \rtimes \langle \tau_\alpha \rangle. \end{cases}$$

Hence, Remark 12 yields

$$(q-2)(q-3) \cdot \begin{cases} |PGL(2, q)_{0B}| \\ |PSL(2, q)_{0B}| \end{cases} \cdot |\langle \tau_\alpha \rangle| = (k-1)(k-2)(k-3)(k-4) |\langle \tau_\alpha \rangle|.$$

As $k = |0^{G_B}| = [G_B : G_{0B}]$, we obtain more precisely

(i) for $G_{0B} = PGL(2, q)_{0B} \rtimes \langle \tau_\alpha \rangle$:

$$2(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k}, \text{ or}$$

(ii) for $G_{0B} = PSL(2, q)_{0B} \rtimes \langle \tau_\alpha \rangle$:

$$(q-2)(q-3) |PSL(2, q)_{0B}| = (k-1)(k-2)(k-3)(k-4)$$

$$\text{with } |PSL(2, q)_{0B}| = \frac{|PSL(2, q)_B|}{k} \cdot \begin{cases} 2, & \text{if } G_B = PGL(2, q)_B \rtimes \langle \tau_\alpha \rangle \\ 1, & \text{if } G_B = PSL(2, q)_B \rtimes \langle \tau_\alpha \rangle. \end{cases}$$

Again, we may argue here exactly as in the earlier case $N = G$, and the claim follows.

Case (3): $N = M_v$, $v = 11, 12, 22, 23, 24$.

If $v = 12$ or 24 , then $G = M_v$ is always 5-transitive, and thus [35, Thm. 3] yields the designs described in Main Theorem 3. Obviously, flag-transitivity holds as the 5-transitivity of G implies that G_x acts block-transitively on the derived Steiner 4-design \mathcal{D}_x for any $x \in X$. By Corollary 11, we obtain for $v = 11$ that $k \leq 6$, and for $v = 22$ or 23 that $k \leq 8$, and the very small number of cases for k can easily be ruled out by hand using Lemma 8.

Case (4): $N = M_{11}$, $v = 12$.

As it is known, this exceptional permutation action occurs inside the Mathieu group M_{24} in its action on 24 points. This set can be partitioned into two sets X_1 and X_2 of 12 points each such that the setwise stabilizer of X_1 is the Mathieu group M_{12} . The stabilizer in this latter group of a point x in X_1 is isomorphic to M_{11} and operates (apart from its natural 4-transitive action on $X_1 \setminus \{x\}$) 3-transitively on the 12 points of X_2 . The geometry preserved by the 3-transitive action of M_{11} is not a Steiner t -design, but a 3-(12, 6, 2) design (e.g. [4, Ch. IV, 5.3]).

This completes the proof of Main Theorem 3.

Chapter 7

The Non-Existence of Flag-transitive Steiner 6-Designs

We prove the following result:

Main Theorem 4. *There are no non-trivial Steiner 6-designs \mathcal{D} admitting a flag-transitive group $G \leq \text{Aut}(\mathcal{D})$ of automorphisms.*

7.1 Groups of Automorphisms of Affine Type

In the following, we begin with the proof of Main Theorem 4. Using the notation as before, let us assume that $\mathcal{D} = (X, \mathcal{B}, I)$ is a non-trivial Steiner 6-design with $G \leq \text{Aut}(\mathcal{D})$ acting flag-transitively on \mathcal{D} . We will examine in this section successively those cases where G is of affine type.

Case (1): $G \cong \text{AGL}(1, 8)$, $\text{AGL}(1, 8)$ or $\text{AGL}(1, 32)$.

As trivial Steiner 5-designs are excluded, we may assume that $k > 6$. If $v = 8$, then Corollary 11 implies that $k = 6$, which is impossible with regard to Lemma 9 (c). For $v = 32$, we have $|G| = 5v(v - 1)$ and Lemma 8 immediately implies that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 6-design \mathcal{D} .

Case (2): $G_0 \cong SL(d, 2)$, $d \geq 2$.

Using the same notation as in Chapter 6, we will prove by contradiction that $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 6-design \mathcal{D} . To exclude trivial Steiner 6-designs, let $v = 2^d > k > 6$. For $d = 3$, we have $v = 8$ and $k = 7$ by Corollary 11, which is not possible in view of Lemma 9 (c). So, we may assume that $d > 3$. We remark that clearly any six distinct points are non-coplanar in $AG(d, 2)$ and hence generate an affine subspace of dimension at least 3. Let $\mathcal{E} = \langle e_1, e_2, e_3 \rangle$ denote the 3-dimensional vector subspace spanned by e_1, e_2, e_3 . Then again $SL(d, 2)_{\mathcal{E}}$, and hence also $G_{0, \mathcal{E}}$, acts point-transitively on $V \setminus \mathcal{E}$. If the unique block $B \in \mathcal{B}$ which is incident with the 6-subset $\{0, e_1, e_2, e_3, e_1 + e_2, e_2 + e_3\}$ contains some point outside \mathcal{E} , then it would already contain all points of $V \setminus \mathcal{E}$. But then, we would have $k \geq 2^d - 8 + 6 = 2^d - 2$, a contradiction to Corollary 11. Therefore, B lies entirely in \mathcal{E} , and by the flag-transitivity of G , it follows that each block must be contained in a 3-dimensional affine subspace. Hence, obviously $k \leq 8$. But, on the other hand, for \mathcal{D} to be a block-transitive 6-design admitting $G \leq \text{Aut}(\mathcal{D})$, we deduce from [13, Prop. 3.6 (b)] the necessary condition that $2^d - 3$ must divide $\binom{k}{4}$, and hence it follows for each respective value of k that $d = 3$, contradicting our assumption.

Case (3): $G_0 \cong A_7$, $v = 2^4$.

As $v = 2^4$, we have $k \leq 8$ by Corollary 11. But, Lemma 9 (c) obviously eliminates the cases when $k = 7$ or 8.

7.2 Groups of Automorphisms of Almost Simple Type

Maintaining the same notation, let us assume that $\mathcal{D} = (X, \mathcal{B}, I)$ is a non-trivial Steiner 6-design with $G \leq \text{Aut}(\mathcal{D})$ acting flag-transitively on \mathcal{D} . We will examine in this section successively those cases where G is of almost simple type.

Case (1): $N = A_v$, $v \geq 5$.

As trivial Steiner 6-designs are excluded, we may assume that $v \geq 8$. But then A_v , and hence also G , is 6-transitive and does not act on any non-trivial Steiner 6-design \mathcal{D} due to [35, Thm. 3].

Case (2): $N = PSL(2, q)$, $v = q + 1$, $q = p^e > 3$.

For the existence of flag-transitive Steiner 6-designs, necessarily

$$r = \frac{q(q-1)(q-2)(q-3)(q-4)}{(k-1)(k-2)(k-3)(k-4)(k-5)} \mid |G_0| \mid |P\Gamma L(2, q)_0| = q(q-1)e$$

must hold in view of Lemma 8. Thus, we have in particular

$$(q-2)(q-3)(q-4) \mid (k-1)(k-2)(k-3)(k-4)(k-5)e, \text{ where } e \leq \log_2 q. \quad (7.1)$$

But, on the other hand, Corollary 11 yields $k \leq \lfloor \sqrt{q+1} + \frac{9}{2} \rfloor < q^{\frac{1}{2}} + 5$. Hence, in view of property (7.1), we have only a small number of possibilities to check, which can easily be ruled out by hand using Lemma 9 (c). Therefore, $G \leq \text{Aut}(\mathcal{D})$ cannot act flag-transitively on any non-trivial Steiner 6-design \mathcal{D} . This has also been proven in [13, Cor. 4.3], whereas our estimation is slightly better.

Case (3): $N = M_v$, $v = 11, 12, 22, 23, 24$.

Due to Corollary 11, we obtain for $v = 11$ or 12 that $k \leq 7$, and for $v = 22, 23$ or 24 that $k \leq 9$, and the very small number of cases for k can easily be eliminated by hand using Lemma 8.

Case (4): $N = M_{11}$, $v = 12$.

By the same arguments as in the corresponding case in Main Theorem 3, it follows that $G \leq \text{Aut}(\mathcal{D})$ cannot act on any Steiner t -design \mathcal{D} .

This completes the proof of Main Theorem 4.

Acknowledgment

I gratefully acknowledge support by the Deutsche Forschungsgemeinschaft (DFG-grant Hu954/1-1;1-2;1-3). Furthermore, I thank C. Hering and W. M. Kantor for helpful conversations.

Bibliography

- [1] W. O. Alltop, *5-designs in affine spaces*, Pacific J. Math. **39** (1971), 547–551.
- [2] M. Aschbacher, *Chevalley groups of type G_2 as the group of a trilinear form*, J. Algebra **109** (1987), 193–259.
- [3] R. Baer, *Polarities in finite projective planes*, Bull. Amer. Math. Soc. **52** (1946), 77–93.
- [4] Th. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Vol. I and II, Encyclopedia of Math. and Its Applications **69/78**, Cambridge Univ. Press, Cambridge, 1999.
- [5] F. Beukers, *On the generalized Ramanujan-Nagell equation, I*, Acta Arith. **38** (1980/81), 389–410.
- [6] R. E. Block, *Transitive groups of collineations on certain designs*, Pacific J. Math. **15** (1965), 13–18.
- [7] F. Buekenhout, A. Delandtsheer, and J. Doyen, *Finite linear spaces with flag-transitive groups*, J. Combin. Theory, Series A **49** (1988), 268–293.
- [8] 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.
- [9] P. J. Cameron, *Parallelisms of Complete Designs*, London Math. Soc. Lecture Note Series **23**, Cambridge Univ. Press, Cambridge, 1976.
- [10] ———, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

- [11] P. J. Cameron and W. M. Kantor, *2-transitive and anti-flag transitive collineation groups of finite projective and polar spaces*, J. Algebra **60** (1979), 384–422.
- [12] P. J. Cameron, H. R. Maimani, G. R. Omidi, and B. Tayfeh-Rezaie, *3-designs from $PSL(2, q)$* , submitted.
- [13] P. J. Cameron and C. E. Praeger, *Block-transitive t -designs, II: large t* , in: Finite Geometry and Combinatorics (Deinze 1992), ed. by F. De Clerck et al., London Math. Soc. Lecture Note Series **191**, Cambridge Univ. Press, Cambridge, 1993, 103–119.
- [14] R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Ginn, Boston, 1937; Reprint: Dover Publications, New York, 1956.
- [15] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.
- [16] C. W. Curtis, W. M. Kantor, and G. M. Seitz, *The 2-transitive permutation representations of the finite Chevalley groups*, Trans. Amer. Math. Soc. **218** (1976), 1–59.
- [17] A. Delandtsheer, *Finite (line, plane)-flag-transitive planar spaces*, Geom. Dedicata **41** (1992), 145–153.
- [18] ———, *Dimensional linear spaces*, in: Handbook of Incidence Geometry, ed. by F. Buekenhout, Elsevier Science, Amsterdam, 1995, 193–294.
- [19] ———, *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.
- [20] 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.
- [21] P. Dembowski, *Finite Geometries*, Springer, Berlin, Heidelberg, New York, 1968; Reprint: Springer, 1997.
- [22] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901; Reprint: Dover Publications, New York, 1958.

- [23] D. A. Foulser, *The flag-transitive collineation groups of the finite desarguesian affine planes*, *Canad. J. Math.* **16** (1964), 443–472.
- [24] ———, *Solvable flag-transitive affine groups*, *Math. Z.* **86** (1964), 191–204.
- [25] D. Gorenstein, *Finite Simple Groups. An Introduction to Their Classification*, Plenum Publishing Corp., New York, London, 1982.
- [26] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*, *Geom. Dedicata* **2** (1974), 425–460.
- [27] ———, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II*, *J. Algebra* **93** (1985), 151–164.
- [28] D. G. Higman and J. E. McLaughlin, *Geometric ABA-groups*, *Illinois J. Math.* **5** (1961), 382–397.
- [29] M. Huber, *Classification of flag-transitive Steiner quadruple systems*, *J. Combin. Theory, Series A* **94** (2001), 180–190.
- [30] ———, *The classification of flag-transitive Steiner 3-designs*, *Adv. Geom.* **5** (2005), 195–221.
- [31] ———, *The classification of flag-transitive Steiner 4-designs*, submitted (2005), 34 pages.
- [32] ———, *On highly symmetric combinatorial designs*, submitted (2005), 31 pages.
- [33] B. Huppert, *Zweifach transitive, auflösbare Permutationsgruppen*, *Math. Z.* **68** (1957), 126–150.
- [34] ———, *Endliche Gruppen I*, Springer, Berlin, Heidelberg, New York, 1967.
- [35] W. M. Kantor, *Homogeneous designs and geometric lattices*, *J. Combin. Theory, Series A* **38** (1985), 66–74.
- [36] ———, *Flag-transitive planes*, in: *Finite Geometries* (Winnipeg, Can., 1984), ed. by C. A. Baker and L. M. Batten, *Lecture Notes in Pure and Applied Math.* **103**, Dekker, New York, 1985, 179–181.

- [37] ———, *Primitive permutation groups of odd degree, and an application to finite projective planes*, J. Algebra **106** (1987), 15–45.
- [38] ———, *2-transitive and flag-transitive designs*, in: Coding Theory, Design Theory, Group Theory, Proc. Marshall Hall Conf. (Burlington, VT, 1990), ed. by D. Jungnickel et al., J. Wiley, New York, 1993, 13–30.
- [39] P. B. Kleidman, *The finite flag-transitive linear spaces with an exceptional automorphism group*, in: Finite Geometries and Combinatorial Designs (Lincoln, NE, 1987), ed. by E. S. Kramer and S. S. Magliveras, Contemp. Math. **111**, Amer. Math. Soc., Providence, RI, 1990, 117–136.
- [40] 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.
- [41] M. W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. (3) **54** (1987), 477–516.
- [42] ———, *The classification of finite linear spaces with flag-transitive automorphism groups of affine type*, J. Combin. Theory, Series A **84** (1998), 196–235.
- [43] D. Livingstone and A. Wagner, *Transitivity of finite permutation groups on unordered sets*, Math. Z. **90** (1965), 393–403.
- [44] H. Lüneburg, *Fahnenhomogene Quadrupelsysteme*, Math. Z. **89** (1965), 82–90.
- [45] E. Maillet, *Sur les isomorphes holoédriques et transitifs des groupes symétriques ou alternés*, J. Math. Pures Appl. (5) **1** (1895), 5–34.
- [46] D. K. Ray-Chaudhuri and R. M. Wilson, *On t -designs*, Osaka J. Math. **12** (1975), 737–744.
- [47] J. Saxl, *On finite linear spaces with almost simple flag-transitive automorphism groups*, J. Combin. Theory, Series A **100** (2002), 322–348.
- [48] M. Suzuki, *On a class of doubly transitive groups*, Ann. Math. (2) **75** (1962), 105–145.

- [49] H. N. Ward, *On Ree's series of simple groups*, Trans. Amer. Math. Soc. **121** (1966), 62–89.
- [50] E. Witt, *Die 5-fach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg **12** (1938), 256–264.
- [51] ———, *Über Steinersche Systeme*, Abh. Math. Sem. Univ. Hamburg **12** (1938), 265–275.
- [52] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. für Math. u. Phys. **3** (1892), 265–284.