Klassifikationen fahnentransitiver Steiner Designs

DISSERTATION

der Mathematischen Fakultät
der Eberhard-Karls-Universität Tübingen
zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von
MICHAEL HUBER
aus Geislingen

2001

Tag der mündlichen Prüfung:	06. Juli 2001
Dekan:	Prof. Dr. Ch. Lubich
1. Berichterstatter:	Prof. Dr. Ch. Hering
2. Berichterstatter:	Prof. Dr. W. Knapp

Inhaltsverzeichnis

Einleitung **3**

Notation **7**

1 Grundlagen **9**
1.1 Inzidenzstrukturen und Steiner Designs 9
1.2 Endliche zweifach transitive Permutationsgruppen 12
1.3 Der Satz von Zsigmondy 16

2 Fahnentransitive Steiner Designs **19**
2.1 Eigenschaften 19
2.2 Beispiele 20

3 Fahnentransitive Steinerquadrupelsysteme **25**
3.1 Steinerquadrupelsysteme 25
3.2 Klassifikation 27

4 Fahnentransitive Steiner 3-Designs **39**
4.1 Projektive Automorphismengruppe 39
4.2 Automorphismengruppe vom Typ affin 43
4.3 Klassifikation bei kleinen Blöcken 49

Literaturverzeichnis **55**

Lebenslauf **59**

Einleitung

In den letzten Jahrzehnten wurden mit großem Interesse $t-(v,k,\lambda)$ Designs mit gewissen Transitivitätseigenschaften klassifiziert. Dabei beschränkte man sich meist auf die Betrachtung des Falles $\lambda = 1$. Häufig spricht man hierbei auch von *Steinersystemen* oder *Steiner Designs*. Beispielsweise charakterisierte Kantor [32] alle 2-fach punkttransitiven $2-(v,k,1)$ Designs. Wenige Jahre später gelang Buekenhout et al. [9] eine Klassifikation aller fahnentransitiven $2-(v,k,1)$ Designs. Beide Resultate benötigen die Klassifikation der endlichen einfachen Gruppen.

Für $3-(v,k,1)$ Designs hingegen ist es bisher noch nicht gelungen, Klassifikationen mit obigen Transitivitätseigenschaften zu erreichen:
Die Klassifikation fahnentransitiver $3-(v,k,1)$ Designs ist ein „still open and longstanding problem" und die der 2-fach punkttransitiven erscheint sogar als hoffnungslos (siehe [16] und [17, S. 273]).

In der vorliegenden Arbeit werden wir alle fahnentransitiven $3-(v,k,1)$ Designs für kleine Parameter k klassifizieren. Dabei benutzen wir die Klassifikation der endlichen 2-fach transitiven Permutationsgruppen.
Für $k = 4$ erhalten wir genau eines der folgenden Designs $\mathcal{D}$ mit ihrer zugehörigen fahnentransitiven Automorphismengruppe G:

(1) *$\mathcal{D}$ ist isomorph zum $3-(2^d,4,1)$ Design, bestehend aus den Punkten und Ebenen von $AG(d,2)$, und es tritt einer der folgenden Fälle auf:*

- (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 $G \cong A\Gamma L(1,32)$,*

(2) *$\mathcal{D}$ ist isomorph zu einem* $3-(3^d+1,4,1)$ *Design, dessen Punkte die Elemente von* $GF(3^d)\cup\{\infty\}$ *und dessen Blöcke die Bilder von* $GF(3)\cup\{\infty\}$ *unter* $PGL(2,3^d)$ *mit* $d\geq 2$ *(resp.* $PSL(2,3^d)$ *mit* $d>1$ *ungerade) sind, und das abgeleitete Design ist isomorph zum* $2-(3^d,3,1)$ *Design, bestehend aus den Punkten und Geraden von* $AG(d,3)$*, und* $PSL(2,3^d)\leq G\leq P\Gamma L(2,3^d)$*,*

(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* $\{0,1,\infty,\varepsilon\}$ *unter* $PSL(2,q)$ *sind, wobei* ε *eine primitive sechste Einheitswurzel in* $GF(q)$ *ist, und das abgeleitete Design ist isomorph zum Nettotripelsystem, und* $PSL(2,q)\leq G\leq P\Sigma L(2,q)$*.*

Für $k=5$ ergeben sich lediglich die (analog zu den unter (2) beschriebenen) Kreisgeometrien über $GF(4)$. Im Fall $k=6$ tritt neben den Kreisgeometrien über $GF(5)$ das Witt $3-(22,6,1)$ Design mit $G\trianglerighteq M_{22}$ als fahnentransitiver Automorphismengruppe auf. Für $k=7$ existieren hingegen keine fahnentransitiven Designs.

Im ersten Kapitel legen wir die Grundlagen für unser weiteres Vorgehen: Wir führen wichtige kombinatorische Eigenschaften von Designs ein, geben die Klassifikation der endlichen 2-fach transitiven Permutationsgruppen an und stellen einige zahlentheoretische Hilfsmittel, insbesondere den Satz von Zsigmondy, zur Verfügung.

Im darauf folgenden Kapitel beweisen wir, dass für $3-(v,k,1)$ Designs die Fahnentransitivität der Automorphismengruppe bereits deren 2-fache Punkttransitivität impliziert (Korollar 2.3). Dieser Sachverhalt folgt aus dem bekannten Satz von Block und ermöglicht uns, bei den nachfolgenden Klassifikationen die Klassifikation der endlichen 2-fach transitiven Permutationsgruppe zu verwenden. Des Weiteren geben wir einige Beispiele bekannter Designs mit ihren zugehörigen Automorphismengruppen an.

Im dritten Kapitel betrachten wir $3-(v,4,1)$ Designs. Diese werden häufig auch *Steinerquadrupelsysteme* genannt. Eine notwendige und hinreichende Bedingung für ihre Existenz gibt der Satz von Hanani an. Wir werden alle fahnentransitiven Steinerquadrupelsysteme klassifizieren (Theorem 3.4).

Unser Resultat verallgemeinert einen Satz von Lüneburg [38], der alle fahnentransitiven Steinerquadrupelsysteme charakterisiert unter der zusätzlichen starken Voraussetzung, dass jedes von der Identität verschiedene Element der Automorphismengruppe höchstens zwei Fixpunkte hat. Unsere Vorgehensweise wie auch unsere Beweise sind dabei unabhängig von Lüneburg. Bereits in [26] beschäftigten wir uns mit dieser Klassifikation. Die dort erzielten Ergebnisse wurden in ihrer Darstellung verbessert und die noch offen gebliebenen Fälle gelöst. Unser Resultat ist erschienen in [27]. Abschließend untersuchen wir als Sonderfall, wann eine fasteinfache Gruppe mit $PSL(2,q)$ als Normalteiler auf einem Steinerquadrupelsystem operiert (Satz 3.5).

Im letzten Kapitel werden wir die Fälle $k = 5, 6$ und 7 untersuchen. Dafür betrachten wir in den ersten beiden Abschnitten zunächst zwei Spezialfälle:
Zum einen setzen wir voraus, dass die Automorphismengruppe des $3-(v,k,1)$ Designs projektiv ist, zum anderen soll die Automorphismengruppe, abgesehen von der eindimensionalen affinen Gruppe, vom Typ affin sein. Für allgemeines k lässt sich jeweils eine vollständige Klassifikation der fahnentransitiven $3-(v,k,1)$ Designs angeben (Sätze 4.1 und 4.2). Daran anschließend geben wir notwendige Bedingungen an für die Existenz fahnentransitiver $3-(v,k,1)$ Designs deren Automorphismengruppe eine der Gruppen $PSU(3,q^2)$, ${}^2G_2(q)$ oder $Sz(q)$ enthält (Propositionen 4.3 bis 4.5). Mittels gruppentheoretischer und kombinatorischer Argumente lassen sich dann alle fahnentransitiven $3-(v,k,1)$ Designs mit den Blockgrößen $k = 5, 6$ und 7 klassifizieren (Theoreme 4.6 bis 4.8).

Ich möchte mich ganz herzlich bei Herrn Prof. Dr. Ch. Hering bedanken für die sehr gute Betreuung der vorliegenden Dissertation. Seine Anregungen sowie die zahlreichen persönlichen Gespräche waren mir stets eine große Hilfe.

Notation

$\mathbb{N}$	Menge der natürlichen Zahlen $\{1, 2, ...\}$
$\mathbb{Q}$	Körper der rationalen Zahlen
$\mathbb{Q}[t]$	Ring der Polynome über $\mathbb{Q}$
$GF(q)$	endlicher Körper der Mächtigkeit q
$GF(q)^*$	multiplikative Gruppe des Körpers $GF(q)$
$\mathrm{Aut}(GF(q))$	Gruppe der Körperautomorphismen
V	Vektorraum über $GF(q)$
$GL(V)$	Gruppe der invertierbaren linearen Abbildungen von V
$\Gamma L(V)$	Gruppe der invertierbaren semilinearen Abbildungen von V
$V(d, q)$	d-dimensionaler Vektorraum über $GF(q)$
$AG(d, q)$	d-dimensionaler affiner Raum über $GF(q)$
$PG(d, q)$	d-dimensionaler projektiver Raum über $GF(q)$
$\mathrm{Aut}(G)$	Automorphismengruppe von G
$\mathrm{Out}(G)$	äußere Automorphismengruppe von G
$[G : H]$	Index der Untergruppe H in G
$\mathrm{Syl}_p(G)$	Menge der p-Sylowuntergruppen von G
C_n	zyklische Gruppe der Ordnung n
S_n, A_n	symmetrische und alternierende Gruppe vom Grad n
$AGL(d, q), ASL(d, q), A\Gamma L(d, q)$	affine Gruppen über $GF(q)$
$PGL(d, q), PSL(d, q), P\Gamma L(d, q)$	projektive Gruppen über $GF(q)$
$Sp(2d, q)$	symplektische Gruppen über $GF(q)$
$PGU(d, q), PSL(d, q), P\Gamma L(d, q)$	projektive unitäre Gruppen über $GF(q)$
(a, b)	größter gemeinsamer Teiler von $a, b \in \mathbb{N}$
$a \mid b,\ a \nmid b$	a ist ein, kein Teiler von b
$r \perp q^d - 1$	r teilt $q^d - 1$, aber nicht $q^a - 1$ für alle $1 \leq a < d$
$[a]$	größte ganze Zahl kleiner oder gleich a
$\lvert M \rvert$	Mächtigkeit der endlichen Menge M

Kapitel 1

Grundlagen

1.1 Inzidenzstrukturen und Steiner Designs

In diesem Abschnitt stellen wir die für unsere Arbeit notwendigen designtheoretischen Grundlagen bereit. Für eine umfassende Einführung in die Theorie der endlichen Geometrien und Designs seien die Werke von Beth, Jungnickel und Lenz [4], Beutelspacher [6], Dembowski [19] sowie von Hughes und Piper [28] empfohlen.

Eine *Inzidenzstruktur* ist ein Tripel $\mathcal{I} = (X, \mathcal{B}, I)$ von Mengen mit

$$X \cap \mathcal{B} = \emptyset \text{ und } I \subseteq X \times \mathcal{B}.$$

Die Elemente von X nennen wir *Punkte*, die von $\mathcal{B}$ heißen *Blöcke* und die von I werden *Inzidenzen* oder auch *Fahnen* genannt. Wir werden Punkte mit kleinen und Blöcke mit großen lateinischen Buchstaben bezeichnen. Anstatt „(x, B) ist eine Fahne" werden wir in der Regel „x inzidiert mit B" sagen. Für eine gegebene Inzidenzstruktur kann man die Rolle der Punkte und Blöcke vertauschen, sodass sich eine neue Inzidenzstruktur ergibt, wobei sich die ursprüngliche Inzidenzrelation umkehrt. Diese nennen wir die *duale* Inzidenzstruktur.

Wir beschränken uns auf *endliche* Inzidenzstrukturen; dies bedeutet dass X und $\mathcal{B}$, und daher auch I, stets endliche Mengen sind. Üblicherweise setzen wir $v := |X|$ und $b := |\mathcal{B}|$.

Definition 1.1. Seien $\mathcal{I}_1 = (X_1, \mathcal{B}_1, I_1)$ und $\mathcal{I}_2 = (X_2, \mathcal{B}_2, I_2)$ zwei Inzidenzstrukturen. Eine bijektive Abbildung

$$\alpha : X_1 \cup \mathcal{B}_1 \longrightarrow X_2 \cup \mathcal{B}_2$$

heißt *Isomorphismus* von $\mathcal{I}_1$ auf $\mathcal{I}_2$, falls gilt:

(i) für $x \in X_1$ und $B \in \mathcal{B}_1$ gilt $x^\alpha \in X_2$ und $B^\alpha \in \mathcal{B}_2$ (d. h.: α bildet Punkte auf Punkte und Blöcke auf Blöcke ab),

(ii) für alle Punkte x und alle Blöcke B von $\mathcal{I}_1$ gilt:

$$(x, B) \in I_1 \Longleftrightarrow (x^\alpha, B^\alpha) \in I_2.$$

Zwei Inzidenzstrukturen $\mathcal{I}_1$ und $\mathcal{I}_2$ nennen wir *isomorph*, wenn es einen Isomorphismus von $\mathcal{I}_1$ auf $\mathcal{I}_2$ gibt. Einen Isomorphismus von $\mathcal{I}_1$ auf sich heißt *Automorphismus* von $\mathcal{I}_1$. Offensichtlich bilden alle Automorphismen einer Inzidenzstruktur bezüglich der Hintereinanderausführung eine Gruppe, die *volle Automorphismengruppe* der Inzidenzstruktur.

Für natürliche Zahlen $t \leq k \leq v$ und λ nennen wir eine Inzidenzstruktur $\mathcal{D} = (X, \mathcal{B}, I)$ ein $t - (v, k, \lambda)$ *Design*, falls jeder Block $B \in \mathcal{B}$ mit k Punkten inzidiert und jede t-elementige Teilmenge von X mit λ Blöcken inzidiert.
Ein $t - (v, k, 1)$ Design werden wir auch *Steiner t-Design* nennen (vgl. beispielsweise [5]). Man spricht in der Literatur hierbei häufig auch von *Steinersystemen*, wenn klar ist, um welchen Parameter t es sich handelt. Wir bemerken, dass für $\lambda = 1$ jeder Block eindeutig bestimmt ist durch die Menge der Punkte, mit denen er inzidiert.

Für beliebiges $x \in X$ definieren wir das *abgeleitete Design* $\mathcal{D}_x = (X_x, \mathcal{B}_x, I_x)$ bezüglich x mit $X_x := X \setminus \{x\}$, $\mathcal{B}_x := \{B \in \mathcal{B} : (x, B) \in I\}$ und $I_x := I|_{X_x \times \mathcal{B}_x}$. Wir bezeichnen $\mathcal{D}$ dann auch als *Erweiterung* von $\mathcal{D}_x$. Offensichtlich ist ein abgeleitetes Design ein $(t-1) - (v-1, k-1, \lambda)$ Design.

Für eine natürliche Zahl $s \leq t$ wählen wir eine s-elementige Teilmenge von X. Sei λ_s die Anzahl der Blöcke $B \in \mathcal{B}$, welche mit jedem Element dieser Teilmenge inzidieren. Via Konvention setzt man $r := \lambda_1$. Durch doppeltes Abzählen erhalten wir

$$\binom{k-s}{t-s} \lambda_s = \lambda \binom{v-s}{t-s}.$$

Damit lassen sich für $t-(v,k,\lambda)$ Designs mit vorgegebenen Parametern t, v, k und λ die Parameter b und r leicht berechnen:

Lemma 1.2. *Falls $(X,\mathcal{B},I)$ ein $t-(v,k,\lambda)$ Design mit $t \geq 1$ ist, dann gilt:*

(a) $bk = vr$.

(b) $\binom{v}{t}\lambda = b\binom{k}{t}$.

(c) $r(k-1) = \lambda_2(v-1)$ *für* $t \geq 2$.

(d) *Falls $t = 3$ ist, dann gilt $(k-2)\lambda_2 = v-2$, insbesondere also $k-2 \mid v-2$.*

Für Steiner t-Designs ergeben sich mithilfe der Parameter t und k untere Schränken für v (siehe [10, Theoreme 3A.4 und 3A.5]):

Satz 1.3. (Cameron). *Falls $t > 2$ und $v > k$ ist, dann gilt für $t-(v,k,1)$ Designs*

$$v - t + 1 \geq (k-t+2)(k-t+1).$$

Satz 1.4. (Cameron). *Falls $v > k$ ist, dann gilt für $t-(v,k,1)$ Designs*

$$v \geq (t+1)(k-t+1).$$

Der erste Satz ist stärker für $k > 2(t-1)$, der zweite für $k < 2(t-1)$. Für $k = 2(t-1)$ ergeben beide $v \geq t^2 - 1$.

Falls $t = 3$ ist, dann erhalten wir aus Satz 1.3 durch einfaches Rechnen die folgende Abschätzung für k, die wir des Öfteren benötigen werden.

Korollar 1.5. *Für nicht-triviale $3-(v,k,1)$ Designs gilt*

$$k \leq \left[\sqrt{v} + \tfrac{3}{2}\right].$$

1.2 Endliche zweifach transitive Permutationsgruppen

In der vorliegenden Arbeit werden stets *endliche* Gruppen betrachtet. Für weiterführende Literatur verweisen wir auf Huppert [30], Huppert und Blackburn [31] sowie auf Kurzweil und Stellmacher [34].

Wir führen zunächst einige grundlegende Bezeichnungen der Gruppentheorie ein. Sei $\mathrm{Sym}(X)$ die Menge aller Permutationen der nicht-leeren, endlichen Menge X. Bezüglich der Hintereinanderausführung ist $\mathrm{Sym}(X)$ eine Gruppe, die *symmetrische Gruppe* auf X. Für $g \in G \leq \mathrm{Sym}(X)$ bezeichne $\mathrm{fix}(g)$ die *Fixpunktmenge* und $\mathrm{supp}(g)$ den *Träger* von g.

Eine Gruppe G *operiert* (oder: *wirkt*) auf X, falls jedem $g \in G$ eine Permutation $x \mapsto x^g$ von X zugeordnet ist, sodass gilt:

(i) $x^1 = x$ für alle $x \in X$ (wobei 1 das Neutralelement von G bezeichnet),

(ii) $(x^g)^h = x^{gh}$ für alle $x \in X$ und alle $g, h \in G$.

Dies ist offenbar genau dann der Fall, wenn die Abbildung

$$\varphi : g \mapsto (x \mapsto x^g)$$

von G in $\mathrm{Sym}(X)$ ein Homomorphismus ist. Ist $\ker \varphi = 1$, dann operiert G *treu* auf X; in diesem Fall heißt G eine *Permutationsgruppe* auf X. Ist hingegen $\ker \varphi = G$, also $x^g = x$ für alle $x \in X$ und alle $g \in G$, dann operiert G *trivial* auf X. Mit $|X|$ bezeichnen wir den *Grad* von G.

Definition 1.6. Sei G resp. G' eine Permutationsgruppe, die auf der Menge X resp. X' wirkt. Wir nennen G und G' *permutationsisomorph*, falls es einen Gruppenisomorphismus $\sigma : G \longrightarrow G'$ und eine Bijektion $\tau : X \longrightarrow X'$ gibt, sodass

$$(x^g)^\tau = (x^\tau)^{(g^\sigma)}$$

gilt für alle $x \in X$ und alle $g \in G$.

Für $x \in X$ bezeichnet die Untergruppe

$$G_x := \{g \in G : x^g = x\}$$

den *(Punkt-)Stabilisator* von x in G und die Menge

$$x^G := \{x^g : g \in G\}$$

die *Bahn* von x unter G. Die Anzahl der Elemente einer Bahn heißt die *Länge* der Bahn. Für $M \subseteq X$ nennen wir die Untergruppe

$$G_M := \{g \in G : M^g = M\}$$

den *globalen Stabilisator* von M in G; die Untergruppe

$$G_{(M)} := \bigcap_{x \in M} G_x$$

hingegen lässt die Menge M punktweise fest. Für $M = \{x, y\}$ schreiben wir hierfür auch $G_{x,y}$.

Eine Permutationsgruppe G operiert *transitiv* auf X, falls G nur eine Bahn besitzt, also $x^G = X$ gilt für alle $x \in X$. Äquivalent dazu ist, dass für jedes Punktepaar $x, y \in X$ stets ein $g \in G$ existiert, so daß $x^g = y$ gilt.
G operiert *regulär* auf X, falls G transitiv auf X operiert und falls $G_x = 1$ gilt für ein $x \in X$.
Für $t \in \mathbb{N}$ heißt G *t-fach transitiv*, wenn für je zwei injektive t-Tupel $(x_1, x_2, ..., x_t)$ und $(y_1, y_2, ..., y_t)$ ein $g \in G$ existiert, sodass ${x_i}^g = y_i$ gilt für alle $i = 1, 2, ..., t$.
G heißt *t-fach homogen*, falls es zu je zwei t-elementigen Teilmengen M und M' von X ein $g \in G$ gibt mit

$$M' = M^g (= \{m^g : m \in M\}).$$

Insbesondere ist jede t-fach transitive Permutationsgruppe auch t-fach homogen.

Grundlegend ist die folgende elementare Aussage (vgl. beispielsweise [34, Satz 3.1.5]):

Satz 1.7. (Bahnenformel). *Für jedes $x \in X$ gilt*

$$|x^G| = |G : G_x| \ .$$

Insbesondere ist die Länge einer Bahn x^G stets ein Teiler von $|G|$.

In unserer Arbeit geht entscheidend die Klassifikation der endlichen 2-fach transitiven Permutationsgruppen ein. Diese wiederum beruht auf der Klassifikation aller endlichen einfachen Gruppen (vgl. hierzu Gorenstein [21], Hering [24], Huppert [29], und Curtis, Seitz und Kantor [15].)

Wir führen alle 2-fach transitiven Permutationsgruppen an:

Theorem 1.8. *Sei G eine endliche 2-fach transitive Permutationsgruppe auf einer nicht-leeren Menge X. Dann gilt entweder*

(A) Typ affin: *G enthält einen regulären elementar-abelschen Normalteiler T der Ordnung $v = p^d$, wobei p eine Primzahl ist. Wenn a ein Teiler von d ist und wenn wir G mit einer Gruppe von affinen Abbildungen*

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

von $V := V(d,p)$ mit $g \in G_0$ und $u \in V$, identifizieren, dann tritt insbesondere einer der folgenden Fälle auf:

(1) $G \leq A\Gamma L(1, p^d)$

(2) $G_0 \trianglerighteq SL(\frac{d}{a}, p^a)$, $d \geq 2a$

(3) $G_0 \trianglerighteq Sp(\frac{2d}{a}, p^a)$, $d \geq 2a$

(4) $G_0 \trianglerighteq G_2(2^a)'$, $d = 6a$

(5) $G_0 \cong A_6$ *oder* A_7, $v = 2^4$

(6) $G_0 \trianglerighteq SL(2,3)$ *oder* $SL(2,5)$, $v = p^2$, $p = 5, 7, 11, 19, 23, 29$ *oder* 59, *oder* $v = 3^4$

(7) G_0 *enthält einen extraspeziellen Normalteiler* E *der Ordnung* 2^5, *und* G_0/E *ist isomorph zu einer Untergruppe von* S_5, $v = 3^4$

(8) $G_0 \cong SL(2,13)$, $v = 3^6$,

oder

(B) Typ fasteinfach: *G enthält einen einfachen Normalteiler N, und es gilt $N \leq G \leq \mathrm{Aut}(N)$. Insbesondere tritt einer der folgenden Fälle auf, wobei wir N und $v = |X|$ angeben:*

(1) A_v, $v \geq 5$

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

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

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

(5) ${}^2G_2(q)$, $v = q^3+1$, $q = 3^{2e+1} > 3$ (Ree Gruppe)

(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 nicht 2-fach transitiv)

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

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

(11) A_7, $v = 15$

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

(13) Co_3, $v = 276$ (Kleinste Conway Gruppe).

Bemerkung 1.9. Diesen Abschnitt abschließend werden wir einige Bezeichnungen einführen, auf die wir in den späteren Kapiteln zurückgreifen werden.

Sei q eine Primzahlpotenz. Bekanntlich gilt

$$\mathrm{Aut}(PSL(2,q)) = P\Gamma L(2,q),$$

$$\text{und } \mathrm{Aut}(PSL(d,q)) = P\Gamma L(d,q) \rtimes \langle \iota \rangle \text{ für } d \geq 3.$$

Mit ι bezeichnen wir dabei den durch die Abbildung, welche jeder regulären Matrix die Transponierte der Inversen zuordnet, induzierten Graphautomorphismus in der Terminologie der Gruppen vom Lie-Typ (vgl. [33, Proposition 2.2.3] und [12, Kap. 12]).

Für eine ungerade Primzahl p definieren wir

$$P\Sigma L(2,p^a) := PSL(2,p^a) \rtimes <\tau_\alpha>,$$

wobei τ_α die durch den Frobenius-Automorphismus $\alpha : GF(p^a) \longrightarrow GF(p^a)$, $x \mapsto x^p$ induzierte Abbildung $\tau_\alpha \in \mathrm{Sym}(GF(p^a) \cup \{\infty\}) \cong S_v$ der Ordnung a bezeichnet. Offensichtlich ist $P\Sigma L(2,p^a)$ eine Untergruppe von $P\Gamma L(2,p^a)$ vom Index 2.

1.3 Der Satz von Zsigmondy

In unserer Arbeit werden wir uns einiger zahlentheoretischer Hilfsmittel bedienen. Für $d \in \mathbb{N}$ sei $\Phi_d(t)$ das d-te Kreisteilungspolynom in $\mathbb{Q}[t]$ und für $2 \leq q \in \mathbb{N}$ sei

$$\Phi_d^*(q) := \frac{\Phi_d(q)}{f^\alpha},$$

wobei $f = (d, \Phi_d(q))$ und f^α die höchste Potenz von f ist, die in $\Phi_d(q)$ aufgeht (vgl. [24]).

Bemerkung 1.10. Aus der elementaren Zahlentheorie ist bekannt, dass für $2 \leq q \in \mathbb{N}$ das p-te Kreisteilungspolynom

$$\Phi_p(q) = \frac{q^p - 1}{q - 1} = \sum_{i=0}^{p-1} q^i$$

für eine Primzahl $p > 2$ nur für $q \equiv 1 \pmod p$ durch p teilbar ist, und dann auch lediglich in erster Potenz. Ferner ist jeder von p verschiedene Primteiler von $\Phi_p(q)$ von der Form $2pn + 1$ für ein $n \in \mathbb{N}$ (vgl. z. B. [1, S. 83 und 109]).

Sei q nun eine Potenz der Primzahl p und $V := V(d,q)$ ein Vektorraum der Dimension $d \geq 2$ über $GF(q)$.

Definition 1.11. Eine natürliche Zahl b heißt *q-primitiver Teiler* von $q^d - 1$, falls $b \mid q^d - 1$ und $(b, q^a - 1) = 1$ gilt für alle a mit $a \mid d$ und $1 \leq a < d$.

Es gilt der bekannte Satz von Zsigmondy (vgl. [23, Hilfssatz 3] oder [43, S. 283]):

Satz 1.12. (Zsigmondy). *Es besitzt $q^d - 1$ einen von 1 verschiedenen q-primitiven Teiler mit Ausnahme der Fälle*

$$d = 6 \;\; \textit{und} \;\; q = 2, \;\; \textit{bzw.} \;\; d = 2 \;\; \textit{und} \;\; q = 2^i - 1 \;\; \textit{für ein} \;\; i \in \mathbb{N}.$$

Lemma 1.13. *Es gelten die folgenden Aussagen:*

(a) *Ist b ein p-primitiver Teiler von $q^d - 1$, dann ist b ein q-primitiver Teiler von $q^d - 1$.*

(b) *Ist b ein q-primitiver Teiler von $q^d - 1$ und c ein Teiler von b, dann ist c ein q-primitiver Teiler von $q^d - 1$.*

(c) *Ist b ein q-primitiver Teiler von $q^d - 1$, dann gilt $b \equiv 1 \pmod{d}$.*

Beweis. Die Aussagen (a) und (b) sind sofort einsichtig. Teil (c) folgt aus [23, Hilfssatz 2]. □

Es ergibt sich in der p-modularen Darstellungstheorie ein Zusammenhang von q-primitiven Teilern von $q^d - 1$ mit irreduziblen Untergruppen von $GL(V)$ (vgl. [24, Theorem 3.5]):

Satz 1.14. (Hering). *Sei r eine Primzahl. Dann sind äquivalent:*

(a) $r \mid \Phi_d^*(q)$.

(b) $(r, q) = 1$ *und d ist die multiplikative Ordnung von q modulo r.*

(c) $r \mid q^d - 1$ *und r teilt nicht $q^a - 1$ für $1 \leq a < d$.*

(d) *r ist ein q-primitiver Teiler von $q^d - 1$.*

(e) *$GL(V)$ enthält nicht-triviale r-Gruppen, und jede nicht-triviale r-Gruppe in $GL(V)$ wirkt irreduzibel auf V.*

Kapitel 2

Fahnentransitive Steiner Designs

Sei im Folgenden $\mathcal{D} = (X, \mathcal{B}, I)$ ein $t-(v,k,1)$ Design und $G \leq \mathrm{Aut}(\mathcal{D})$ eine Automorphismengruppe von $\mathcal{D}$.

Wir nennen G *fahnentransitiv* (resp. *blocktransitiv*), falls G transitiv auf den Fahnen (resp. auf den Blöcken) von $\mathcal{D}$ operiert. Abkürzend heißt $\mathcal{D}$ *fahnentransitiv* (resp. *blocktransitiv, t-fach (punkt-)transitiv*), falls $\mathcal{D}$ eine fahnentransitive (resp. blocktransitive, t-fach (punkt-)transitive) Automorphismengruppe zulässt.

2.1 Eigenschaften

Lemma 2.1. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein $t-(v,k,1)$ Design und $x \in X$ beliebig. Falls $G \leq \mathrm{Aut}(\mathcal{D})$ fahnentransitiv auf $\mathcal{D}$ operiert, dann gilt die Teilungseigenschaft*

$$r \,\big|\, |G_x|\,,$$

das heißt, die Anzahl der Blöcke, welche mit einem beliebigen Punkt inzidieren, teilt stets die Ordnung des Punktstabilisators.

Beweis. Sei $x \in X$ beliebig. Da $G \leq \mathrm{Aut}(\mathcal{D})$ nach Voraussetzung fahnentransitiv auf $\mathcal{D}$ operiert, wirkt G_x transitiv auf den r Blöcken, welche mit $x \in X$ inzidieren. Somit bilden diese eine Bahn von G_x, und Satz 1.7 liefert die Behauptung. $\square$

Für Steiner t-Designs gilt die elementare Aussage, dass die 2-fache Punkttransitivität der Automorphismengruppe bereits deren Fahnentransitivität impliziert, falls $t = 2$ ist. Für $t \geq 3$ hingegen gilt interessanterweise die Umkehrung, wie sich leicht aus dem bekannten Satz von Block (vgl. [7, Theorem 2]) folgern lässt:

Satz 2.2. (Block). *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein $t-(v,k,1)$ Design. Falls $t \geq 2$ gilt und $G \leq \mathrm{Aut}(\mathcal{D})$ blocktransitiv auf $\mathcal{D}$ operiert, dann operiert G auch transitiv auf den Punkten von $\mathcal{D}$.*

Korollar 2.3. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein $t-(v,k,1)$ Design mit $t \geq 3$, und operiere $G \leq \mathrm{Aut}(\mathcal{D})$ fahnentransitiv auf $\mathcal{D}$. Dann operiert G auch 2-fach transitiv auf den Punkten von $\mathcal{D}$.*

Beweis. Sei $x \in X$ beliebig, und $G \leq \mathrm{Aut}(\mathcal{D})$ operiere fahnentransitiv auf $\mathcal{D}$. Offensichtlich wirkt dann G_x blocktransitiv auf dem abgeleiteten Steiner $(t-1)$-Design $\mathcal{D}_x$. Daher operiert G_x nach dem Satz von Block transitiv auf den Punkten von $\mathcal{D}_x$, und die Behauptung folgt. □

2.2 Beispiele

Wir werden im Folgenden einige Beispiele bekannter Steiner Designs mit ihren zugehörigen Automorphismengruppen anführen. In Beispiel 2.7 geben wir dabei ein Steiner 3-Design an mit einer 2-fach punkttransitiven, jedoch nicht fahnentransitiven Automorphismengruppe.

Sei q eine Primzahlpotenz.

Beispiel 2.4. (Projektive Räume).
Als Punktmenge X wählen wir die Menge der 1-dimensionalen Unterräume eines Vektorraums V der Dimension $d \geq 3$ über $GF(q)$. Als Blockmenge $\mathcal{B}$ wählen wir die 2-dimensionalen Unterräume von V. Dann haben wir $v = (q^d-1)/(q-1)$ Punkte und jeder Block $B \in \mathcal{B}$ enthält $k = q+1$ Punkte. Je zwei Punkte entsprechen zwei 1-dimensionalen Untervektorräumen und spannen dadurch eindeutig einen 2-dimensionalen Untervektorraum auf. Daher liegt jedes Paar verschiedener Punkte in genau einem Block. Somit ist der projektive Raum $PG(d-1,q)$ ein Beispiel eines $2-(v,q+1,1)$ Designs mit $v = (q^d-1)/(q-1)$. Die Gruppe $P\Gamma L(d,q)$ ist die volle Automorphismengruppe dieses Steiner Designs.

Beispiel 2.5. (Affine Räume).
Wir wählen als Punktmenge X die Menge der Elemente eines Vektorraums V der Dimension $d \geq 2$ über $GF(q)$. Als Blockmenge $\mathcal{B}$ wählen wir die affinen Geraden des Vektorraums (bekanntlich sind dies die Nebenklassen nach 1-dimensionalen Untervektorräumen). Dann haben wir $v = q^d$ Punkte und jeder Block $B \in \mathcal{B}$ inzidiert mit $k = q$ Punkten. Da je zwei verschiedene Punkte auf genau einer Geraden liegen, inzidieren sie mit genau einem Block. Daher erhalten wir den affinen Raum $AG(d, q)$ als Beispiel eines $2-(q^d, q, 1)$ Designs. Die volle Automorphismengruppe dieses Steiner Designs ist die Gruppe $A\Gamma L(d, q)$.

Beispiel 2.6. In einem beliebigen affinen Raum definieren je drei verschiedene Punkte eine Ebene, wenn sie nicht-kollinear (d. h. auf keiner Geraden liegend) sind. Wenn wir den Körper $GF(2)$ zugrunde legen, dann sind jedoch drei verschiedene Punkte stets nicht-kollinear, denn die Geraden bestehen jeweils nur aus zwei Punkten. Somit bilden die Punkte und die Ebenen des affinen Raums $AG(d, 2)$ ein $3-(2^d, 4, 1)$ Design. Da $AG(d, 2)$ stets desarguessch ist für $d \geq 3$, sind diese sogar bis auf Isomorphie eindeutig bestimmt. Als 3-fach transitive volle Automorphismengruppe haben wir die Gruppe $AGL(d, 2)$.

Beispiel 2.7. (Kreisgeometrien).
Sei $d \geq 2$. Als Punktmenge X wählen wir die Elemente der projektiven Geraden $GF(q^d) \cup \{\infty\}$ über $GF(q^d)$ (wobei ∞ ein Symbol bezeichnet mit $\infty \notin GF(q^d)$). Auf dieser wirkt die Gruppe

$$PGL(2, q^d) = \{x \mapsto \frac{ax+b}{cx+d} : a, b, c, d \in GF(q^d), ad - bc \neq 0\}$$

in natürlicher Weise (mit den üblichen Rechenregeln für ∞). Als Blockmenge $\mathcal{B}$ können wir alle Bilder von $GF(q) \cup \{\infty\}$ unter dieser Gruppe wählen. Wir erhalten somit ein $3-(q^d+1, q+1, 1)$ Design.

Für $d = 2$ erhält man als sog. *Möbiusebenen* $3-(q^2+1, q+1, 1)$ Designs. Für jede Primzahlpotenz q existiert stets eine klassische Möbiusebene mit der Gruppe $PGL(2, q^2)$ als Automorphismengruppe. Falls die natürliche Zahl $e > 1$ ungerade ist, dann existiert ebenfalls (bis auf Isomorphie sogar genau) eine Möbiusebene mit $q := 2^e$ und der Suzukigruppe $Sz(q)$ als 2-fach transitiver Automorphismengruppe (vgl. [37, Sätze 9.1 und 9.3].)

Da $PGL(2,q^2)$ auf den Punkten der projektiven Geraden 3-fach transitiv operiert, wirkt $PGL(2,q^2)$ offensichtlich auch fahnentransitiv auf ihrer zugehörigen Möbiusebene. Die Gruppe $Sz(q)$ hingegen operiert nicht fahnentransitiv auf ihrem Steiner 3-Design: Nach [37, Satz 1.11] hat $Sz(q)$ die Ordnung $(q^2+1)q^2(q-1)$. Aufgrund der Transitivität auf den Punkten hat der Punktstabilisator nach Satz 1.7 daher die Ordnung $q^2(q-1)$. Andererseits erhalten wir $r = q(q+1)$ aus Lemma 1.2 (c). Somit teilt r offensichtlich nicht die Ordnung des Punktstabilisators, und $Sz(q)$ kann aufgrund von Lemma 2.1 demzufolge nicht fahnentransitiv operieren.

Beispiel 2.8. (Nettotripelsysteme).
Sei $q \equiv 7 \pmod{12}$, und sei ε eine primitive sechste Einheitswurzel in $GF(q)$, d. h., es gilt $\varepsilon^2 - \varepsilon + 1 = 0$ in $GF(q)$. Bezeichne ferner $A\Gamma^2L(1,q)$ die Gruppe aller Permutationen von $GF(q)$ der Form

$$x \mapsto a^2x^\alpha + b,$$

wobei $a, b \in GF(q)$ mit $a \neq 0$ und $\alpha \in \mathrm{Aut}(GF(q))$ ist.
Als Punktmenge X wählen wir die Elemente von $GF(q)$ und als Blockmenge $\mathcal{B}$ die Bilder von $\{0,1,\varepsilon\}$ unter $A\Gamma^2L(1,q)$. Somit erhalten wir ein $2-(q,3,1)$ Design, welches wir als *Nettotripelsystem* $N(q)$ bezeichnen (vgl. [18, Sect. 3]).

Offensichtlich gibt es genau zwei primitive sechste Einheitswurzeln in $GF(q)$. Daher erhalten wir zunächst zwei formal unterschiedlichen Nettotripelsysteme. Clapham [13, Proposition 3.3] hat jedoch gezeigt, dass die beiden Designs isomorph sind. Somit existiert für jede Primzahlpotenz q mit $q \equiv 7 \pmod{12}$ (bis auf Isomorphie) genau ein Nettotripelsystem $N(q)$.

Für $q = 7$ ist $N(7)$ offensichtlich isomorph zur projektiven Ebene $PG(2,2)$ und hat somit eine auf den Punkten 2-fach transitive volle Automorphismengruppe. Für $q \neq 7$ hingegen gilt

$$\mathrm{Aut}(N(q)) \cong A\Gamma^2L(1,q),$$

und $A\Gamma^2L(1,q)$ operiert 2-fach homogen, jedoch nicht 2-fach transitiv auf den Punkten von $N(q)$ (siehe [18] und [40]). Daher gibt es lediglich für $q = 7$ eine Koinzidenz zwischen Nettotripelsystemen und projektiven Räumen.

Beispiel 2.9. (Witt-Designs).
Wie sich leicht zeigen lässt, ist die affine Ebene $AG(2,3)$ ein $2-(9,3,1)$ Design, das bis auf Isomorphie eindeutig bestimmt ist. Es stellt sich heraus, dass sich dieses genau dreimal erweitern lässt zu ebenfalls eindeutig bestimmten Designs: das $3-(10,4,1)$ Design ist die Möbiusebene der Ordnung 3 mit $P\Gamma L(2,9)$ als voller Automorphismengruppe, die $4-(11,5,1)$ und $5-(12,6,1)$ Designs werden häufig *Witt-Designs* genannt und besitzen die Mathieugruppen M_{11} bzw. M_{12} als 4-fach bzw. 5-fach transitive volle Automorphismengruppen.

Ausgehend von der projektiven Ebene $PG(2,4)$ lassen sich wieder durch dreimaliges Erweitern die übrigen eindeutig bestimmten Witt-Designs konstruieren: das $3-(22,6,1)$ Design mit $\mathrm{Aut}(M_{22})$ als 3-fach transitiver voller Automorphismengruppe und die $4-(23,7,1)$ und $5-(24,8,1)$ Designs mit M_{23} bzw. M_{24} als 4-fach bzw. 5-fach transitiver voller Automorphismengruppe (vgl. [3, Kap. 18] und [41]).

Bemerkung 2.10. Wenn sich für vorgegebene Parameter $t < k < v$ nicht mit Lemma 1.2 sofort auf eine Nicht-Existenz schließen lässt, ist es in vielen Fällen sehr schwierig und häufig noch offen, ob ein $t-(v,k,1)$ Design überhaupt existiert. Nach Beutelspacher [6, S. 99] gehört dies zu einem der schwierigsten Probleme der endlichen Geometrie. Noch schwieriger gestaltet sich allerdings die Frage nach der Anzahl der nicht-isomorphen Typen eines $t-(v,k,1)$ Designs, falls ein solches existiert.
Wenn wir beispielsweise affine Ebenen der Ordnung q, also $2-(q^2,q,1)$ Designs, betrachten, dann existieren diese vermutlich nur, wenn q eine Primzahlpotenz ist und für den Fall, dass q eine Primzahl ist, gibt es bis auf Isomorphie wahrscheinlich nur einen solchen Typ. Für projektive Ebenen gelten dieselben Vermutungen (vgl. [42]). Bruck und Ryser [8] haben bewiesen, dass keine projektive Ebene der Ordnung q existiert, falls $q \equiv 1$ oder $2 \pmod 4$ und q nicht Summe zweier Quadrate ist. Die erste natürliche Zahl, welche weder diese Hypothese erfüllt noch von Primzahlpotenz ist, ist $q = 10$. Lam et. al [35] haben unter erheblichem Computereinsatz gezeigt, dass es keine projektive Ebene dieser Ordnung geben kann. Andererseits gibt es beispielsweise genau 4 Isomorphietypen von projektiven Ebenen der Ordnung 9, also genau 4 nicht-isomorphe $2-(91,10,1)$ Designs.

Kapitel 3

Fahnentransitive Steinerquadrupelsysteme

3.1 Steinerquadrupelsysteme

Ein *Steinerquadrupelsystem* der Ordnung v ist ein $3-(v,4,1)$ Design, und wird mit $SQS(v)$ bezeichnet. Wie wir in Kapitel 2, Beispiel 2.6 gesehen haben, existieren für $d \geq 3$ stets die eindeutig bestimmten $SQS(2^d)$, bestehend aus den Punkten und Ebenen von $AG(d,2)$.

Mittels aufwendiger rekursiver Konstruktionen lässt sich zeigen, dass die unmittelbar einzusehende notwendige Bedingung für die Existenz eines $SQS(v)$ bereits hinreichend ist.

Satz 3.1. (Hanani [22]). *Ein $SQS(v)$ existiert genau dann, wenn*

$$v \equiv 2 \text{ \textit{oder} } 4 \pmod 6,\ v \geq 4,$$

gilt.

Für $v=8$ und 10 gibt es bis auf Isomorphie jeweils nur ein $SQS(v)$, nämlich das oben erwähnte und die Möbiusebene der Ordnung 3. Dagegen existieren für $v=16$ bereits mehr als 31021 und für $v=28$ sogar über $4 \cdot 10^{20}$ verschiedene Isomorphietypen (vgl. [4] und [36]).

Für die Klassifikation aller fahnentransitiver Steinerquadrupelsysteme im nächsten Abschnitt benötigen wir die folgenden Lemmata:

Lemma 3.2. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein $SQS(2^d)$ mit $d \geq 3$, und $G \leq \mathrm{Aut}(\mathcal{D})$ enthalte einen regulären elementar-abelschen Normalteiler T der Ordnung $v = 2^d$. Falls G fahnentransitiv auf $\mathcal{D}$ operiert und $|G_0| \equiv 1 \pmod 2$ gilt, dann ist $\mathcal{D}$ (bis auf Isomorphie) eindeutig bestimmt, und die Punkte und Blöcke von $\mathcal{D}$ sind genau die Punkte und Ebenen von $AG(d, 2)$.*

Beweis. Da die Gruppe T elementar-abelsch der Ordnung 2^d ist, enthält sie Untergruppen der Ordnung 4. Ferner ist T wegen $|G_0| \equiv 1 \pmod 2$ die einzige 2-Sylowuntergruppe und enthält daher alle Untergruppen von G der Ordnung 4. Nach Voraussetzung wirkt G_B transitiv auf den Punkten eines beliebigen Blocks $B \in \mathcal{B}$. Somit ist 4 ein Teiler der Ordnung von G_B, und G_B enthält mindestens eine Untergruppe S von T der Ordnung 4. Dann ist aber $B \in \mathcal{B}$ eine Bahn von S und daher eine affine Ebene. Da $G \leq \mathrm{Aut}(\mathcal{D})$ blocktransitiv ist, können wir schließen, dass alle Blöcke affine Ebenen sein müssen. Nun identifizieren wir die Punkte von $\mathcal{D}$ mit den Elementen von T, und die Behauptung folgt. $\square$

Lemma 3.3. *Sei $V(d, q)$ ein Vektorraum der Dimension $d > 3$ über $GF(q)$, q eine Primzahlpotenz, und $PG(d-1, q)$ der zugehörige $(d-1)$-dimensionale projektive Raum. Wirke die Gruppe G vom Typ fasteinfach mit $N = PSL(d, q)$ auf $PG(d-1, q)$, und für alle $g \in G$ mit $|M^g \cap M| \geq 3$ gelte $M^g = M$, wobei M eine beliebige Menge von Punkten aus $PG(d-1, q)$ bezeichnet der Mächtigkeit k mit $3 \leq k \leq |\mathcal{H}|$ und $\mathcal{H}$ eine Hyperebene von $PG(d-1, q)$.*

Falls $|M \cap \mathcal{H}| \geq 3$ ist, dann gilt $M \cap \mathcal{H} = M$.

Beweis. Für $k = 3$ ist die Behauptung trivial. Sei daher $3 < k \leq |\mathcal{H}| = \frac{q^{d-1}-1}{q-1}$. In $PG(d-1, q)$ gilt der Satz von Desargues und die Translationen $T(\mathcal{H})$ bilden eine abelsche Gruppe, welche nach dem Satz von Baer scharf transitiv auf den Punkten von $PG(d-1, q) \setminus \mathcal{H}$ operieren. Auf $\mathcal{H}$ hingegen wirkt die Gruppe $T(\mathcal{H})$ trivial, denn die Zentralkollineationen lassen jeden Punkt von $\mathcal{H}$ fest. Somit gilt die Behauptung, falls alle Elemente von M in $\mathcal{H}$ liegen. Um dies zu zeigen, nehmen wir an, dass es ein Element von M gibt, das nicht in $\mathcal{H}$ liegt. Dann enthält M bereits alle Punkte von $PG(d-1, q) \setminus \mathcal{H}$, da $T(\mathcal{H})$ transitiv ist. Daher gilt

$$|M| \geq \frac{q^d - 1}{q - 1} - \frac{q^{d-1} - 1}{q - 1} = \frac{q^d - q^{d-1}}{q - 1} = q^{d-1} > \frac{q^{d-1} - 1}{q - 1} = |\mathcal{H}|,$$

ein Widerspruch zur Voraussetzung $|M| \leq |\mathcal{H}|$. $\square$

3.2 Klassifikation

Wie in der Einleitung erwähnt, ist die Klassifikation fahnentransitiver Steiner 3-Designs ein „still open and longstanding problem"(siehe [16] und [17, p. 273]).

In diesem Abschnitt klassifizieren wir unter Zuhilfenahme der Klassifikation der endlichen 2-fach transitiven Permutationsgruppen alle fahnentransitiven $SQS(v)$. Wir lösen somit das obige Problem für den kleinsten Wert, den der Parameter k annehmen kann. Unser Resultat verallgemeinert einen Satz von Lüneburg [38], der alle fahnentransitiven $SQS(v)$ charakterisiert unter der zusätzlichen starken Voraussetzung, dass jedes von der Identität verschiedene Element der Automorphismengruppe höchstens zwei Fixpunkte hat. Unsere Vorgehensweise wie auch unsere Beweise sind dabei unabhängig von Lüneburg. Bereits in [26] beschäftigten wir uns mit dieser Klassifikation. Die dort erzielten Ergebnisse haben wir in ihrer Darstellung verbessert und die noch offen gebliebenen Fälle gelöst. Unser Resultat ist erschienen in [27]. Abschließend betrachten wir noch einen Sonderfall (Satz 3.5).

Theorem 3.4. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $SQS(v)$. Genau dann operiert $G \leq \mathrm{Aut}(\mathcal{D})$ fahnentransitiv auf $\mathcal{D}$, wenn einer der folgenden Fälle auftritt:*

(1) *$\mathcal{D}$ ist isomorph zum $SQS(2^d)$, bestehend aus den Punkten und Ebenen von $AG(d, 2)$, 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 $G \cong A\Gamma L(1, 32)$,*

(2) *$\mathcal{D}$ ist isomorph zu einem $SQS(3^d + 1)$, dessen Punkte die Elemente von $GF(3^d) \cup \{\infty\}$ und dessen Blöcke die Bilder von $GF(3) \cup \{\infty\}$ unter $PGL(2, 3^d)$ mit $d \geq 2$ (resp. $PSL(2, 3^d)$ mit $d > 1$ ungerade) sind, und das abgeleitete Design ist isomorph zum $2-(3^d, 3, 1)$ Design, bestehend aus den Punkten und Geraden von $AG(d, 3)$, und $PSL(2, 3^d) \leq G \leq P\Gamma L(2, 3^d)$,*

(3) *$\mathcal{D}$ ist isomorph zu einem $SQS(q+1)$, dessen Punkte die Elemente von $GF(q) \cup \{\infty\}$ mit einer Primzahlpotenz $q \equiv 7 \pmod{12}$ und dessen Blöcke die Bilder von $\{0, 1, \infty, \varepsilon\}$ unter $PSL(2,q)$ sind, wobei ε eine primitive sechste Einheitswurzel in $GF(q)$ ist, und das abgeleitete Design ist isomorph zum Nettotripelsystem $N(q)$, und $PSL(2,q) \leq G \leq P\Sigma L(2,q)$.*

Das *Nettotripelsystem* haben wir in Kapitel 2, Beispiel 2.8 ausführlich beschrieben.

Beweis. Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein $SQS(v)$. Aufgrund von Korollar 2.3 können wir von der Klassifikation der endlichen 2-fach transitiven Permutationsgruppen (Theorem 1.8) ausgehen. Die dort auftretenden Gruppen G werden wir im Folgenden sukzessive daraufhin untersuchen, ob $G \leq \mathrm{Aut}(\mathcal{D})$ fahnentransitiv auf $\mathcal{D}$ operiert.

(A) Affiner Fall.

Wie in Theorem 1.8 angeführt, hat eine endliche 2-fach transitive Permutationsgruppe G vom Typ affin den Grad $v = p^d$. Wegen Satz 3.1 gilt in diesem Fall somit $v = 2^d$. Um triviale $SQS(v)$ auszuschließen, sei $d \geq 3$.

Fall (1): $G \leq A\Gamma L(1, 2^d)$.

Wir setzen zunächst voraus, dass $G \leq \mathrm{Aut}(\mathcal{D})$ fahnentransitiv auf $\mathcal{D}$ operiert. Lemma 2.1 und der Satz von Lagrange liefern dann

$$r = \tfrac{1}{3}(2^d - 1)(2^{d-1} - 1) \,\Big|\, |G_0| \,\Big|\, \big|A\Gamma L(1, 2^d)_0\big| = \big|\Gamma L(1, 2^d)\big| = d(2^d - 1).$$

Daher gilt $d = 3, 5$. Sei zunächst $d = 3$. Dann gilt $|A\Gamma L(1,8)| = |T|\,|\Gamma L(1,8)| = 8 \cdot 7 \cdot 3$. Da G 2-fach transitiv ist, erhalten wir $8 \cdot 7 \mid |G|$, und daher $|G| = 8 \cdot 7$ oder $8 \cdot 7 \cdot 3$. Letzteres impliziert $G \cong A\Gamma L(1,8)$. Sei also $|G| = 8 \cdot 7$. Da $A\Gamma L(1,8)$ auflösbar und G eine $\{2,7\}$-Halluntergruppe ist, können wir nach dem π-Sylowsatz schließen, dass $G \cong AGL(1,8)$ gilt. Für $d = 5$ erhalten wir entsprechend $|G| = 32 \cdot 31$ oder $32 \cdot 31 \cdot 5$. Da wir für $|G| = 32 \cdot 31$ mit Lemma 2.1 einem Widerspruch erhalten, folgt $G \cong A\Gamma L(1,32)$.

Umgekehrt haben wir zu zeigen, dass $G \cong AGL(1,8)$, $A\Gamma L(1,8)$ resp. $A\Gamma L(1,32)$ fahnentransitiv operiert auf dem angegebenen $SQS(8)$ resp. $SQS(32)$.

Für $v = 8$ gibt es (bis auf Isomorphie) nur das eindeutig bestimmte $SQS(v)$, bestehend aus den Punkten und Ebenen von $AG(3,2)$. Da $G \cong AGL(1,8)$ transitiv auf den Punkten operiert, genügt es zu zeigen, dass $G_0 \cong GL(1,8)$ transitiv auf den mit 0 inzidenten Blöcken operiert. Nun sind dies genau die 2-dimensionalen Unterräume des zugrunde liegenden Vektorraums. Daher gilt

$$B_1 := \{0, 1, t, t+1\} \neq B_1^t = \{0, t, t^2, t^2+1\} \quad \text{für} \quad 1 \neq t \in GL(1,8) \cong GF(8)^*.$$

Dann ist $|B_1^{GL(1,8)}| \neq 1$, und wegen $r = 7$ folgt die Behauptung nach Satz 1.7. Offensichtlich wirkt dann auch $G \cong A\Gamma L(1,8)$ fahnentransitiv auf $\mathcal{D}$. Für $v = 32$ gilt $|G_0| = |\Gamma L(1,32)| \equiv 1 \pmod 2$ und wir erhalten daher mit Lemma 3.2 ebenso lediglich das eindeutig bestimmte $SQS(v)$, bestehend aus den Punkten und Ebenen von $AG(5,2)$. Um einzusehen, dass $G_0 \cong \Gamma L(1,32)$ fahnentransitiv auf den mit 0 inzidenten Blöcken wirkt, zeigt man wie vorher, dass $|B_1^{GL(1,32)}| \neq 1$ gilt. Nach Satz 1.7 ist dann $|GL(1,32)_B| = 1$ für $0 \in B \in \mathcal{B}$ beliebig. Somit gilt $|B^{\Gamma L(1,32)}| = 31$ oder $31 \cdot 5$. Angenommen, die erste Aussage gelte. Wiederum mit Satz 1.7 erhalten wir dann $|\Gamma L(1,32)_B| = 5$. Sei H eine zyklische Gruppe der Ordnung 5. Dann gilt $|H_B| \neq 1$ für $0 \in B \in \mathcal{B}$ beliebig. Andererseits ist aber 5 ein 2-primitiver Teiler von $2^4 - 1$. Daher besitzt H infolge von Satz 1.14 irreduzible Moduln vom Grad 4. Da nach dem Satz von Maschke der 5-dimensionale $GF(32)H$-Modul vollständig reduzibel ist, hat H als irreduzible Moduln nur den trivialen Modul und einen weiteren vom Grad 4. Falls jedoch H einen beliebigen 2-dimensionalen Untervektorraum fest lassen würde, dann hätte H, wiederum nach dem Satz von Maschke, als irreduzible Moduln zwei 1-dimensionale Moduln, ein Widerspruch. Daher muss $|B^{\Gamma L(1,32)}| = 31 \cdot 5$ gelten, und wegen $r = 31 \cdot 5$ folgt dann die Behauptung.

Fall (2): $G_0 \trianglerighteq SL(\frac{d}{a}, 2^a)$, $d \geq 2a$.

Für $a = 1$ haben wir $G \cong AGL(d,2)$. Dann ist G 3-fach transitiv und nach [32, Theorem 3] ist das $SQS(v)$, bestehend aus den Punkten und Ebenen von $AG(d,2)$, $d \geq 3$, das einzige, auf welchem G operiert. Offensichtlich wirkt G auf diesem auch fahnentransitiv. Wegen $d \geq 2a$ können wir im Folgenden annehmen, dass a ein echter Teiler von d ist. Wir werden zeigen, dass hier kein fahnentransitives $SQS(v)$ existiert.

Aufgrund von Lemma 2.1, genügt es zu zeigen, dass r kein Teiler von $|G_0|$ ist. Bekanntlich gilt

$$\left|SL(\tfrac{d}{a}, 2^a)\right| = 2^{d(\frac{d}{a}-1)/2} \prod_{i=2}^{\frac{d}{a}} (2^{ia} - 1),$$

$$\text{und} \quad [\Gamma L(\tfrac{d}{a}, 2^a) : SL(\tfrac{d}{a}, 2^a)] = |\mathrm{Aut}(GF(2^a))|\,|GF(2^a)^*| = a \cdot (2^a - 1).$$

Daher genügt es zu zeigen, dass r nicht $a \cdot (2^a - 1) \cdot \left|SL(\frac{d}{a}, 2^a)\right|$ teilt. Nach den Sätzen 1.12 und 1.14 sowie Lemma 1.13 (b) hat

$$2^{d-1} - 1$$

einen 2-primitiven Primteiler $\tilde{r}$ mit $\tilde{r} \perp 2^{d-1} - 1$. Offensichtlich ist $\tilde{r} \neq 2$. Ferner gilt $\tilde{r} \nmid 3a$, denn $\tilde{r} \equiv 1 \pmod{(d-1)}$ nach Lemma 1.13 (c) und d ist echt teilbar durch a.
Daher gilt

$$2^{d-1} - 1 \nmid 3a \cdot 2^{d(\frac{d}{a}-1)/2} \prod_{i=1}^{\frac{d}{a}-1} (2^{ia} - 1)$$

und die Behauptung folgt.

Fälle (3)-(4): Diese Fälle können analog zu Fall (2) eliminiert werden mithilfe der Lemmata 1.13 und 2.1 sowie den Sätzen 1.12 und 1.14. (Ausführlich ist dies dargestellt in [26, S. 72 ff.]; für $|\mathrm{Out}(G_0)|$ siehe beispielsweise [33, S. 170, Tables 5.1 A und 5.1 B]).

Fall (5): $G_0 \cong A_6$ oder A_7, $v = 2^4$.

Falls $G \cong A_6$ gilt, dann impliziert Lemma 2.1, dass G auf keinem $SQS(v)$ fahnentransitiv operieren kann.

Da $G \cong A_7$ 3-fach transitiv ist und nach [32, Theorem 3] das aus den Punkten und Ebenen von $AG(4, 2)$ bestehende $SQS(v)$ das einzige ist, auf welchem G operiert, liegt in diesem Fall Fahnentransitivität vor.

Fälle (6)-(8): Diese Fälle können nicht auftreten, da v keine 2-Potenz ist.

(B) Fasteinfacher Fall.

Die Fälle (3), (5), (8), (12) aus Theorem 1.8, wobei G vom Typ fasteinfach ist, können mittels Lemma 2.1 leicht ausgeschlossen werden (vgl. [26, S. 91 ff.]).

Offensichtlich können die Fälle $(4), (7), (10), (11), (13)$ wegen Satz 3.1 nicht auftreten.

Fall (1): $N = A_v$, $v \geq 5$. In diesem Fall ist G 3-fach transitiv und operiert nach [32, Theorem 3] auf keinem nicht-trivialen $3-(v,k,1)$ Design.

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

Wir unterscheiden zwei Unterfälle:

(i) $N = PSL(2,q)$, $v = q+1$.

Es gilt $q \geq 5$, denn $PSL(2,4) \cong PSL(2,5)$, und $\mathrm{Aut}(N) = P\Gamma L(2,q)$. Sei zunächst G 3-fach transitiv. Aufgrund von [32, Theorem 3] erhalten wir dann lediglich das in (2) beschriebene $SQS(3^d+1)$ mit $PSL(2,3^d) \leq G \leq P\Gamma L(2,3^d)$. Offensichtlich liegt hier auch Fahnentransitivität vor. Da $PGL(2,q)$ eine transitive Erweiterung von $AGL(1,q)$ ist, sieht man leicht, dass das abgeleitete Design in einem beliebigen Punkt von $GF(3^d) \cup \{\infty\}$ isomorph ist zum $2-(3^d,3,1)$ Design, bestehend aus den Punkten und Geraden von $AG(d,3)$.

Nun nehmen wir an, dass G 3-fach homogen, aber nicht 3-fach transitiv ist. Da hier $PSL(2,q)$ eine transitive Erweiterung von $AG^2L(1,q)$ ist, können wir aus [18] schließen, dass das abgeleitete Design entweder der affine Raum $AG(d,3)$ mit den Geraden als Blöcken oder das Nettotripelsystem $N(q)$ ist. Somit gilt (2) mit der Aussage in Klammern oder (3) mit $PSL(2,3^d) \leq G \leq P\Sigma L(2,3^d)$. Umgekehrt ist G aufgrund der 3-fachen Homogenität auch blocktransitiv. In beiden Fällen haben wir $PSL(2,q)_B \cong A_4$ für $B \in \mathcal{B}$ beliebig, denn $PSL(2,q)_B$ hat nach Satz 1.7 die Ordnung 12 und $PSL(2,q)_B \longrightarrow \mathrm{Sym}(B) \cong S_4$ ist eine treue Darstellung. Somit liegt in jedem der beiden Fälle Fahnentransitivität vor.

Sei schließlich G nicht 3-fach homogen. Da $PGL(2,q)$ 3-fach homogen ist, zerfällt die $PGL(2,q)$-Bahn auf den 3-elementigen Teilmengen daher unter $PSL(2,q)$ in genau zwei Bahnen gleicher Länge. Sei M eine beliebige 3-elementige Teilmenge. Dann gilt $|PSL(2,q)_M| = |PGL(2,q)_M| = 6$ nach Satz 1.7. Da $PGL(2,q)$ 3-fach transitiv ist, haben wir folglich

$$PSL(2,q)_M \cong S_3$$

für jede Bahn.

Falls $PSL(2,q)$ blocktransitiv auf einem beliebigen $SQS(v)$ operieren würde, dann wäre wiederum
$$PSL(2,q)_B \cong A_4$$
für $B \in \mathcal{B}$ beliebig. Jedoch würde dies nach der Definition von $SQS(v)$ implizieren, dass $PSL(2,q)_{\tilde{B}}$, wobei $\tilde{B}$ den durch M eindeutig bestimmten Block bezeichnet, $PSL(2,q)_M$ enthält, ein Widerspruch. Somit kann $PSL(2,q)$ auf einem beliebigen $SQS(v)$ nicht fahnentransitiv operieren. Nun zeigen wir, dass auch G auf keinem $SQS(v)$ fahnentransitiv operiert. Ohne Einschränkung können wir $\mathcal{O}_1$ als die $PSL(2,q)$-Bahn wählen, die das Tripel $\{0,1,\infty\}$ enthält. Einfaches Rechnen ergibt
$$P\Sigma L(2,q)_{0,1,\infty} = \langle \tau_\alpha \rangle$$
mit τ_α wie in Bemerkung 1.9 eingeführt. Dann ist $P\Sigma L(2,q)_{\mathcal{O}_1}$ in $P\Gamma L(2,q)$ enthalten, und es gilt sogar Gleichheit, denn $P\Sigma L(2,q)$ ist vom Index 2 in $P\Gamma L(2,q)$ und $P\Gamma L(2,q)$ ist 3-fach transitiv. Daher haben wir lediglich
$$PSL(2,q) \leq G \leq P\Sigma L(2,q)$$
zu betrachten. Das Dedekind'sche Gesetz liefert
$$G = PSL(2,q) \rtimes (G \cap \langle \tau_\alpha \rangle)$$
und
$$G_{(B)} = PSL(2,q)_{(B)} \rtimes (G \cap \langle \tau_\alpha \rangle) = G \cap \langle \tau_\alpha \rangle \cong C_m$$
mit $m \mid d$ für einen beliebigen Block $B \in \mathcal{B}$, denn jedes von der Identität verschiedene Element von $PSL(2,q)$ lässt höchstens zwei Punkte fest. Angenommen, G wirke nun blocktransitiv auf einem beliebigen $SQS(v)$. Dann können wir $B \in \mathcal{B}$ derart wählen, dass B das Tripel $\{0,1,\infty\}$ enthält. Da $G_{(B)}$ der Kern der Darstellung $G_B \longrightarrow \mathrm{Sym}(B) \cong S_4$ ist und $PSL(2,q)_B \cong A_4$ gilt, erhalten wir somit wiederum nach dem Dedekind'schen Gesetz
$$G_B = PSL(2,q)_B \times (G \cap \langle \tau_\alpha \rangle) \cong A_4 \times C_m.$$
Jedoch ergibt sich wegen $PSL(2,q)_{\{0,1,\infty\}} \cong S_3$ analog
$$G_{\{0,1,\infty\}} = PSL(2,q)_{\{0,1,\infty\}} \times (G \cap \langle \tau_\alpha \rangle) \cong S_3 \times C_m,$$
wiederum nach der Definition von $SQS(v)$ ein Widerspruch.

(ii) $N = PSL(d,q)$, $d \geq 3$, $v = \frac{q^d-1}{q-1}$.

Hier gilt $\mathrm{Aut}(N) = P\Gamma L(d,q) \rtimes \langle \iota \rangle$ (vgl. Bemerkung 1.9). Wir werden zeigen, dass G auf keinem $SQS(v)$ operiert. Für $d = 3$ ist dies offensichtlich, denn $v = q^2 + q + 1$ ist stets ungerade, ein Widerspruch zu Satz 3.1.

Sei also $d > 3$ und $\mathcal{H}$ eine Hyperebene des projektiven Raums $PG(d-1,q)$. Angenommen, die Behauptung wäre falsch. Dann gibt es ein Gegenbeispiel mit minimalem d. Ohne Einschränkung können wir drei beliebige Punkte x, y, z aus $\mathcal{H}$ wählen. Für $d > 3$ gilt

$$|\mathcal{H}| = \frac{q^{d-1}-1}{q-1} > 4.$$

Daher ist der durch x, y, z eindeutig bestimmte Block in $\mathcal{H}$ enthalten nach Lemma 3.3. Folglich induziert $\mathcal{H}$ ein $SQS(\frac{q^{d-1}-1}{q-1})$, auf welchem die Gruppe G, die $PSL(d-1,q)$ enthält, operiert. Nach Induktion erhalten wir dann das minimale Gegenbeispiel für $d = 3$. Somit operiert die Gruppe G, welche $PSL(3,q)$ enthält, auf einem $SQS(\frac{q^3-1}{q-1})$. Da jedoch $\frac{q^3-1}{q-1} = q^2 + q + 1$ stets ungerade ist, folgt der gewünschte Widerspruch.

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

Es gilt $N = G$, denn $|Out(N)| = 1$ (vgl. [33, S. 170, Table 5.1 A]). Wir zeigen, dass G Elemente enthält, die genau drei Punkte fix lassen und somit auf keinem $SQS(v)$ operieren kann nach Definition.

Bezeichne X^+ resp. X^- die Menge der Punkte, auf der G operiert mit $|X^+| = 2^{2d-1} + 2^{d-1}$ resp. $|X^-| = 2^{2d-1} - 2^{d-1}$. Für einen Primteiler p von $|G|$ definieren wir

$$m_p(G) := \min\{|\mathrm{supp}(g)| : 1 \neq g \in G,\ g \text{ ein } p\text{-Element von } G\}$$

als den *p-Minimalgrad* einer transitiven Permutationsgruppe G (vgl. [25]).

Zunächst nehmen wir an, d sei gerade. Nach den Sätzen 1.12 und 1.14 sowie Lemma 1.13 (b) besitzt

$$2^{d-1} - 1$$

einen 2-primitiven Primteiler p mit $p \perp 2^{d-1} - 1$. Ferner teilt p die Ordnung von G, denn es gilt $|G| = 2^{d^2} \prod_{i=1}^{d} (2^{2i} - 1)$ (siehe z. B. [33, S. 19, Table 2.1 C]). Aufgrund von [25, Theorem 3.7] erhalten wir in X^+ daher

$$m_p(G) = 2^{2d-2(d-1)-1}(2^{2(d-1)} - 1) + 2^{d-(d-1)-1}(2^{d-1} - 1) = \left|X^+\right| - 3.$$

Somit existiert ein $g \in G$ von Primzahlordnung p, welches genau drei Punkte fest lässt in X^+.

Für $d \neq 4$ existiert wie oben ein 2-primitiver Primteiler p mit $p \perp 2^{2(d-1)} - 1$, und da p ein Teiler von $|G|$ ist, erhalten wir wiederum mit [25, Theorem 3.7] in X^-

$$m_p(G) = 2^{2d-2(d-1)-1}(2^{2(d-1)} - 1) - 2^{d-(d-1)-1}(2^{d-1} + 1) = \left|X^-\right| - 3.$$

Falls $d = 4$ ist, dann liefert [14, S. 123], dass $|\mathrm{fix}(g)| = 3$ ist in X^- für $g \in 3D$, wobei $3D$ eine Konjugiertenklasse in [14] bezeichnet.

Nun nehmen wir an, d sei ungerade. Wieder erhalten wir die Existenz eines 2-primitiven Primteilers p mit $p \perp 2^{2(d-1)} - 1$, und $m_p(G) = |X^-| - 3$ in X^-.

Falls $d \neq 7$ gilt, dann existiert ein 2-primitiver Primteiler p mit $p \perp 2^{d-1} - 1$. Wir wählen $\begin{pmatrix} A_0 & A_1 \\ A_2 & A_3 \end{pmatrix} \in S \in \mathrm{Syl}_p(Sp(d-1, 2))$ und definieren

$$h := \begin{pmatrix} A_0 & & & A_1 & & \\ & A_0 & & & A_1 & \\ & & 1 & & & 0 \\ A_2 & & & A_3 & & \\ & A_2 & & & A_3 & \\ & & 0 & & & 1 \end{pmatrix}.$$

Aus dem Beweis von [25, Theorem 3.7] ergibt sich $|\mathrm{fix}(h)| = 3$ in X^+ und $|\mathrm{fix}(h)| = 1$ in X^-.
Für $d = 7$ wählen wir $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ und definieren

$$i := \mathrm{diag}(A,\, A,\, A,\, 1,\, {}^t\!A^{-1},\, {}^t\!A^{-1},\, {}^t\!A^{-1},\, 1).$$

Wieder ist $|\mathrm{fix}(i)| = 3$ in X^+ und $|\mathrm{fix}(i)| = 1$ in X^-. Somit ist die Behauptung gezeigt.

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

Hier ist nach Satz 3.1 nur $v = 22$ möglich. Da M_{22} 3-fach transitiv ist, liefert jedoch [32, Theorem 3], dass das Witt $3-(22, 6, 1)$ Design das einzige Steiner 3-Design ist, auf welchem M_{22} resp. $\mathrm{Aut}(M_{22})$ operiert. Somit kann dieser Fall nicht auftreten, und das Theorem ist bewiesen. □

Es lässt sich leicht zeigen, dass die in Theorem 3.4 unter (1) (iv) und (3) angegebenen $SQS(32)$ nicht isomorph sind: Es genügt dafür die abgeleiteten Designs zu betrachten. Einerseits haben wir das Nettotripelsystem $N(31)$, andererseits erhalten wir mit [19, Kap. 2.4, Satz 34] das Steiner 2-Design, welches aus den Punkten und Geraden von $PG(4,2)$ besteht. Wie wir jedoch in Beispiel 2.8 gesehen haben, gibt es nur für $q = 7$ eine Koinzidenz zwischen Nettotripelsystemen und projektiven Räumen.

Abschließend betrachten wir folgenden Sonderfall: Sei G als Automorphismengruppe eines Steinerquadrupelsystems vom Typ fasteinfach mit $N = PSL(2,q)$. Wenn G 3-fach homogen ist, dann sind die $SQS(v)$, auf denen G operiert nach dem vorangegangenen Theorem bekannt. Wir wollen daher voraussetzen, dass G nicht 3-fach homogen ist. Es lässt sich zeigen, dass dies genau dann der Fall ist, wenn $q \equiv 1 \pmod 4$ gilt (vgl. [26, S. 89]). Wie wir gesehen haben, existiert in diesem Fall kein fahnentransitives $SQS(v)$. Es stellt sich allerdings die Frage, ob es ein $SQS(v)$ gibt mit obiger Automorphismengruppe G, wenn wir von der Eigenschaft der Fahnentransitivität absehen. Analog zum vorangegangenen Beweis genügt es dabei, $PSL(2,q) \leq G \leq P\Sigma L(2,q)$ zu betrachten. Wir erhalten die folgende Aussage:

Satz 3.5. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $SQS(v)$. Genau dann operiert $G \leq \mathrm{Aut}(\mathcal{D})$ mit $PSL(2,q) \leq G \leq P\Sigma L(2,q)$, q eine Primzahlpotenz, und G nicht 3-fach homogen auf $\mathcal{D}$, wenn $\mathcal{D}$ isomorph ist zu einem $SQS(3^{2d}+1)$, dessen Punkte die Elemente von $GF(3^{2d}) \cup \{\infty\}$ und dessen Blöcke die disjunkte Vereinigung der Bilder von $\{0,1,-1,\infty\}$ unter $PSL(2,3^{2d})$ und $\{0,1,a,\infty\}$ unter $PSL(2,3^{2d})$ mit $d \in \mathbb{N}$, $a \notin GF(3^{2d})^{*2}$ sind, und $PSL(2,3^{2d}) \leq G \leq P\Sigma L(2,3^{2d})$.*

Beweis. Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $SQS(v)$. Wegen $v = q+1 > 4$ können $(d,q) = (2,2),(2,3)$ nicht auftreten. Also ist G stets 2-fach transitiv, nach Voraussetzung jedoch nicht 3-fach homogen. Somit genügt es, $G = PSL(2,q)$ zu betrachten.
Da $PGL(2,q)$ 3-fach homogen ist, zerfällt die $PGL(2,q)$-Bahn auf den 3-elementigen Teilmengen daher unter G in genau zwei Bahnen gleicher Länge. Nach der Definition von $SQS(v)$ hat G folglich genau zwei Bahnen auf den Blöcken von möglicherweise ungleicher Länge. Da für einen beliebigen Block $B \in \mathcal{B}$ aus jeder Bahn die Darstellung $G_B \longrightarrow \mathrm{Sym}(B) \cong S_4$ treu ist, erhal-

ten wir mit der Bahnenformel (1.7), dass die beiden Bahnen auf den Blöcken in der Tat gleiche Länge haben und

$$G_B \cong S_4$$

gilt auf jeder Bahn für jedes $B \in \mathcal{B}$ der jeweiligen Bahn. Wir bemerken, dass G_B dann vier 3-Sylowuntergruppen besitzt. Im Folgenden haben wir aufgrund von Satz 3.1 und der Bedingung $q \equiv 1 \pmod 4$ zwei Fälle zu unterscheiden:

(i) $q = 3^{2d}$, $d \in \mathbb{N}$.

Wegen $3 \mid q$ hat jede 3-Sylowuntergruppe genau einen Fixpunkt. Folglich haben wir höchstens eine Bahn der Länge 4 unter G_B.
Andererseits ist der Normalisator einer 3-Sylowuntergruppe in der symmetrischen Gruppe S_3 bereits S_3 selbst; daher lässt S_3 den jeweiligen Fixpunkt fest. Der Stabilisator dieses Fixpunktes in der symmetrischen Gruppe S_4 hat mindestens die Ordnung 6. Nun ist dieser offensichtlich 3-abgeschlossen, kann also nicht S_4 selbst sein. Ferner kann er auch nicht die alternierende Gruppe A_4 sein, da diese S_3 nicht enthält. Folglich kann er nur die Ordnung 6 haben. Also gibt es mindestens eine Bahn der Länge 4.
Somit haben wir auf jeder der beiden Bahnen von Blöcken genau eine Bahn der Länge 4 unter G_B. Dies liefert uns die angegebenen Kreisgeometrien, wobei wir $a \notin GF(q)^{*2}$ wählen, denn es gilt allgemein $-1 \in GF(q)^{*2} \Longleftrightarrow q \equiv 1 \pmod 4$ (vgl. [6, Kap. 3.1, Lemma 5 (b)]). Wegen $2^4 \mid (3^d - 1)(3^d + 1)(3^{2d} + 1) = 3^{4d} - 1$ für alle $d \in \mathbb{N}$, ist für $q = 3^{2d}$, $d \in \mathbb{N}$, stets auch $q^2 \equiv 1 \pmod{16}$ erfüllt. Daher haben wir in G

$$\frac{(q+1)q(q-1)}{24}$$

zu S_4 isomorphe Untergruppen, verteilt auf zwei Konjugiertenklassen gleicher Länge (siehe [20, S. 285] bzw. [30, Kap. II, Hilfssatz 8.16 und Satz 8.18 (a)]). Nun haben wir aber genau

$$\frac{b}{2} = \frac{(q+1)q(q-1)}{2 \cdot 24}$$

Kreise auf jeder Bahn von Blöcken. Daher erhalten wir außer den Kreisgeometrien keine weiteren Steinerquadrupelsysteme.

(ii) $q \equiv 1 \pmod{12}$.

Angenommen, wir hätten eine Bahn der Länge 4 unter G_B. Dann ist der Stabilisator eines Punktes in G_B isomorph zu S_3. In dieser zur S_3 isomorphen Untergruppe U haben wir einen Normalteiler der Ordnung 3. Dieser hat genau zwei Fixpunkte, denn es gilt insbesondere $3 \mid q-1$. Eine Involution in U lässt diese aber beide fest, daher hat U zwei Fixpunkte.
Andererseits ist jedoch der Stabilisator auf zwei Punkten in $PSL(2,q)$ bekanntlich zyklisch. Somit erhalten wir einen Widerspruch, da S_3 nicht-abelsch ist. Also existiert keine Bahn der Länge 4 unter G_B und daher auch kein Steinerquadrupelsystem. Dies liefert uns die Behauptung. $\square$

Kapitel 4

Fahnentransitive Steiner 3-Designs

Nachdem wir im vorangegangenen Kapitel das Problem der Klassifikation fahnentransitiver Steiner 3-Designs für den kleinsten Parameter $k = 4$ gelöst haben, werden wir in diesem Kapitel die Fälle $k = 5, 6$ und 7 untersuchen.
Dafür betrachten wir in den ersten beiden Abschnitten zunächst zwei Spezialfälle: Zum einen setzen wir voraus, dass die Automorphismengruppe des Steiner 3-Designs projektiv ist, zum anderen soll die Automorphismengruppe, abgesehen von der eindimensionalen affinen Gruppe, vom Typ affin sein. Für allgemeines k lässt sich jeweils eine vollständige Klassifikation der fahnentransitiven Steiner 3-Designs angeben (Sätze 4.1 und 4.2). Daran anschließend lassen sich alle fahnentransitiven Steiner 3-Designs mit den Blockgrößen $k = 5, 6$ und 7 klassifizieren.

4.1 Projektive Automorphismengruppe

Satz 4.1. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $3-(v, k, 1)$ Design, und sei $G \leq \mathrm{Aut}(\mathcal{D})$ vom Typ fasteinfach mit $N = PSL(d, q^e)$, q eine Primzahlpotenz. Genau dann operiert G fahnentransitiv auf $\mathcal{D}$, wenn einer der folgenden Fälle auftritt:*

(1) *$\mathcal{D}$ 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) mit $q \geq 3$, $e \geq 2$ sind, und das abgeleitete Design ist isomorph zum $2-(q^e, q, 1)$ Design, bestehend aus den Punkten und Geraden von $AG(e, q)$, und $PSL(2, q^e) \leq G \leq P\Gamma L(2, q^e)$,*

(2) $\mathcal{D}$ *ist isomorph zu einem* $3-(q+1,4,1)$ *Design, dessen Punkte die Elemente von* $GF(q) \cup \{\infty\}$ *mit* $q \equiv 7 \pmod{12}$ *und dessen Blöcke die Bilder von* $\{0,1,\infty,\varepsilon\}$ *unter* $PSL(2,q)$ *sind, wobei* ε *eine primitive sechste Einheitswurzel in* $GF(q)$ *ist, und das abgeleitete Design ist isomorph zum Nettotripelsystem* $N(q)$*, und* $PSL(2,q) \leq G \leq P\Sigma L(2,q)$*.*

Beweis. Aufgrund von Theorem 1.8 sei im Folgenden $N = PSL(d,q^e)$, $d \geq 2$, $v = \frac{(q^e)^d-1}{q^e-1}$ die Anzahl der Punkte von $PG(d-1,q^e)$, und $(d,q^e) \neq (2,2),(2,3)$. Wir unterscheiden zwei Fälle:

(i) $N = PSL(2,q^e)$, $v = q^e+1$.

Hier gilt $q^e \geq 5$, denn $PSL(2,4) \cong PSL(2,5)$, und $\mathrm{Aut}(N) = P\Gamma L(2,q^e)$. Zuerst nehmen wir an, G sei 3-fach transitiv. Nach [32, Theorem 3] haben wir dann lediglich das in (1) beschriebene $3-(q^e+1,q+1,1)$ Design mit $PSL(2,q^e) \leq G \leq P\Gamma L(2,q^e)$, $q \geq 3$, $e \geq 2$. Offensichtlich liegt hier Fahnentransitivität vor. Da $PGL(2,q^e)$ eine transitive Erweiterung von $AGL(1,q^e)$ ist, sieht man leicht, dass das abgeleitete Design in einem beliebigen Punkt von $GF(q^e) \cup \{\infty\}$ isomorph ist zum $2-(q^e,q,1)$ Design, welches aus den Punkten und Geraden von $AG(e,q)$ besteht.

Nun nehmen wir an, G sei 3-fach homogen, jedoch nicht 3-fach transitiv. Da hier $PSL(2,q^e)$ eine transitive Erweiterung von $AG^2L(1,q^e)$ ist, können wir aus [18] schließen, dass das abgeleitete Design entweder der affine Raum $AG(e,q)$ mit den Geraden als Blöcken oder das Nettotripelsystem $N(q)$ ist. Daher gilt (1) mit der Aussage in Klammern oder Aussage (2) mit $PSL(2,q^e) \leq G \leq P\Sigma L(2,q^e)$. Umgekehrt ist G aufgrund der 3-fachen Homogenität auch blocktransitiv. Mit der Bahnenformel (1.7) erhalten wir folglich $|PSL(2,q^e)_B| = |PSL(2,q)|$ und mit [20, S. 286] bzw. [30, Kap. II, Satz 8.26 (12)] sogar

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

für $B \in \mathcal{B}$ beliebig. Da $PSL(2,q)$ 2-fach transitiv auf $k = q+1$ Punkten wirkt, liegt somit in beiden Fällen Fahnentransitivität vor.

Schließlich nehmen wir an, G sei nicht 3-fach homogen. Dann hat G in diesem Fall wiederum genau zwei Bahnen gleicher Länge auf den 3-elementigen Teilmengen. Nach der Definition von Steiner 3-Designs hat G folglich genau zwei Bahnen (möglicherweise ungleicher Länge) auf den Blöcken. Daher kann G auf keinem nicht-trivialen $3-(v,k,1)$ Design blocktransitiv operieren, folglich auch nicht fahnentransitiv.

(ii) $N = PSL(d, q^e)$, $d \geq 3$, $v = \frac{(q^e)^d - 1}{q^e - 1}$.

Sei im Folgenden $\bar{q} := q^e$. Hier gilt $\mathrm{Aut}(N) = P\Gamma L(d, \bar{q}) \rtimes \langle\iota\rangle$ (vgl. Bemerkung 1.9). Wir werden zeigen, dass G als Automorphismengruppe auf keinem nicht-trivialen $3-(v,k,1)$ Design operiert. Sei zunächst $d = 3$. Da durch je drei Punkte genau ein Block geht, können wir ohne Einschränkung von drei nicht-kollinearen Punkten x, y, z ausgehen. Wir unterscheiden zwei Unterfälle:

(a) der durch x, y, z eindeutig festgelegte Block enthält mindestens einen weiteren Punkt des Dreiecks durch x, y, z.

(b) der Block enthält keinen weiteren Punkt des Dreiecks.

ad (a): Bezeichne $\mathcal{G}$ eine projektive Gerade. Da in $PG(2, \bar{q})$ der Satz von Desargues gilt, wirkt die Gruppe der Translationen $T(\mathcal{G})$ nach dem Satz von Baer scharf transitiv auf den Punkten von $PG(2, \bar{q}) \setminus \mathcal{G}$. Auf $\mathcal{G}$ hingegen wirkt die Gruppe $T(\mathcal{G})$ trivial, denn die Zentralkollineationen lassen jeden Punkt von $\mathcal{G}$ fest. Somit müsste der in (a) genannte Block alle Punkte von $PG(2, \bar{q}) \setminus \mathcal{G}$, also mindestens $\bar{q}^2$ viele, enthalten. Dies sind jedoch offensichtlich mehr als die Hälfte der Punkte von $PG(2, \bar{q})$, im Widerspruch zu $k \leq \left[\frac{v}{4} + 2\right]$ nach Satz 1.4.

ad (b): Wie leicht zu sehen ist, besteht der punktweise Stabilisator von drei Punkten in der Gruppe $SL(3, \bar{q})$ genau aus den Diagonalmatrizen und hat daher die Ordnung $(\bar{q} - 1)^2$ (vgl. [30, Kap. II, Satz 7.2 (b)]). Diesem entspricht in der $PSL(3, \bar{q})$ eine Untergruppe U der Ordnung

$$\tfrac{1}{n}(\bar{q} - 1)^2 \quad \text{mit} \quad n = (3, \bar{q} - 1).$$

Da U semiregulär außerhalb des Dreiecks wirkt, erhalten wir n Bahnen mit gleicher Länge $\frac{1}{n}(\bar{q} - 1)^2$, denn falls U einen weiteren Punkt außerhalb des Dreiecks fest lassen würde, dann würde U ein nicht-ausgeartetes Viereck fest lassen. Dies würde aber bedeuten, dass U die Identität sein müsste, ein Widerspruch. Somit erhalten wir

$$k \geq 3 + \tfrac{1}{n}(\bar{q} - 1)^2.$$

Andererseits wissen wir aber, dass der in (b) genannte Block ein Bogen ist, also maximal $\bar{q}+1$ Punkte für $\bar{q}$ ungerade bzw. $\bar{q}+2$ Punkte für $\bar{q}$ gerade enthalten kann (vgl. [19, Kap. 3.2, Satz 24]). Lediglich für $\bar{q} = 2$ und 4 sind beide Aussagen erfüllt. Jedoch existieren wegen Lemma 1.2 (d) keine nicht-trivialen $3-(7,k,1)$ Designs und $3-(21,k,1)$ Designs. Somit operiert G für $d = 3$ auf keinem nicht-trivialen $3-(\bar{q}^2+\bar{q}+1,k,1)$ Design.

Sei nun $d > 3$. Auch hier werden wir zeigen, dass G auf keinem nicht-trivialen $3-(v,k,1)$ Design operiert. Sei $\mathcal{H}$ eine Hyperebene des projektiven Raums $PG(d-1,\bar{q})$. Der Beweis erfolgt als Widerspruchsbeweis mittels Induktion nach d:
Angenommen, die Behauptung wäre falsch. Dann gibt es ein Gegenbeispiel mit minimalem d. Ohne Einschränkung können wir drei beliebige Punkte x, y, z aus der Hyperebene $\mathcal{H}$ wählen. Zunächst zeigen wir, dass der durch x, y, z eindeutig bestimmte Block eines $3-(v,k,1)$ Designs vollständig in $\mathcal{H}$ liegt: Analog zu oben wirkt die Gruppe der Translationen $T(\mathcal{H})$ scharf transitiv auf den Punkten von $PG(d-1,\bar{q})\setminus\mathcal{H}$, auf $\mathcal{H}$ jedoch trivial. Falls der durch x, y, z eindeutig bestimmte Block mindestens einen Punkt außerhalb von $\mathcal{H}$ enthalten würde, dann müsste er bereits alle Punkte von $PG(d-1,\bar{q})\setminus\mathcal{H}$, also mindestens $\bar{q}^{d-1}$ viele, enthalten. Wegen

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

sind dies jedoch mehr als die Hälfte der Punkte von $PG(d-1,\bar{q})$, wie oben ein Widerspruch. Somit induziert $\mathcal{H}$ ein

$$3-(\tfrac{\bar{q}^{d-1}-1}{\bar{q}-1},k,1) \text{ Design},$$

auf welchem G mit $PSL(d-1,\bar{q}) \leq G \leq P\Gamma L(d-1,\bar{q}) \rtimes \langle\iota\rangle$ operiert. Induktiv erhält man das kleinste Gegenbeispiel für $d = 3$. Wie wir jedoch gesehen haben, operiert G mit $PSL(3,\bar{q}) \leq G \leq P\Gamma L(3,\bar{q}) \rtimes \langle\iota\rangle$ auf keinem nicht-trivialen $3-(\bar{q}^2+\bar{q}+1,k,1)$ Design, und die Behauptung folgt. □

4.2 Automorphismengruppe vom Typ affin

Satz 4.2. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $3-(v,k,1)$ Design, und sei $G \leq \mathrm{Aut}(\mathcal{D})$ vom Typ affin mit $G \nleq A\Gamma L(1,v)$. Genau dann operiert G fahnentransitiv auf $\mathcal{D}$, wenn $\mathcal{D}$ isomorph ist zum $SQS(2^d)$, bestehend aus den Punkten und Ebenen von $AG(d,2)$, und es gilt eine der beiden Aussagen:*

(i) *$d \geq 3$, und $G \cong AGL(d,2)$,*

(ii) *$d = 4$, und $G_0 \cong A_7$.*

Beweis. Sei G vom Typ affin mit $G \nleq A\Gamma L(1,v)$. Wir haben sukzessive die Fälle (2)-(8) aus Theorem 1.8 zu betrachten.

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

Im Folgenden werden Vektoren stets von links an Matrizen heranmultipliziert. Ferner bezeichne e_i den i-ten Einheitsvektor des Vektorraums $V := V(\frac{d}{a}, p^a)$ und $\langle e_i \rangle$ den von e_i erzeugten 1-dimensionalen Untervektorraum. Wirke G als Automorphismengruppe nun fahnentransitiv auf einem nicht-trivialen $3-(v,k,1)$ Design. Wir werden zeigen, dass in diesem Fall lediglich das oben genannte $SQS(2^d)$ mit $d \geq 3$ und $G \cong AGL(d,2)$ auftreten kann. Sei zunächst $p^a \neq 2$. Für $d = 2a$ sei $T := T(\langle e_1 \rangle) \leq G_0$ die Transvektionsuntergruppe zu $\langle e_1 \rangle$. Dann besteht T aus allen Elementen der Form

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

Offensichtlich lässt T als Punkte lediglich die Elemente von $\langle e_1 \rangle$ fest. Daher hat G_0 Bahnen mindestens der Länge p^a außerhalb der Geraden durch $0, e_1$. Sei nun $x \in \langle e_1 \rangle$. Falls der durch $0, e_1, x$ eindeutig bestimmte Block mindestens einen Punkt außerhalb der Geraden $\langle e_1 \rangle$ fest lassen würde, dann wäre folglich $k \geq p^a + 3$. Nach Korollar 1.5 haben wir jedoch in diesem Fall $k \leq p^a + 1$, ein Widerspruch. Also liegt der durch $0, e_1, x$ eindeutig bestimmte Block vollständig in $\langle e_1 \rangle$. Aufgrund der Fahnentransitivität von G liegt dann aber jeder Block in einer affinen Geraden. Nach der Definition von Steiner 3-Designs müssten aber je drei nicht-kollineare Punkte ebenso stets einen Block eindeutig bestimmen, ein Widerspruch.

Für $d \geq 3a$ betrachten wir $(\frac{d}{a} \times \frac{d}{a})$-Matrizen der Form

$$A_i := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ x_1 & & & & \\ 0 & & B_i & & \\ \vdots & & & & \\ 0 & & & & \end{pmatrix}, \; 1 \leq i \leq \tfrac{d}{a} - 1, \; x_1 \in GF(p^a) \text{ beliebig,}$$

wobei

$$B_1 := \begin{pmatrix} x_2 & x_3 & x_4 & \cdots & x_{\frac{d}{a}} \\ 0 & x_2^{-1} & & & \\ 0 & & 1 & * & \\ \vdots & 0 & & \ddots & \\ 0 & & & & 1 \end{pmatrix}, \; x_2 \neq 0,$$

$$B_2 := \begin{pmatrix} 0 & x_3 & x_4 & x_5 & \cdots & x_{\frac{d}{a}} \\ x_3^{-1} & 0 & & & & \\ 0 & & -1 & & * & \\ 0 & & & 1 & & \\ \vdots & & 0 & & \ddots & \\ 0 & & & & & 1 \end{pmatrix}, \; x_3 \neq 0$$

$$\text{und } B_i := \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & x_{i+1} & x_{i+2} & \cdots & x_{\frac{d}{a}} \\ 0 & 1 & & & & & & & \\ \vdots & & \ddots & & & & & & \\ 0 & & & 1 & & & * & & \\ 0 & & & & -1 & & & & \\ x_{i+1}^{-1} & & & & & 0 & & & \\ 0 & & & & & & 1 & & \\ \vdots & & & 0 & & & & \ddots & \\ 0 & & & & & & & & 1 \end{pmatrix}, \; x_{i+1} \neq 0, \; 3 \leq i \leq \tfrac{d}{a} - 1.$$

Offensichtlich gilt $B_i \in SL(\frac{d}{a}-1, p^a)$ für $1 \leq i \leq \frac{d}{a}-1$, und daher $A_i \in SL(\frac{d}{a}, p^a)_{e_1}$ nach dem Entwicklungssatz von Laplace. Da wir bei Multiplikation von e_2 mit den Matrizen A_i $(1 \leq i \leq \frac{d}{a} - 1)$ als Bilder genau die Vektoren von $V \setminus \langle e_1 \rangle$ erhalten, wirkt $SL(\frac{d}{a}, p^a)_{e_1}$ transitiv außerhalb der Geraden durch $0, e_1$, und daher auch G_{0,e_1}. Nun wählen wir wieder $x \in \langle e_1 \rangle$. Falls der durch $0, e_1, x$ eindeutig bestimmte Block einen Punkt außerhalb von $\langle e_1 \rangle$ fest lassen würde, dann müsste er folglich bereits alle Punkte außerhalb, also mindestens $p^d - p^a + 3$ viele, enthalten, im offensichtlichen Widerspruch zu Korollar 1.5. Also liegt der durch $0, e_1, x$ eindeutig bestimmte Block wiederum vollständig in $\langle e_1 \rangle$ und wir erhalten analog zu oben, dass auch hier G auf keinem nicht-trivialen $3-(v,k,1)$ Design fahnentransitiv operieren kann.

Sei nun $p^a = 2$. Um nicht-triviale $3-(v,k,1)$ Designs zu erhalten, muss $v = 2^d > 4$ gelten. Für $v = 8$ erhalten wir mit Lemma 1.2, dass notwendig $k = 4$ ist. Für $v > 8$ werden wir zeigen, dass ebenso lediglich Steinerquadrupelsysteme in Betracht kommen. Theorem 3.4 liefert dann die Behauptung.
Sei also $d > 3$. Da in $AG(d,2)$ je drei Punkte nicht-kollinear sind, bestimmen diese stets eindeutig eine affine Ebene. Sei $\mathcal{E} := \langle e_1, e_2 \rangle$ der von e_1 und e_2 erzeugte 2-dimensionale Untervektorraum. Wir betrachten $(d \times d)$-Matrizen der Form

$$A_i := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ x_1 & x_2 & & & \\ 0 & 0 & & B_i & \\ \vdots & \vdots & & & \\ 0 & 0 & & & \end{pmatrix}, \ 1 \leq i \leq d-2;\ x_1,\, x_2 \in GF(2) \text{ beliebig}$$

mit

$$B_1 := \begin{pmatrix} x_3 & x_4 & x_5 & \cdots & x_d \\ 0 & x_3^{-1} & & & \\ 0 & & 1 & * & \\ \vdots & & 0 & \ddots & \\ 0 & & & & 1 \end{pmatrix}, \ x_3 \neq 0,$$

$$B_2 := \begin{pmatrix} 0 & x_4 & x_5 & x_6 & \cdots & x_d \\ x_4^{-1} & 0 & & & & \\ 0 & & -1 & & * & \\ 0 & & & 1 & & \\ \vdots & & 0 & & \ddots & \\ 0 & & & & & 1 \end{pmatrix}, \ x_4 \neq 0$$

$$\text{und } B_i := \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & x_{i+2} & x_{i+3} & \cdots & x_d \\ 0 & 1 & & & & & & & \\ \vdots & & \ddots & & & & & & \\ 0 & & & 1 & & & \ast & & \\ 0 & & & & -1 & & & & \\ x_{i+2}^{-1} & & & & & 0 & & & \\ 0 & & & & & & 1 & & \\ \vdots & & & 0 & & & & \ddots & \\ 0 & & & & & & & & 1 \end{pmatrix}, \ x_{i+2} \neq 0,\ 3 \leq i \leq d-2.$$

Es gilt $B_i \in SL(d-2,2)$ für $1 \leq i \leq d-2$, und daher $A_i \in SL(d,2)_{\mathcal{E}}$. Durch Multiplikation von e_3 mit den Matrizen A_i $(1 \leq i \leq d-2)$ erhalten wir als Bilder genau die Vektoren von $V \setminus \mathcal{E}$. Somit wirkt $SL(d,2)_{\mathcal{E}}$, und daher auch $G_{0,\mathcal{E}}$, transitiv auf $V \setminus \mathcal{E}$. Falls nun der durch $0, e_1, e_2$ eindeutig bestimmte Block einen Punkt außerhalb von $\mathcal{E}$ enthalten würde, dann müsste er bereits alle Punkte von $V \setminus \mathcal{E}$ enthalten. Dann wäre aber $k \geq 2^d - 4 + 3 = 2^d - 1$, im Widerspruch zu Korollar 1.5. Daher liegt der durch $0, e_1, e_2$ eindeutig bestimmte Block vollständig in $\mathcal{E}$. Wegen der Fahnentransitivität von G liegt dann aber jeder Block in einer affinen Ebene. Daher gilt $k \leq 4$, und aufgrund der Definition von Steiner 3-Designs erhalten wir $k = 4$.

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

Wir werden zeigen, dass G als Automorphismengruppe auf keinem nichttrivialen $3-(v,k,1)$ Design fahnentransitiv operiert. Angenommen, die Behauptung wäre falsch. Sei zunächst $p^a \neq 2$. Auf den Punkten des zugehörigen projektiven Raums ist die Permutationsgruppe $PSp(\frac{2d}{a}, p^a)$ eine Rang 3 Gruppe und die Bahnen des Punktstabilisators sind bekannt (siehe beispielsweise [30, Kap. II, Satz 9.15 (b)]). Folglich hat $G_0 \trianglerighteq Sp(\frac{2d}{a}, p^a)$ genau zwei Bahnen auf $V \setminus \langle x \rangle$ $(0 \neq x \in V)$ mindestens der Länge

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

Sei $y \in \langle x \rangle$. Falls der durch $0, x, y$ eindeutig bestimmte Block mindestens einen Punkt von $V \setminus \langle x \rangle$ fest lassen würde, dann wäre daher $k > p^d + 3$. Andererseits gilt nach Korollar 1.5 in diesem Fall $k \leq p^d + 1$, ein Widerspruch. Somit können wir wie im Fall (2) argumentieren, um den gewünschten Widerspruch zu erhalten.

Sei nun $p^a = 2$. Um triviale $3-(v, k, 1)$ Designs auszuschließen, sei $v = 2^{2d} > 4$. Für $d = 2$ (hier gilt $Sp(4, 2) \cong S_6$ (vgl. [30, Kap. II, Satz 9.21])) haben wir $k \leq 5$ nach Korollar 1.5. Wegen $k - 2 \nmid v - 2$ für $k = 5$, genügt es nach Lemma 1.2 (d) den Fall $k = 4$ zu betrachten. Für $d > 2$ werden wir zeigen, dass wir uns ebenfalls auf Steinerquadrupelsysteme beschränken können. Wiederum mit Theorem 3.4 folgt dann die Behauptung.
Sei $\{x, y\}$ ein nach [30, Kap. II, Satz 9.6 (b)] stets existierendes hyperbolisches Paar in dem nicht-ausgearteten symplektischen Raum $V := V(2d, 2)$ und sei $\mathcal{E} := \langle x, y\rangle$ die von $\{x, y\}$ erzeugte hyperbolische Ebene. Aus dem Beweis von [30, Kap. II, Satz 9.13] ergibt sich $Sp(2d, 2)_{\{x,y\}} \cong Sp(2d - 2, 2)$. Wegen $\mathrm{Out}(Sp(2d, 2)) = 1$ (vgl. [33, S. 170, Table 5.1 B]) haben wir daher

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

Da $Sp(2d - 2, 2)$ transitiv wirkt auf den von 0 verschiedenen Vektoren des $(2d - 2)$-dimensionalen symplektischen Unterraums, sieht man leicht, dass die kleinste Bahn in $V \setminus \mathcal{E}$ unter $G_{0,\mathcal{E}}$ mindestens die Länge $2^{2d-2} - 1$ hat. Falls der durch 0 und $\{e_1, e_2\}$ eindeutig bestimmte Block B einen Punkt von $V \setminus \mathcal{E}$ enthalten würde, dann wäre bereits $k \geq 2^{2d-2} - 1 + 3 = 2^{2d-2} + 2$, im Widerspruch zu Korollar 1.5. Daher liegt der Block B vollständig in $\mathcal{E}$. Aufgrund der Fahnentransitivität von G liegt dann aber jeder Block in einer affinen Ebene. Somit gilt $k \leq 4$, und nach der Definition von Steiner 3-Designs erhalten wir $k = 4$.

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

Wir werden hier ebenfalls zeigen, dass G als Automorphismengruppe auf keinem nicht-trivialen $3 - (v, k, 1)$ Design fahnentransitiv operieren kann. Wieder nehmen wir an, die Behauptung wäre falsch. Sei zunächst $a = 1$. Dann haben wir $v = 2^6 = 64$ und nach Korollar 1.5 folglich $k \leq 9$. Andererseits gilt $|G_2(2)'| = 2^5 \cdot 3^3 \cdot 7$ und $|\mathrm{Out}(G_2(2)')| = 2$ (vgl. [14, S. 14]). Wir erhalten mit Lemma 2.1 daher

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

Dies bedeutet jedoch, dass k ein Vielfaches von 32 oder 33 ist, ein Widerspruch.

Sei nun $a > 1$. Da hier $G_2(2^a)$ nicht-abelsch einfach ist, genügt es, $G_0 \trianglerighteq G_2(2^a)$ zu betrachten. Als Permutationsgruppe ist $G_2(2^a)$ eine Rang 4 Gruppe und für

$0 \neq x \in V$ hat $G_2(2^a)_x$ genau drei Bahnen $\mathcal{O}_i$ $(i = 1, 2, 3)$ auf $V \setminus \langle x \rangle$ der Länge $q^3 - q, q^5 - q^3, q^6 - q^5$ (siehe beispielsweise [2] oder [11, Theorem 3.1].) Somit hat G_0 genau drei Bahnen auf $V \setminus \langle x \rangle$ mindestens der Länge $|\mathcal{O}_i|$. Sei $y \in \langle x \rangle$. Wir zeigen wiederum, dass der durch $0, x, y$ eindeutig bestimmte Block B vollständig in $\langle x \rangle$ liegt.
Falls der Block B mindestens einen Punkt von $V \setminus \langle x \rangle$ in $\mathcal{O}_2$ oder $\mathcal{O}_3$ enthält, dann erhalten wir wie oben einen Widerspruch zu Korollar 1.5. Es bleibt also nur zu betrachten, dass B Punkte aus $V \setminus \langle x \rangle$ enthält, die alle in $\mathcal{O}_1$ liegen. Nach [2] ist die Bahn $\mathcal{O}_1$ genau bekannt und es gilt

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

wobei $x\Delta := \{y \in V \mid f(x, y, z) = 0 \text{ für alle } z \in V\}$ mit einer alternierenden Trilinearform f auf V. Dann besteht der Block B, ausgenommen von Elementen aus $\langle x \rangle$, genau aus $\mathcal{O}_1$. Wegen $|\mathcal{O}_1| \neq 1$ können wir $\langle \bar{x} \rangle \in x\Delta$ wählen mit $\langle \bar{x} \rangle \neq \langle x \rangle$. Aus Symmetriegründen bestimmen dann aber $0, \bar{x}, \bar{y}$ mit $\bar{x} \neq \bar{y} \in \langle \bar{x} \rangle$ ebenso eindeutig den Block B, ein Widerspruch zur Definition von Steiner 3-Designs. Somit liegt B vollständig in $\langle x \rangle$, und wir können wie in den obigen Fällen argumentieren.

Fall (5): $G_0 \cong A_6$ oder A_7, $v = 2^4$. Wegen $v = 2^4$ gilt $k \leq 5$ nach Korollar 1.5. Falls $k = 4$ ist, dann liefert Theorem 3.4 den Teil (ii) unserer Behauptung. Für $k = 5$ erhalten wir mit Lemma 1.2 (d) einen Widerspruch.

Fälle (6)-(8): Für die Existenz von nicht-trivialen $3-(v, k, 1)$ Designs haben wir in diesen Fällen nur endlich viele Möglichkeiten für k zu betrachten. Diese können mithilfe von Korollar 1.5 und Lemma 1.2 (b) und (d) leicht von Hand ausgeschlossen werden, und der Satz ist bewiesen. □

4.3 Klassifikation bei kleinen Blöcken

Proposition 4.3. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $3-(v,k,1)$ Design. Falls $G \leq \mathrm{Aut}(\mathcal{D})$ mit $PSU(3,q^2) \leq G \leq P\Gamma U(3,q^2)$, $q := p^a > 2$ eine Primzahlpotenz, fahnentransitiv auf $\mathcal{D}$ operiert, dann gelten die folgenden Aussagen, wobei $a_0 := |G|/(q^3+1)q^3(q^2-1)$ ist (sodass $\frac{1}{3} \leq a_0 \leq 2a$ gilt):*

(a) $k \,\big|\, (q^3+1)q^3(q^2-1)a_0$ *und* $r \geq q^3$.

(b) $\Phi_3(q) \,\big|\, (k-1)(k-2)a_0$.

Insbesondere gilt $k \equiv 1$ oder $2 \pmod{6n+1}$ für mindestens ein $n \in \mathbb{N}$.
Falls $q \equiv 1 \pmod 3$ ist, dann gilt zusätzlich $(k-1)(k-2)a_0 \equiv 0 \pmod 3$.

Beweis. ad (a): Da G fahnentransitiv ist, gilt $k \,\big|\, |G_B| \,\big|\, |G|$ für $B \in \mathcal{B}$ beliebig, und daher die erste Behauptung. Die Menge der Blöcke durch einen beliebigen Punkt $x \in X$ bilden die Blöcke eines $2-(v-1,k-1,1)$ Designs $\mathcal{D}_x$. Mit [39, Theorem 1] ist die Anzahl dieser Blöcke $r \geq q^3$.

ad (b): Wegen $(q^2+q+1, q+1) = 1$ erhalten wir durch vollständiges Kürzen die Teilbarkeitsaussage aus Lemma 2.1. Da $a \leq \frac{q}{2}$ gilt, folgt $3a_0 < \Phi_3(q)$ für alle q. Somit enthält $k-1$ oder $k-2$ aufgrund von Bemerkung 1.10 mindestens einen Faktor der Form $6n+1$ ($n \in \mathbb{N}$), und es gilt zusätzlich $(k-1)(k-2)a_0 \equiv 0 \pmod 3$, falls $q \equiv 1 \pmod 3$ ist. □

Entsprechend erhalten wir Proposition 4.4 (man beachte, dass hier stets $q \not\equiv 1 \pmod 3$ gilt) und Proposition 4.5. Für $|\mathrm{Out}(^2G_2(q))|$ und $|\mathrm{Out}(Sz(q))|$ verweisen wir dabei auf [33, S. 170, Table 5.1 B].

Proposition 4.4. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $3-(v,k,1)$ Design. Falls $G \leq \mathrm{Aut}(\mathcal{D})$ mit $^2G_2(q) \leq G \leq \mathrm{Aut}(^2G_2(q))$, $q := 3^{2e+1} > 3$, fahnentransitiv auf $\mathcal{D}$ operiert, dann gelten die folgenden Aussagen, wobei $a_0 := |G|/(q^3+1)q^3(q-1)$ ist (sodass $1 \leq a_0 \leq 2e+1$ gilt):*

(a) $k \,\big|\, (q^3+1)q^3(q-1)a_0$ *und* $r \geq q^3$.

(b) $\Phi_3(q) \,\big|\, (k-1)(k-2)a_0$.

Insbesondere gilt $k \equiv 1$ oder $2 \pmod{6n+1}$ für mindestens ein $n \in \mathbb{N}$.

Proposition 4.5. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $3-(v,k,1)$ Design. Falls $G \leq \mathrm{Aut}(\mathcal{D})$ mit $Sz(q) \leq G \leq \mathrm{Aut}(Sz(q))$, $q := 2^{2e+1} > 2$, fahnentransitiv auf $\mathcal{D}$ operiert, dann gelten die folgenden Aussagen, wobei $a_0 := |G| / (q^2+1)q^2(q-1)$ ist (sodass $1 \leq a_0 \leq 2e+1$ gilt):*

(a) $k \mid (q^2+1)q^2(q-1)a_0$ *und* $r \geq q^2$.

(b) $\Phi_2(q) \mid (k-1)(k-2)a_0$.

Theorem 4.6. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $3-(v,5,1)$ Design. Genau dann operiert $G \leq \mathrm{Aut}(\mathcal{D})$ fahnentransitiv auf $\mathcal{D}$, wenn $\mathcal{D}$ isomorph ist zu einem $3-(4^d+1,5,1)$ Design, dessen Punkte die Elemente von $GF(4^d) \cup \{\infty\}$ und dessen Blöcke die Bilder von $GF(4) \cup \{\infty\}$ unter $PGL(2,4^d)$ mit $d \geq 2$ (resp. $PSL(2,4^d)$ mit $d > 1$ ungerade) sind, und das abgeleitete Design ist isomorph zum $2-(4^d,4,1)$ Design, bestehend aus den Punkten und Geraden von $AG(d,4)$, und $PSL(2,4^d) \leq G \leq P\Gamma L(2,4^d)$.*

Beweis. Wegen Korollar 2.3 werden wir wieder die in Theorem 1.8 angegebenen Gruppen G sukzessive daraufhin untersuchen, ob G als Automorphismengruppe fahnentransitiv auf einem nicht-trivialen $3-(v,5,1)$ Design operiert.

(A) Affiner Fall.

Fall (1): $G \leq A\Gamma L(1,p^d)$.

Für die Existenz fahnentransitiver $3-(v,5,1)$ Designs muss nach Lemma 2.1 notwendig

$$\begin{aligned} &\frac{(p^d-1)(p^d-2)}{4\cdot 3} \mid |G_0| \mid d(p^d-1) \\ \iff & p^d-2 \mid d\cdot 4\cdot 3 \qquad (*) \end{aligned}$$

gelten. Die Ungleichung $p^d-2 \leq d\cdot 4\cdot 3$ gilt bei $p=2$ nur für $d<7$, bei $p=3$ für $d<4$, bei $p=5$ für $d<3$ und bei $p=7$ für $d<2$. Falls $d=1$ ist, dann ist die Ungleichung lediglich für $2 \leq p \leq 13$ erfüllt. Von diesen endlich vielen Möglichkeiten erfüllen jedoch nur $p^d = 3,4,5,8,32$ das Teilbarkeitskriterium $(*)$. Da wir triviale $3-(v,5,1)$ Designs ausschließen, bleiben in der Tat nur $v = p^d = 8$ und 32 zu betrachten. In beiden Fällen erhalten wir aber mit Lemma 1.2 (c) deren Nicht-Existenz.

Fälle (2)-(8): Nach Satz 4.2 existieren in diesen Fällen keine nicht-trivialen fahnentransitiven $3-(v,5,1)$ Designs.

(B) Fasteinfacher Fall.

Fall (1): $N = A_v$, $v \geq 5$. Hier ist G 3-fach transitiv und operiert nach [32, Theorem 3] auf keinem nicht-trivialen $3-(v,k,1)$ Design.

Fall (2): $N = PSL(d,q)$, $d \geq 2$, $v = \frac{q^d-1}{q-1}$, wobei $(d,q) \neq (2,2),(2,3)$. Mit Satz 4.1 erhalten wir für $k = 5$ das angegebene Design.

Fall (3): $N = PSU(3,q^2)$, $v = q^3+1$, $q > 2$. Aus Proposition 4.3 folgt, dass für $k \leq 7$ keine nicht-trivialen fahnentransitiven $3-(v,k,1)$ Designs existieren können.

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

Für $q \geq 2^7$ gilt stets $\Phi_2(q) > (k-1)(k-2)a_0$. Für die übrigen Werte von q ist Proposition 4.5 (b) lediglich für $q = 8$ erfüllt, und dies auch nur, wenn $G \cong \mathrm{Aut}(Sz(8))$ ist. Angenommen, G wirke in diesem Falle fahnentransitiv auf einem nicht-trivialen $3-(65,5,1)$ Design. Insbesondere ist G dann blocktransitiv. Nach der Bahnenformel (1.7) hat der Stabilisator G_B eines beliebigen Blocks $B \in \mathcal{B}$ daher die Ordnung 20, denn es gilt $|G| = 65 \cdot 64 \cdot 7 \cdot 3$ (vgl. beispielsweise [33, S. 170, Table 5.1 B]). Andererseits hat G nach dem Satz von Sylow eine 3-Sylowuntergruppe U. Wegen $v = 65 \equiv 2 \pmod 3$ besitzt U mindestens zwei Fixpunkte. Im Folgenden werden wir zeigen, dass U sogar mindestens drei Fixpunkte hat.
Die Untergruppe U lässt eine 2-Sylowuntergruppe der Ordnung 64 fest, daher auch ihr Zentrum der Ordnung 8. Wegen $7 \equiv 1 \pmod 3$ kommutiert U als Gruppe von Automorphismen auf dem Zentrum mit mindestens einem Gruppenelement $\tau \neq 1$ der Ordnung 2. Das Element τ operiert auf der Fixpunktmenge von U, und U kommutiert mit τ. Folglich kommutiert auch τ mit U und lässt die Fixpunktmenge von U invariant. Da Involutionen in $Sz(q)$ genau einen Fixpunkt haben (siehe z. B. [31, Kap. XI, Lemma 1.7 (b)]), wird einer der beiden obigen Fixpunkte von τ bewegt. Daher hat U mindestens drei Fixpunkte. Dies bedeutet aber, dass U nach der Definition von Steiner 3-Designs im Stabilisator des durch diese drei Fixpunkte eindeutig bestimmten Blocks liegt. Jedoch hat dieser, wie oben gezeigt, die Ordnung 20, ein Widerspruch nach dem Satz von Lagrange.

Fall (5): $N = {}^2G_2(q)$, $v = q^3 + 1$, $q = 3^{2e+1} > 3$. Für $k \leq 7$ existieren nach Proposition 4.4 keine nicht-trivialen fahnentransitiven $3 - (v, k, 1)$ Designs.

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

Wegen $2 \nmid (2^{2d-1} \pm 2^{d-1} - 1)(2^{2d-2} \pm 2^{d-2} - 1)$ folgt $(k-1)(k-2) \nmid (v-1)(v-2)$. Daher kann G nach Lemma 1.2 (c) auf keinem $3 - (v, 5, 1)$ Design operieren.

Fälle (7)-(13): Im Fall (9) ist G stets 3-fach transitiv und mit [32, Theorem 3] können wir folgern, dass G lediglich auf dem zugehörigen Witt Design fahnentransitiv operiert. Für $k = 5$ existiert jedoch kein solches. In den übrigen Fällen können wir mittels Korollar 1.5 und Lemma 1.2 (c) und (d) leicht zeigen, dass für die vorgegebenen Werte von v keine $3 - (v, 5, 1)$ Designs existieren können, und das Theorem ist bewiesen. □

Theorem 4.7. *Sei $\mathcal{D} = (X, \mathcal{B}, I)$ ein nicht-triviales $3 - (v, 6, 1)$ Design. Genau dann operiert $G \leq \mathrm{Aut}(\mathcal{D})$ fahnentransitiv auf $\mathcal{D}$, wenn einer der beiden Fälle auftritt:*

(1) *$\mathcal{D}$ ist isomorph zu einem $3-(5^d+1, 6, 1)$ Design, dessen Punkte die Elemente von $GF(5^d) \cup \{\infty\}$ und dessen Blöcke die Bilder von $GF(5) \cup \{\infty\}$ unter $PGL(2, 5^d)$ mit $d \geq 2$ (resp. $PSL(2, 5^d)$ mit $d > 1$ ungerade) sind, und das abgeleitete Design ist isomorph zum $2 - (5^d, 5, 1)$ Design, bestehend aus den Punkten und Geraden von $AG(d, 5)$, und $PSL(2, 5^d) \leq G \leq P\Gamma L(2, 5^d)$,*

(2) *$\mathcal{D}$ ist isomorph zum Witt $3 - (22, 6, 1)$ Design, und $G \trianglerighteq M_{22}$.*

Beweis. Wiederum können wir von Theorem 1.8 ausgehen.

(A) Affiner Fall.

Fall (1): $G \leq A\Gamma L(1, p^d)$. Analog zum entsprechenden Fall in Theorem 4.6 erhalten wir mit den übrigen Aussagen von Lemma 1.2, dass auch hier keine nicht-trivialen fahnentransitiven $3 - (v, 6, 1)$ Designs existieren.

Die Fälle (2)-(13) lassen sich wieder mit Satz 4.2 ausschließen.

(B) Fasteinfacher Fall.

Die Fälle (1)-(3), (5), (7)-(13) lassen sich analog zu denen in Theorem 4.6 behandeln. In Fall (9) ergibt sich hierbei das angegebene Witt-Design.

Fall (4): $N = Sz(q)$, $v = q^2 + 1$, $q = 2^{2e+1} > 2$. Für $q \geq 2^9$ gilt stets $\Phi_2(q) > (k-1)(k-2)a_0$. Für die übrigen Werte von q ist Proposition 4.5 (b) ebenfalls nicht erfüllt, sodass wir hier keine nicht-trivialen fahnentransitiven $3-(v,6,1)$ Designs erhalten können.

Fall (6): $N = Sp(2d,2)$, $d \geq 3$, $v = 2^{2d-1} \pm 2^{d-1}$. Da $2^{2d-2} \pm 2^{d-2} - 1$ stets ungerade ist, erhalten wir, dass $k-2$ kein Teiler von $v-2$ sein kann. Folglich operiert G nach Lemma 1.2 (d) auf keinem nicht-trivialen $3-(v,6,1)$ Design, und die Behauptung ist gezeigt. □

Theorem 4.8. *Es existiert kein nicht-triviales* $3-(v,7,1)$ *Design mit einer fahnentransitiven Automorphismengruppe.*

Beweis. Der affine Fall ergibt sich wie in Theorem 4.7. Es bleibt also nur noch zu betrachten:

(B) Fasteinfacher Fall.

In den Fällen (1)-(3), (5), (7)-(13) können wir wieder wie in Theorem 4.6 vorgehen. Offensichtlich kann dabei für $k = 7$ der Fall (2) nicht auftreten.

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

Für $q \geq 2^9$ gilt stets $\Phi_2(q) > (k-1)(k-2)a_0$. Für die übrigen Werte von q ist Proposition 4.5 (b) lediglich für $q = 8$ erfüllt. Jedoch erhalten wir in diesem Fall wegen $v = 65$ einen Widerspruch zu Lemma 1.2 (d). Also existieren auch hier keine nicht-trivialen fahnentransitiven $3-(v,7,1)$ Designs.

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

Falls G auf einem nicht-trivialen $3-(v,7,1)$ Design operiert, dann muss nach Lemma 1.2 (d) notwendig $k-2 \mid v-2$, also $5 \mid 2(2^{2d-2} \pm 2^{d-2} - 1)$ gelten. Dies ist gleichbedeutend zu $2^{2d-2} \pm 2^{d-2} - 1 \equiv 0 \pmod 5$. Nun sieht man aber leicht (durch einfaches Einsetzen bzw. Rechnen in $GF(5)$), dass $4x^2 \pm x \not\equiv 1 \pmod 5$ gilt, und folglich $2^{2n+2} \pm 2^n \not\equiv 1 \pmod 5$ für $n \geq 1$. Mit $n := d-2$ erhalten wir dann aber $2^{2d-2} \pm 2^{d-2} \not\equiv 1 \pmod 5$, ein Widerspruch. Daher folgt die Behauptung. □

Literaturverzeichnis

[1] A. Aigner, *Zahlentheorie*, De Gruyter, Berlin, New York, 1975.

[2] M. Aschbacher, *Chevalley groups of type G_2 as the group of a trilinear form*, J. Algebra **109** (1987), 193–259.

[3] M. Aschbacher, *Sporadic Groups*, Cambridge Univ. Press, Cambridge, 1994.

[4] Th. Beth, D. Jungnickel und H. Lenz, *Design Theory*, Vol. I und II, Encyclopedia of Math. and Its Applications **69**, Cambridge Univ. Press, Cambridge, 1999.

[5] A. Betten, R. Laue und A. Wassermann, *A Steiner 5-Design on 36 points*, Designs, Codes, Cryptography **17** (1999), 181–186.

[6] A. Beutelspacher, *Einführung in die endliche Geometrie I: Blockpläne*, Bibliographisches Institut, Mannheim, Wien, Zürich, 1982.

[7] R. E. Block, *Transitive groups of collineations on certain designs*, Pacific J. Math. **15** (1965), 13–18.

[8] R. H. Bruck und H. J. Ryser, *The non-existence of certain finite projective planes*, Canad. J. Math. **1** (1949), 88–93.

[9] F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck und J. Saxl, *Linear spaces with flag-transitive automorphism groups*, Geom. Dedicata **36** (1990), 89–94.

[10] P. J. Cameron, *Parallelisms of Complete Designs*, London Math. Soc. Lecture Note Series **23**, Cambridge Univ. Press, Cambridge, 1976.

[11] P. J. Cameron und W. M. Kantor, 2-*transitive and antiflag transitive collineation groups of finite projective and polar spaces*, J. Algebra **60** (1979), 384–422.

[12] R. W. Carter, *Simple Groups of Lie Type*, J. Wiley, New York, 1972; Nachdruck: J. Wiley, 1989.

[13] P. C. Clapham, *Steiner triple systems with block-transitive automorphism groups*, Discrete Math. **14** (1976), 121–131.

[14] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker und R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[15] C. W. Curtis, G. M. Seitz und W. M. Kantor, *The* 2-*transitive permutation representations of the finite Chevalley groups*, Trans. Amer. Math. Soc. **218** (1976), 1–59.

[16] A. Delandtsheer, *Finite (line, plane)-flag-transitive planar spaces*, Geom. Dedicata **41** (1992), 145–153.

[17] A. Delandtsheer, *Dimensional linear spaces*, in: Handbook of Incidence Geometry, hrsg. von F. Buekenhout, Elsevier Science, Amsterdam, 1995, 193-294.

[18] A. Delandtsheer, J. Doyen, J. Siemons und C. Tamburini, *Doubly homogeneous* $2-(v,k,1)$ *designs*, J. Combin. Theory, Series A **43** (1986), 140–145.

[19] P. Dembowski, *Finite Geometries*, Springer, Berlin, Heidelberg, New York, 1968; Nachdruck: Springer, 1997.

[20] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901; Nachdruck: Dover Publications, New York, 1958.

[21] D. Gorenstein, *Finite Simple Groups. An Introduction to Their Classification*, Plenum Press, New York, London 1982.

[22] H. Hanani, *On quadruple systems*, Canad. J. Math. **12** (1960), 145–157.

[23] Ch. Hering, *Zweifach transitive Permutationsgruppen, in denen* 2 *die maximale Anzahl von Fixpunkten von Involutionen ist*, Math. Z. **104** (1968), 150–174.

[24] Ch. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*, Geom. Dedicata **2** (1974), 425–460.

[25] J. Höchsmann, *On minimal p-degrees in* 2*-transitive permutation groups*, Arch. Math **72** (1999), 405–417.

[26] M. Huber, $t-(v,k,1)$ *Designs mit fahnentransitiver Automorphismengruppe*, Diplomarbeit, Univ. Tübingen, Tübingen, 1999.

[27] M. Huber, *Classification of flag-transitive Steiner quadruple systems*, J. Combin. Theory, Series A **94** (2001), 180–190.

[28] D. R. Hughes und F. C. Piper, *Design Theory*, Cambridge Univ. Press, Cambridge, 1985.

[29] B. Huppert, *Zweifach transitive, auflösbare Permutationsgruppen*, Math. Z. **68** (1957), 126–150.

[30] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, Heidelberg, New York, 1967.

[31] B. Huppert und N. Blackburn, *Finite Groups III*, Springer, Berlin, Heidelberg, New York, 1982.

[32] W. M. Kantor, *Homogeneous designs and geometric lattices*, J. Combin. Theory, Series A **38** (1985), 66–74.

[33] P. B. Kleidman und M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series **129**, Cambridge Univ. Press, Cambridge, 1990.

[34] H. Kurzweil und B. Stellmacher, *Theorie der endlichen Gruppen*, Springer, Berlin, Heidelberg, New York, 1998.

[35] C. Lam, L. Thiel und S. Swiercz, *The non-existence of finite projective planes of order* 10, Canad. J. Math. **41** (1989), 1117–1123.

[36] C. C. Lindner und A. Rosa, *There are at least* $31,021$ *non-isomorphic Steiner quadruple systems of order* 16, Utilitas Math. **10** (1976), 61–64.

[37] H. Lüneburg, *Die Suzukigruppen und ihre Geometrien*, Lecture Notes in Math. **10**, Springer, Berlin, Heidelberg, New York, 1965.

[38] H. Lüneburg, *Fahnenhomogene Quadrupelsysteme*, Math. Z. **89** (1965), 82–90.

[39] D. K. Ray-Chaudhuri und R. M. Wilson, *On t-designs*, Osaka J. Math. **12** (1975), 737–744.

[40] R. M. Robinson, *The structure of certain triple systems*, Math. Comput. **29** (1975), 223–241.

[41] E. Witt, *Die 5-fach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg **12** (1938), 256–264.

[42] E. Witt, *Über Steinersche Systeme*, Abh. Math. Sem. Univ. Hamburg **12** (1938), 265–275.

[43] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. für Math. u. Phys. **3** (1892), 265–284.

Lebenslauf

22.12.1972	geboren in Geislingen/ Steige als Sohn des Andreas und der Astrid Huber, geb. Treml
1979-1983	Besuch der Grundschule in Merklingen
1983-1992	Besuch des Albert-Schweitzer-Gymnasiums in Laichingen
16.6.1992	Abitur
1992-1993	Zivildienst bei der Heilsarmee in Hamburg
WS 1993/1994	Beginn des Lehramtsstudiengangs für Gymnasien in den Hauptfächern Mathematik und Deutsch
WS 1995/1996	Auslandsstipendium an der University of Massachussetts in Amherst/ USA
4.7.1997	Heirat mit Susanne Huber, geb. Kötzer
1997-1999	wiss. Hilfskraft an der Universität Tübingen
WS 1998/1999	Beginn des Diplomstudiengangs Mathematik mit Nebenfach Germanistik (Doppelstudium)
13.10.1998	Staatsexamen in Deutsch
19.4.1999	Staatsexamen in Mathematik
23.6.1999	Diplom in Mathematik
Juli 1999	Beginn der Dissertation bei Prof. Dr. Ch. Hering
seit 1.9.1999	wiss. Angestellter an der Universität Hohenheim

Meine akademischen Lehrer in Mathematik waren die Herren Professoren und Dozenten

R. Bödi, U. Felgner, Ch. Hering, M. Hochbruck, W. Knapp, F. Loose, Ch. Lubich, E. Manes, R. Nagel, F. Räbiger, H. Salzmann, P. Schmid, D. St. Mary, M. Voit, C. Zirbel