

Translationsebenen der Ordnung 32

Diplomarbeit
im Fachbereich Mathematik
der Technischen Universität Kaiserslautern

vorgelegt von
Robert Rockenfeller
eingereicht am 23.09.2011

Betreuer
Prof. Dr. Ulrich Dempwolff

Vorwort

Die Idee zu dieser Arbeit lieferte der Vortrag von Rudolf Mathon von der Universität Toronto über „Translation planes of order 32 with non-trivial translation complement“ (siehe [MAT] und Anhang A.1). In diesem Vortrag behauptet Mathon, dass es, bis auf Isomorphie, genau neun verschiedene Translationsebenen der Ordnung 32 gibt, die ein nicht-triviales Translationskomplement besitzen.

Da das Untersuchen von Translationsebenen sehr viele Aufschlüsse über die Struktur allgemeiner projektiver Ebenen liefert, ist natürlich eine Liste aller bekannter Translationsebenen kleinerer Ordnung ≤ 100 erstrebenswert. Eine solche Liste bis zur Ordnung 32 bietet [MOR]. Des Weiteren wurden etwa durch Ulrich Dempwolff oder Rudolf Mathon die Ebenen der Ordnung 49, 64 und 81 klassifiziert.

Diese Arbeit versucht, die Behauptung von Mathon zu belegen und die Liste der Translationsebenen kleiner Ordnung zu erweitern.

Im ersten Abschnitt des ersten Kapitels geben wir einen Überblick über die Begriffe aus der (linearen) Algebra, die wir in dieser Arbeit voraussetzen.

Einen Überblick über die Begriffe aus der projektiven Geometrie gibt Abschnitt zwei. Es werden Notationen festgelegt und einfache Sätze ohne Beweise angegeben. Die Grundlagen können sämtlich etwa in [DEM], [LÜN] oder [KAL] nachgelesen werden.

Der dritte Abschnitt bietet eine grundlegende Beschreibungen von Translationsebenen im Sinne von [DEM] durch so genannte *Faserungen* oder *Spreads*. Da wir uns mit Translationsebenen der Ordnung 32 befassen, setzen wir voraus, dass alle betrachteten Ebenen endlich sind. Es sei darauf hingewiesen, dass viele der im Kapitel angegebenen Begriffe und Eigenschaften auch ohne die Endlichkeitsvoraussetzung auskommen.

Das für unsere Berechnungen verwendete Programmpaket GAP wird in Abschnitt vier näher erläutert.

In Kapitel zwei wird die Behauptung von Mathon aufgegriffen und durch einen Satz beschrieben. Der Beweis dieses Satzes erfolgt durch eine Untersuchung aller möglicher Automorphismen von Primzahlordnung, bei der erst die Struktur des zugehörigen Translationskomplementes theoretisch untersucht wird und anschließend die Berechnung am Computer erfolgt.

Ein gesondertes Kapitel gilt der Untersuchung symplektischer Spread-Mengen im Sinne von [DEM, Kap. 12, S. 112] und [KAN]. Es wird sich zeigen, dass die zunächst unscheinbare Voraussetzung, Spread-Mengen mit symmetrischen Matrizen erzeugen zu wollen, eine neue Herangehensweise fordert.

Im Anschluss erfolgt in Kapitel vier eine Identifikation aller gefundenen Translationsebenen. Neben der Desargueschen Ebene finden wir acht weitere, die als Konsequenz aus [PRI] und [WAL] schon bekannt sind und im Falle der Automorphismen der Ordnung 31 sogar zur Entstehung des Artikels [POL] geführt haben.

Eine konkrete Angabe der Erzeuger der Translationskomplemente, der Automorphismengruppenordnung sowie der Erzeuger aller Spread-Mengen finden sich in Kapitel fünf.

Zum Schluss findet in Kapitel sechs ein Exkurs über fraktional-dimensionale Unterebenen unserer Ebenen statt. Diese wurden zuletzt von Vikram Jha und Norman Johnson in [DIM] untersucht.

Inhaltsverzeichnis

1. Grundlagen	7
1.1. Grundlagen aus der linearen Algebra und Algebra	7
1.2. Grundlagen aus der projektiven Geometrie	9
1.3. Grundlagen über Translationsebenen	12
1.4. Die verwendete Software	25
2. Die Translationsebenen der Ordnung 32	26
2.1. Hauptergebnis und elementare Beweise	26
2.2. Kollineationen der Ordnung 31	30
2.2.1. Theoretische Vorbereitung der Computersuche	30
2.2.2. Praktische Durchführung	33
2.3. Kollineationen der Ordnung 11	35
2.3.1. Theoretische Vorbereitung der Computersuche	35
2.3.2. Praktische Durchführung	36
2.4. Kollineationen der Ordnung 7	38
2.4.1. Theoretische Vorbereitung der Computersuche	38
2.4.2. Praktische Durchführung	41
2.5. Kollineationen der Ordnung 5	42
2.5.1. Theoretische Vorbereitung der Computersuche	42
2.5.2. Praktische Durchführung	44
2.6. Kollineationsgruppen der Ordnung 6	46
2.6.1. Theoretische Vorbereitung der Computersuche	46
2.6.2. Praktische Durchführung	50
2.7. Kollineationsgruppe der Ordnung 4	51
2.7.1. Theoretische Vorbereitung der Computersuche	51
2.7.2. Praktische Durchführung	54
3. Symplektische Spread-Mengen	55
3.1. Theoretische Vorbereitung der Computersuche	55
3.2. Praktische Durchführung	63
4. Identifikation der Ebenen	68
4.1. Kollineationen der Ordnung 31	68
4.2. Kollineationen der Ordnung 11	68
4.3. Kollineationen der Ordnung 5	68
4.4. Kollineationsgruppe der Ordnung 4	68
4.5. Symplektische Spread-Mengen	69
5. Die neun Translationsebenen der Ordnung 32	70
6. Fraktional-Dimensionale Unterebenen	74

Inhaltsverzeichnis

A. Anhang	77
A.1. Originalvortrag von Prof. Rudolf Mathon	77
B. Literatur	91
C. Erklärung	93

Symbolverzeichnis

Symbol	Bedeutung
\mathbb{A}	Affine Ebene
\mathbb{P}	Projektive Ebene
\mathbb{T}	Affine oder projektive Translationsebene
$A \cong B$	A ist isomorph zu B
\mathbf{S}	Spread-Menge
$\mathbb{T}(\mathbf{S})$	Translationsebene bezüglich einer Spread-Menge \mathbf{S}
\mathfrak{S}	Faserung einer Translationsebene
$\mathfrak{S}(\mathbf{S})$	Faserung bezüglich einer Spread-Menge \mathbf{S}
$GL(n, q)$	Allgemeine lineare Gruppe vom Grad n über $GF(q)$
$SL(n, q)$	Spezielle lineare Gruppe vom Grad n über $GF(q)$
A^t	Die zu A transponierte Matrix
$\text{diag}(A, A)$	Diagonalmatrix der Form $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$
M_{k*}	Die k -te Zeile der Matrix M
M_{*k}	Die k -te Spalte der Matrix M
K^*	Einheitengruppe eines Körpers K
$N_G(U)$	Normalisator von U in G
$C_G(U)$	Zentralisator von U in G
$Syl_p(G)$	Menge der p -Sylowuntergruppen von G
$[A, B]$	Der Kommutator von A und B , d.h. $[A, B] = ABA^{-1}B^{-1}$
C_n	Zyklische Gruppe der Ordnung n
$U \sqcup W$	Disjunkte Vereinigung von U und W
$[n]$	Die Menge $\{1, 2, \dots, n\}$
$V(T)$	Fasern einer Translationsebene
$Rad(\beta)$	Radikal einer Bilinearform β
$G(\mathbf{S})$	Groß-Spread-Menge von \mathbf{S}
$\Delta(M), \Delta(\mathbf{S})$	Koeffizienten des charakt. Polynoms sowie des Minimalpolynoms von M , beziehungsweise aller $M \in \mathbf{S}$, als Vektor(en)
$\phi _V$	Die Abbildung ϕ eingeschränkt auf V
$\underbrace{\quad}_\in, \underbrace{\quad}_\equiv$	Nach Voraussetzung enthalten in oder gleich

1. Grundlagen

1.1. Grundlagen aus der linearen Algebra und Algebra

Lemma 1.1.

Sei V ein endlich-dimensionaler K -Raum und $X, Y \in GL(V)$. Genau dann sind X und Y konjugiert, wenn sie die gleiche rationale Normalform besitzen.

Beweis.

Konsequenz aus [BON, Kap. 3, S. 5ff]. □

Definition 1.2.

Sei W ein endlich-dimensionaler Vektorraum über einem endlichen Körper K . Eine zyklische Gruppe heißt **Singer-Gruppe**, wenn sie scharf transitiv auf $W \setminus \{0\}$ operiert. Ein Erzeugendes Element der Singer-Gruppe heißt **Singer-Zyklus**.

Bemerkung 1.3.

Bekannt ist:

- a) Singer-Zyklen können wie folgt konstruiert werden: Seien $\dim V = d$ über K . Identifiziere W mit K^d . Definiere für ein erzeugendes Element θ mit $\langle \theta \rangle = (K^d)^*$ die Abbildung

$$\Theta : K^d \rightarrow K^d, f \mapsto f\theta.$$

Die Gruppe $\langle \theta \rangle$ ist dann eine Singer-Gruppe.

Sei ferner $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0$ das Minimalpolynom von θ vom Grad d über K . Dann ist die Begleitmatrix

$$\beta := \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ 0 & & 0 & 1 \\ a_1 & a_2 & \cdots & a_d \end{pmatrix}$$

von f die Matrix eines Singer-Zykluses. Des Weiteren ist f Minimalpolynom und charakteristisches Polynom von β , siehe [BON, Kap. 3, S. 5].

- b) Alle Singer-Gruppen in $GL(V)$ sind konjugiert. Siehe [COS, S.98].
c) $N_{GL(V)}(Z) \cong Z \cdot C$, mit $C \cong Gal(GF(q^d) : K)$ nach [HUP, Kap. II, Satz 7.3, S. 187].

1. Grundlagen

Lemma 1.4.

Es sei $T \in GL(n, q)$ irreduzibel. Genau dann ist T zu T^k konjugiert, wenn $k \equiv q^l \pmod{|T|}$ für $0 \leq l < n$.

Beweis.

Nach Voraussetzung ist das Minimalpolynom $\mu_T \in K[X]$ irreduzibel vom Grad n . Also gilt

$$GF(q^n) \cong K[X] / \mu_T.$$

Sei ω eine Nullstelle von μ_T in $GF(q^n)$. Setze

$$g_\omega := (X - \omega) \cdot (X - \omega^q) \cdots (X - \omega^{q^{n-1}}).$$

Dann ist $g_\omega \in K[X]$ und g_ω annulliert ω . Also ist $g_\omega = \mu_T$ und folglich hat T die Eigenwerte $\omega, \omega^q, \dots, \omega^{q^{n-1}}$ über $GF(q^n)$.

Die rationale Normalform von T ist die Begleitmatrix $B = B(g_\omega)$ von g_ω . Auch T^{q^l} hat die Eigenwerte $\omega, \omega^q, \dots, \omega^{q^{n-1}}$, das heißt B ist ebenfalls Begleitmatrix von T^{q^l} . Aus Lemma 1.1 folgt, dass T zu T^{q^l} konjugiert ist.

Angenommen T^k ist ebenfalls zu T konjugiert, besitzt also ebenfalls die rationale Normalform B und die Eigenwerte $\omega, \omega^q, \dots, \omega^{q^{n-1}}$. Andererseits hat aber T^k die Eigenwerte $\omega^k, \omega^{kq}, \dots, \omega^{(kq)^{n-1}}$. Also für $0 \leq l < n$ gilt

$$\omega^k \equiv \omega^{q^l} \pmod{|T|}$$

das heißt $k \equiv q^l \pmod{|T|}$. □

Folgerung 1.5.

Es sei $B = B(f)$ die Begleitmatrix des irreduziblen Polynoms $f \in GF(q)[X]$ mit $\text{Grad}(f) = m$. Ferner sei $0 \leq j \in \mathbb{N}$ und $A \in GL(j + m, q)$ habe die rationale Normalform:

$$A := \begin{pmatrix} \mathbb{1}_{j \times j} & \\ & B \end{pmatrix}.$$

Genau dann ist A zu A^k konjugiert, wenn $k \equiv q^l \pmod{|T|}$ für $0 \leq l < m$

Beweis.

Angenommen $A^k = \begin{pmatrix} \mathbb{1} & \\ & B^k \end{pmatrix}$ sei zu A konjugiert. Dann muss B die rationale Normalform von B^k sein. Nach Lemma 1.4 gilt, dass $k \equiv q^l \pmod{|A|}$ für $0 \leq l < m$. Das heißt A ist genau zu den Potenzen A^{q^l} mit $0 \leq l < m$ konjugiert. □

1.2. Grundlagen aus der projektiven Geometrie

Definition 1.6.

Eine Inzidenzstruktur $\mathbb{A} = (P, L)$, wobei P die Menge der Punkte und L die Menge der Geraden bezeichnet, heißt **affine Ebene**, wenn folgende Axiome gelten:

1. *Inzidenz*: Zu je zwei Punkten $x, y \in P$ existiert genau eine Gerade $l \in L$ mit $x, y \in l$.
2. *Parallelenaxiom*: Zu jeder Geraden l und zu jedem Punkt p existiert genau eine zu l parallele Gerade g , die p enthält, d.h. $g \cap l = \emptyset$ oder $g = l$.
3. *Reichhaltigkeit*: Es gibt mindestens drei nicht kollineare Punkte. Dabei heißt eine Menge von Punkten **kollinear**, wenn sie auf einer gemeinsamen Geraden liegen, das heißt mit ihr inzident sind.

Definition 1.7.

Ein Paar $\mathbb{P} = (P, L)$ heißt **projektive Ebene**, wenn folgende Axiome gelten:

1. *Verbinden*: Zu je zwei Punkten $x, y \in P$ existiert genau eine Gerade $l \in L$ mit $x, y \in l$.
2. *Schneiden*: Zu je zwei Geraden $l, m \in L$ existiert genau ein Punkt $p \in P$ mit $p \in l \cap m$.
3. *Reichhaltigkeit*: Es existieren vier Punkte, von denen keine drei kollinear sind.

Bemerkung 1.8.

Jede affine Ebene kann durch Hinzunahme einer ausgezeichneten Geraden, der **unendlich fernen Geraden**, zu einer projektiven Ebene ergänzt werden, siehe [DEM, Kap 1.9, S. 5]. Wir bezeichnen die unendlich ferne Gerade mit l_∞ .

Zeichnet man in einer projektiven Ebene eine Gerade l_∞ aus, so nennt man diejenigen Punkte, die nicht auf l_∞ liegen **affin**.

Satz 1.9.

Zu einer projektiven Ebene \mathbb{P} existiert eine natürliche Zahl n , die **Ordnung** von \mathbb{P} , sodass gilt:

1. $|P| = |L| = n^2 + n + 1$.
2. Die Anzahl der Geraden, die durch einen Punkt gehen, ist gleich der Anzahl der Punkte pro Gerade ist gleich $n + 1$.

1. Grundlagen

Definition 1.10.

Ein **Morphismus** von Ebenen $\mathbb{P} = (P, L)$ und $\mathbb{P}' = (P', L')$ ist eine Abbildung $\varphi : P \rightarrow P'$ mit $P\varphi \subseteq P'$ und $L\varphi \subseteq L'$ so, dass für $p \in P$ und $l \in L$ gilt:

Aus $p \in l$ folgt $p\varphi \in l\varphi$.

Falls φ bijektiv und φ^{-1} ebenfalls ein Morphismus, so ist φ ein **Isomorphismus**. Isomorphismen von \mathbb{P} nach \mathbb{P} heißen **Kollineationen** oder **Automorphismen**.

Definition 1.11.

Eine Gerade $l \in L$ heißt **Achse** einer Kollineation φ , wenn $\varphi(p) = p$ für alle $p \in l$.

Ein Punkt $p \in P$ heißt **Zentrum** einer Kollineation φ , wenn alle Geraden durch p auf sich selbst abgebildet werden, das heißt $\varphi(l) = l$ für alle l mit $p \in l$.

Satz 1.12.

Eine Kollineation hat ein Zentrum genau dann, wenn sie eine Achse hat.

Definition 1.13.

Eine Kollineation einer Ebene \mathbb{P} , die ein Zentrum besitzt (und damit auch eine Achse) nennt man auch Zentral-Axial-Kollineation oder kurz **Zentralkollineation**.

Eine Zentralkollineation mit Zentrum $p \in P$ und Achse $l \in L$ heißt:

- **Homologie**, falls $p \notin l$
- **Kernhomologie**, falls $l = l_\infty$ und $p \notin l_\infty$
- **Elation**, falls $p \in l$
- **Translation**, falls $l = l_\infty$ und $p \in l_\infty$

Im Falle der Homologie und der Elation wird \mathbb{P} aufgefasst als projektive Ebene, im Fall der Kernhomologie und der Translation wird aufgrund der ausgezeichneten Geraden \mathbb{P} als affine Ebene aufgefasst.

Definition 1.14.

Eine affine Ebene heißt **Translationsebene**, wenn gilt:

Für je zwei affine Punkte $x, y \in P$ existiert genau eine Translation τ mit $\tau(x) = y$.

Bezeichne im Folgenden Translationsebenen mit \mathbb{T} .

Bemerkung 1.15.

Im Folgenden werden wir ohne Einschränkung *nicht* zwischen projektiven und affinen Translationsebenen unterscheiden, solange dies nicht explizit erforderlich ist.

Satz 1.16.

Die Translationen einer Translationsebene \mathbb{T} bilden eine abelsche Gruppe. Diese operiert scharf transitiv auf den affinen Punkten von \mathbb{T} .

1.3. Grundlagen über Translationsebenen

Im Folgenden seien K ein endlicher Körper, W und V endlich-dimensionale K -Räume.

Definition 1.17.

Sei \mathfrak{S} eine Menge von nichttrivialen Unterräumen von W . Wir nennen \mathfrak{S} eine **Faserung** oder **Spread** auf W , wenn gilt:

1. $|\mathfrak{S}| \geq 2$
2. $W = \bigcup_{X \in \mathfrak{S}} X$
3. $W = X \oplus Y$ mit $X, Y \in \mathfrak{S}$ und $X \neq Y$

Die Elemente von \mathfrak{S} heißen **Fasern**.

Bemerkung 1.18.

Aus der Dimensionsformel [DEM, Kap. 1.19, S. 9] folgt, dass für alle Fasern $X \in \mathfrak{S}$ gilt:

$$\dim(X) = \frac{1}{2} \cdot \dim(W).$$

Definition 1.19.

Seien K wie oben und V ein K -Raum. Sei $0 \in \mathbf{S} \subseteq \text{End}_K(V)$.

1. Eine Menge \mathbf{S} heißt **partielle Spread-Menge**, falls für $t, t' \in \mathbf{S}$ mit $t \neq t'$ der Operator $t - t'$ invertierbar ist.
2. \mathbf{S} heißt **Spread-Menge**, falls zusätzlich $\mathbf{S} \setminus \{0\}$ scharf transitiv auf $V \setminus \{0\}$ operiert.
3. Eine partielle Spread-Menge der Größe m heißt **m -Spread-Menge**.
4. Eine Spread-Menge heißt **normiert**, falls $1 \in \mathbf{S}$.

Der Zusammenhang zwischen Faserungen, Spread-Mengen und Translationsebenen wird durch die Sätze 1.20 und 1.22 deutlich:

Satz 1.20.

Sei W ein K -Raum, \mathfrak{S} eine Faserung von W .

Dann ist $\mathbb{T} = (W, L_{\mathfrak{S}})$ eine Translationsebene, wobei $L_{\mathfrak{S}} := \{w + X \mid w \in W, X \in \mathfrak{S}\}$ die Menge der Geraden ist und die Translationsgruppe operiert durch Addition mit Elementen aus W .

Beweis.

Siehe [WIL, Kap. 1.1] □

Bemerkung 1.21.

Die projektive Erweiterung von $\mathbb{T} = (W, L_{\mathfrak{S}})$ kann wie folgt beschrieben werden:
Sei $\mathfrak{S} = \{X_i \mid i \in I\}$ eine Faserung von W . Definiere die *nicht affinen* Punkte durch Hinzunahme der Symbole (i) mit $i \in I$ und bezeichne

- $l_{\infty} := \{(i) \mid i \in I\}$,
- $P := W \cup \{(i) \mid i \in I\}$,
- $l_{i,w} := \{v + w \mid v \in X_i \in \mathfrak{S}\} \cup \{(i)\}$ für $i \in I$ und $w \in W$,
- $L := \{l_{i,w} \mid i \in I, w \in W\} \cup \{l_{\infty}\}$.

Dann ist $\mathbb{T} = (P, L)$ die projektive Erweiterung.

Satz 1.22.

Sei V ein K -Raum derart, dass $W = V \oplus V$, und $\mathcal{S} \subset GL(V)$ eine Menge von linearen Abbildungen, die scharf transitiv auf $V \setminus \{0\}$ operiert.

Setze

- $V(\infty) := \{(0, v) \mid v \in V\}$
- $V(0) := \{(v, 0) \mid v \in V\}$
- $V(T) := \{(v, vT) \mid v \in V\}$, für $T \in \mathcal{S}$

Dann ist die Menge $\mathfrak{S}(\mathcal{S}) = \{V(\infty)\} \cup \{V(0)\} \cup \{V(T) \mid T \in \mathcal{S}\}$ eine Faserung auf W und die Menge \mathcal{S} ist eine Spread-Menge von \mathbb{T} .

Beweis.

Siehe [WIL, Kap. 1.1] □

Bemerkung 1.23.

Satz 1.22 liefert ein konkretes Verfahren, um aus einer gegebenen Spread-Menge eine Faserung zu konstruieren.

Vice versa ist dies ebenfalls möglich, wie das folgende Lemma und Algorithmus 1 zeigen.

Lemma 1.24.

Seien \mathfrak{S} eine partielle Faserung auf $W = V \oplus V$ und $\dim W = 2n$. Gegeben seien zwei Fasern X und Y mit den Basen $B_X = \{v_1, \dots, v_n\}$, $B_Y = \{w_1, \dots, w_n\}$. Dann gilt:

1. Grundlagen

1. Ist Z eine dritte Faser, so existiert genau eine Matrix $A_Z = (a_{ij}) \in GL(V)$ mit

$$Z = \langle v_i + \sum_{j=1}^n a_{ij} w_j \mid 1 \leq i \leq n \rangle$$

2. Die Basis B_Y kann (in Abhängigkeit von B_X) so gewählt werden, dass für $Z \in \mathfrak{S} \setminus \{X, Y\}$ die Matrix A_Z gleich $\mathbb{1}_{n \times n}$ ist.

Beweis.

Zu 1: Da $X \oplus Y = W$ nach Voraussetzung, existiert zu jedem $v_i \in B_X$ ein eindeutiges $\hat{w}_i \in Y$ mit $v_i + \hat{w}_i \in Z$. Falls $\hat{w}_i = \sum_{j=1}^n a_{ij} w_j$ eine Linearkombination der Basisvektoren aus B_Y ist, so setze $A_Z = (a_{ij})$. Es gilt $A_Z \in GL(V)$, da $X \cap Z = Y \cap Z = 0$.

Zu 2: Sei $B_X = \{v_1, \dots, v_n\}$ fest gewählt, A_Z wie oben. Setze $C := A_Z^{-1} = (c_{ij})$, dann ist die Menge $\{w_1 \cdot C, \dots, w_n \cdot C\}$ eine Basis von Y und die Faser

$$Z = \langle v_i + \sum_{j=1}^n a_{ij} \cdot w_j \cdot c_{jk} \mid 1 \leq i \leq n \rangle = \langle v_i + \sum_{j=1}^n w_j \mid 1 \leq i \leq n \rangle$$

hat die Koeffizientenmatrix $\mathbb{1}$. □

Bemerkung 1.25.

Seien X und Y Fasern eines Spreads \mathfrak{S} . Entsprechend zu Lemma 1.24 seien Basen B_X von X und B_Y von Y gewählt, sodass der Faser $U \in \mathfrak{S} \setminus \{X, Y\}$ die Matrix A_U zugeordnet sei.

Identifiziere V mit K^n , W mit $V \oplus V$, X mit $V(0) := V \oplus 0$, Y mit $V(\infty) := 0 \oplus V$ und für $U \in \mathfrak{S} \setminus \{X, Y\}$ identifiziere

$$U = V(A_U) := \{(v, vA_U) \mid v \in V\}.$$

Dann ist \mathfrak{S} die Faserung, die durch die Spread-Menge $\mathbf{S} := \{A_U \mid U \in \mathfrak{S}\}$ im Sinne von Satz 1.22 definiert ist. Wählt man die Basen insbesondere so, dass $A_Z = \mathbb{1}$ für $Z \in \mathfrak{S} \setminus \{X, Y\}$ gilt, so ist $Z = V(1) := \{(v, v) \mid v \in V\}$.

Lemma 1.26.

Algorithmus 1 liefert eine Spread-Menge.

Beweis.

Die Konstruktionsvorschrift entspricht derjenigen in Lemma 1.24. □

Algorithmus 1 Konstruktion einer Spread-Menge aus einer Faserung auf W

Eingabe: Faserung \mathfrak{S} **Ausgabe:** Spread-Menge \mathbf{S} mit $\mathfrak{S} = \mathfrak{S}(\mathbf{S})$ *Initialisierung:* Setze $\mathbf{S} = \emptyset$ und B_X, B_Y als die Basen von zwei beliebigen Fasern X und $Y \in \mathfrak{S}$ **for** $Z \in \mathfrak{S} \setminus \{X, Y\}$ **do** $M := \emptyset$ **for** j in $[1..Size(B_X)]$ **do** $w := \text{false}$ **while** $k \leq Size(Y)$ und $w = \text{false}$ **do**Setze $z := B_X[j] + Y[k]$ **if** $z \in Z$ **then** $w := \text{true}$ Stelle die Koeffizienten von $Y[k]$ bezüglich B_Y darSetze den so erhaltenen Koeffizientenvektor als die j -te Zeile von M .**end if****end while****end for**Füge M zu \mathbf{S} hinzu**end for**Ausgabe \mathbf{S} **Definition 1.27.**Sei \mathfrak{S} eine Faserung auf $W = V \oplus V$ und X, Y, Z seien drei Fasern aus \mathfrak{S} .Wähle zwei Basen B_X von X und B_Y von Y . Es sei weiterhin

$$\mathbf{S} = \{A_Z \in GL(V) \mid Z \in \mathfrak{S} \setminus \{X, Y\}\}$$

gemäß Satz 1.24. Wir nennen \mathbf{S} eine **Koordinatisierung** von \mathfrak{S} bezüglich des **Referenzduos** (X, Y) .Sind B_X und B_Y insbesondere so gewählt, dass $A_Z = \mathbb{1}$, so nennen wir die normierte Spread-Menge eine Koordinatisierung von \mathfrak{S} bezüglich des **Referenztripels** (X, Y, Z) .Schreibt man $\mathfrak{S} = \{V_i \mid i \in I\}$ und ist $X = V_j, Y = V_k$ und $Z = V_l$, so sprechen wir von einer Koordinatisierung von \mathfrak{S} bezüglich des Referenzduos (j, k) , beziehungsweise bezüglich des Referenztripels (j, k, l) .Für eine Menge $\mathbf{S} \subset GL(V)$ ist in Algorithmus 2 ein einfaches Testverfahren angegeben, um zu entscheiden, ob es sich bei \mathbf{S} um eine Spread-Menge handelt oder nicht.**Definition 1.28.**Seien $W = V \oplus V$ und $\mathbf{S} \subset GL(V)$ eine Spread-Menge von Matrizen. Die Menge

$$G(\mathbf{S}) = \{(\mathbb{1}, T) \mid T \in \mathbf{S}\} \cup \{(\emptyset, \mathbb{1})\} \subseteq K^{\dim(V) \times \dim(W)}$$

1. Grundlagen

Algorithmus 2 Spread-Mengen-Test

Eingabe: Menge $\mathbf{S} \subset GL(V)$

Ausgabe: „true“, falls \mathbf{S} eine (partielle) Spread-Menge, „false“ falls nicht.

Initialisierung: $w := \text{true}$

```
while  $i \leq \text{Size}(\mathbf{S}) - 1$  do  
   $j := i + 1$   
  while  $j \leq \text{Size}(\mathbf{S})$  und  $w = \text{true}$  do  
     $w := \det(\mathbf{S}[i] - \mathbf{S}[j]) \neq 0$   
  end while  
end while  
Ausgabe  $w$ 
```

nennen wir die **Groß-Spread-Menge** zu \mathbf{S} .

Algorithmus 3 Koordinatisierung, kurz *KOORD*

Eingabe: Normierte Spread-Menge $\mathbf{S} = \{t_0 = 0, t_1 = 1, \dots, t_n\}$ bezüglich $(\infty, 0, 1)$, sowie Koordinaten (a, b, c)

Ausgabe: Normierte Spread-Menge \mathbf{S}' bezüglich (a, b, c) , Transformationsmatrix T mit $G(\mathbf{S}') = G(\mathbf{S}) \cdot T$

if $a = \infty$ **then**

$$T = \begin{pmatrix} t_c - t_b & -t_b \\ 0 & 1 \end{pmatrix}$$

end if

if $b = \infty$ **then**

$$T = \begin{pmatrix} -t_a & t_c - t_a \\ 1 & 0 \end{pmatrix}$$

end if

if $c = \infty$ **then**

$$T = \begin{pmatrix} -t_a & -t_b \\ 1 & 1 \end{pmatrix}$$

end if

if $a, b, c \neq \infty$ **then**

$$T = \begin{pmatrix} -t_a \cdot (t_c - t_a)^{-1} & -t_b \cdot (t_c - t_b)^{-1} \\ (t_c - t_a)^{-1} & (t_c - t_b)^{-1} \end{pmatrix}, \text{ vergleiche mit [TRA, Kap. 2.2, S. 106].}$$

end if

Bemerkung 1.29.

Aus Satz 1.24 und Definition 1.27 geht hervor, dass \mathfrak{S} noch *nicht* eindeutig durch eine Koordinatisierung bezüglich (X, Y, Z) bestimmt ist, da die Wahl von B_X immer noch frei bleibt.

Satz 1.30.

Seien \mathfrak{S} eine Faserung auf W und \mathbf{S} eine normierte Spread-Menge bezüglich des Referenztripels $(\infty, 0, 1)$. Sei \mathbf{S}' diese Spread-Menge bezüglich (x, y, z) , dann lässt sich \mathbf{S} zu \mathbf{S}' umkoordinatisieren durch eine endliche Anzahl folgender Operationen:

1. $op_0(g) : \mathbf{S} \rightarrow g^{-1}\mathbf{S}g$, mit $g \in GL(V)$, entspricht einem Basiswechsel.
2. $op_1(T) : \mathbf{S} \rightarrow T^{-1}\mathbf{S}$, $T \in \mathbf{S}$ und $(\infty, 0, 1) \mapsto (\infty, 0, T)$.
3. $op_2 : \mathbf{S} \rightarrow \mathbf{S}^{-1} = \{0\} \cup \{T^{-1} \mid T \in \mathbf{S}\}$ und $(\infty, 0, 1) \mapsto (0, \infty, 1)$.
4. $op_3 : \mathbf{S} \rightarrow \mathbb{1} - \mathbf{S} = \{\mathbb{1} - T \mid T \in \mathbf{S}\}$ und $(\infty, 0, 1) \mapsto (\infty, 1, 0)$.

Beweis.

Siehe [DEM, Satz 10.8, S. 97]. □

Definition 1.31.

Wir nennen zwei normierte Spread-Mengen \mathbf{S} , \mathbf{S}' genau dann **äquivalent**, wenn \mathbf{S}' aus der Anwendung endlich vieler Operationen des Typs op_0, \dots, op_3 auf \mathbf{S} hervorgeht.

Algorithmus 4 Konjugiertheit zweier normierter Spread-Mengen, kurz *ISO*

Eingabe: Zwei normierte Spread-Mengen \mathbf{S} , \mathbf{S}'

Ausgabe: Matrix T mit $T^{-1}\mathbf{S}T = \mathbf{S}'$ oder die Nullmatrix

Initialisierung: Setze $T := 0$, $J := \emptyset$

Berechne von jeder Matrix in \mathbf{S} und \mathbf{S}' die Koeffizienten Δ des charakteristischen Polynoms sowie des Minimalpolynoms

Finde $t_s := \min_{t \in B(\mathbf{S})} \{|C_{GL(V)}(t)|\}$

for j in $[1..Size(\mathbf{S}')] \mathbf{do}$

Teste, ob $\Delta(t_s) = \Delta(\mathbf{S}'[j])$ und falls zutreffend, speichere j in J

end for

$w := \text{false}$

while $k \leq Size(J)$ und $w = \text{false}$ **do**

Finde $x \in GL(V)$ mit $x^{-1}t_s x = \mathbf{S}'[J[k]]$. Falls ein solches x existiert setze

$l := 1$

while $l \leq Size(C_{GL(V)}(t_s))$ und $w = \text{false}$ **do**

$y := C_{GL(V)}(t_s)[l] \cdot x$

$w := y^{-1}\mathbf{S}y \subseteq \mathbf{S}'$

if $w = \text{true}$ **then**

$T := y$

end if

end while

end while

Ausgabe T

1. Grundlagen

Bemerkung 1.32.

In Algorithmus 4 benutzen wir den aus Lemma 1.1 bekannten Zusammenhang zwischen ähnlichen Matrizen und ihren Minimalpolynomen.

Algorithmus 5 Äquivalenz normierter Spread-Mengen, kurz *EQUIV*

Eingabe: Zwei normierte Spread-Mengen \mathbf{S}, \mathbf{S}'

Ausgabe: „true“ falls $\mathbf{S} \sim \mathbf{S}'$, im Sinne der Definition 1.31, „false“ falls nicht.

Initialisierung: $T := 0$, $w := \text{false}$, $I := \{(\infty), (0), (1), \dots, (\text{Size}(\mathbf{S}))\}$, $a := (\infty)$

while $a \in I$ und $w = \text{false}$ **do**

$I_a := I \setminus \{a\}$. Wähle $b \in I_a$ zufällig

while $b \in I_a$ und $w = \text{false}$ **do**

$I_{a,b} := I \setminus \{a, b\}$. Wähle $c \in I_{a,b}$ zufällig

while $c \in I_{a,b}$ und $w = \text{false}$ **do**

Setze $\mathbf{S}_k := \text{KOORD}(\mathbf{S}, a, b, c)$. Berechne die Koeffizienten δ der charakteristischen Polynome und der Minimalpolynome der Matrizen von \mathbf{S}_k und \mathbf{S}' .

if $\delta(\mathbf{S}_k) = \delta(\mathbf{S}')$ **then**

$$T := \text{ISO}(\mathbf{S}_k, \mathbf{S}'), w := \begin{cases} \text{true}, & \text{falls } \det(T) \neq 0 \\ \text{false}, & \text{falls } T = 0 \end{cases}$$

end if

end while

end while

end while

Ausgabe w

Bemerkung 1.33.

- Offenbar sind alle Äquivalenzabbildungen der Spread-Mengen aus Algorithmus 5 Produkte der Operationen op_0, \dots, op_3 aus Satz 1.30. Des Weiteren werden alle möglichen Koordinatisierungen durchlaufen, also alle Äquivalenzen gefunden.
- Es ist bekannt [MAD, Kap. 3, Prop 1], dass zwei Translationsebenen $\mathbb{T}(\mathbf{S}_1), \mathbb{T}(\mathbf{S}_2)$, die durch zwei äquivalente Spread-Mengen $\mathbf{S}_1, \mathbf{S}_2$ induziert werden, isomorph sind.

Satz 1.34.

Sei \mathbb{T} eine Translationsebene mit Translationsgruppe T über dem K -Raum W mit $W = V \oplus V$. Dann gilt

$$\text{Aut}(\mathbb{T}) = T \cdot \mathbf{G}$$

mit einem Translationskomplement \mathbf{G} .

Es gilt außerdem für $W = W_{GF(p)}$:

$$\mathbf{G} = G_0 = \{x \in GL(W) \mid Yx \in \mathfrak{E}, \text{ für alle } Y \in \mathfrak{E}\}.$$

Beweis.

Sei $\mathbf{A} = \text{Aut}(\mathbb{T})$. Die Gruppe \mathbf{A} operiert treu auf W und ist transitiv, da schon die Translationsgruppe transitiv ist.

Also gilt: $\mathbf{A} = T \cdot \mathbf{G}$, wobei $\mathbf{G} = G_0$ gleich dem Stabilisator des Nullvektors in W ist.

Sei $v \in W$ und $\sigma \in \mathbf{A}$, so gilt: $0\sigma\tau_{-0\sigma} = 0$. Also liegt $\sigma\tau_{-0\sigma}$ in $\mathbf{G} = G_0$ und $\sigma = (\sigma\tau_{-0\sigma})\tau_{0\sigma} \in \mathbf{G} \cdot T$.

Daraus folgt $\mathbf{A} = \mathbf{G} \cdot T = T \cdot \mathbf{G}$ und $\mathbf{G} \cap T = 1$, denn nur die Translation $\tau_0 = 1$ lässt den Nullvektor fix.

Für $\tau \in T$, mit $\tau : W \rightarrow W$ gilt: $\tau_{v+v'} = \tau_v \cdot \tau_{v'}$ mit $v, v' \in W$.

Sei $\omega \in \mathbf{G}$. Es ist $0\omega^{-1}\tau_v\omega = 0\tau_v\omega = v\omega = 0\tau_{v\omega}$. Wir wissen bereits, dass $\omega^{-1}\tau_v\omega, \tau_{v\omega} \in T$ und können damit folgern $\omega^{-1}\tau_v\omega = \tau_{v\omega}$.

Damit ist $\tau_{(v+w)\omega} = \tau_{v\omega} \cdot \tau_{w'\omega} = \tau_{v\omega+v'\omega}$ und mit Satz 1.22 folgt, dass $\omega \in GL(W)$, wobei W als $GF(p)$ -Raum aufgefasst wird.

Identifiziere daher ω mit einer linearen Abbildung und G_0 als die Menge der linearen Abbildungen, die die Fasern von \mathfrak{S} fix lassen. Die Fasern von \mathfrak{S} werden also nach Satz 1.16 mit den Punkten auf l_∞ identifiziert, da $G_0 = G_{0,l_\infty}$. \square

Bemerkung 1.35.

Sei x eine Kollineation und bezüglich einer konkreten Koordinatisierung sei $x \in GL(W)$ durch die Matrix

$$x = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$$

dargestellt, wobei $A_1, \dots, A_4 \in GL(V)$.

- Ist $V(0)$ fix unter x , so ist $A_2 = 0$, denn

$$V(0) \cdot x \ni (v, 0) \cdot \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} = (vA_1, vA_2) \overset{!}{\in} V(0) \implies A_2 = 0$$

- Ist $V(\infty)$ fix unter x , so ist $A_3 = 0$, denn

$$V(\infty) \cdot x \ni (0, v) \cdot \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix} = (vA_3, vA_4) \overset{!}{\in} V(\infty) \implies A_3 = 0$$

- Sind $V(0).V(\infty)$ Fixfasern von x , so gilt für eine beliebige Faser $V(T)$

$$V(T) \cdot x \ni (v, vT) \cdot \begin{pmatrix} A_1 & \\ & A_4 \end{pmatrix} = (vA_1, vA_4) = (w, A_1^{-1}TA_4) \in V(A_1^{-1}TA_4)$$

- Ist zusätzlich zu $V(0)$ und $V(\infty)$ auch $V(1)$ fix unter x , so ist $A_4 = A_1$, denn

$$V(1) \cdot x \ni (v, v) \cdot \begin{pmatrix} A_1 & \\ & A_4 \end{pmatrix} = (vA_1, vA_4) \overset{!}{\in} V(1) \implies A_1 = A_4$$

1. Grundlagen

Wir wollen nun die Automorphismengruppe einer Translationsebene bezüglich einer gegebenen Spread-Menge konkret berechnen. Dazu benötigen wir die Erzeuger des Translationskomplementes \mathbf{G} , die wir aus der iterativen Berechnung der Stabilisatoren der Fasern erhalten. Siehe Algorithmus 6 und 7.

Algorithmus 6 Stabilisatoren der Fasern, kurz *STAB*

Eingabe: Normierte Spread-Menge $\mathbf{S} = \{t_0 = \mathbb{0}, t_1 = \mathbb{1}, t_2, \dots, t_m\}$, ein Erzeugendensystem gen_0 des Stabilisators der Fasern $V(\infty), V(t_0), \dots, V(t_k)$ mit $1 < k \leq m$.

Ausgabe: Ein Erzeugendensystem gen des Stabilisators von $V(\infty), V(t_0), \dots, V(t_{k-1})$
Initialisierung: $R := \{t_k, \dots, t_m\}$, $C := C_{GL(V)}(\{t_1, \dots, t_{k-1}\})$, $C_0 := C_{GL(V)}(t_k)$,
 $gen := gen_0$, $H := \langle gen \rangle$, $J := \{t_k\}$, $I := R \setminus J$.

while $\text{Size}(I) > 0$ **do**

1) Sei $B \subseteq I$ eine beliebige H -Bahn. Teste, ob ein $g \in C$ existiert mit $g^{-1}t_k g \in B$
if Kein solches g existiert **then**

2) Setze $J := J \cup B$ und $I := I \setminus B$.

else if Es existiert ein solches g **then**

Teste, ob ein $h \in C_0$ existiert mit $(hg)^{-1}\mathbf{S}(hg) = \mathbf{S}$.

if Kein solches h existiert **then**

Gehe zu Schritt 2).

else if Ein solches h existiert **then**

3) Setze $gen := gen \cup \{hg\}$ und $H := \langle gen \rangle$. Seien B_1, \dots, B_l die H -Bahnen auf R . Setze $J := \bigcup_{B_i \cap J \neq \emptyset} B_i$, $I := \bigcup_{B_j \cap I = \emptyset} B_j$ und gehe zu Schritt 1).

end if

end if

end while

Ausgabe gen

Lemma 1.36.

Algorithmus 6 berechnet den Stabilisator von $V(\infty), V(t_0), \dots, V(t_{k-1})$

Beweis.

Zunächst ist zu bemerken, dass der Algorithmus überhaupt terminiert, da in Schritt 2) und 3) die Menge I jeweils echt verkleinert wird.

Sei H_1 der Stabilisator von $V(\infty), V(t_0), \dots, V(t_{k-1})$, und H_0 bezeichne den Stabilisator von $V(\infty), V(t_0), \dots, V(t_k)$. Wir werden nun zeigen, dass die Gruppe H , die zu Beginn des Algorithmus gleich H_0 ist, am Ende des Algorithmus gleich H_1 ist, also dass

$$(J \setminus t_k^H) \cap t_k^{H_1} = \emptyset$$

wobei die Notation t_k^H die Bahn von t_k unter H bezeichnet.
 Induktion nach $|J|$:

Zu Beginn ist $J = \{t_k\}$ also $(J \setminus t_k^H) \cap t_k^{H_1} = \emptyset \cap t_k^{H_1} = \emptyset$

Sei also $|J| > 1$ und es gelte die Behauptung für den Vorgänger von J , J_{Alt} . Wir untersuchen die Elemente, die durch die Iteration zu J_{Alt} hinzukommen.

Angenommen, J_{Alt} wird in Schritt 2) vergrößert, d.h. $J = J_{Alt} \cup B$. Wir wissen, es existiert ein $s \in B$ mit $s \notin t_k^{H_1}$, also $s^{H_1} \cap t_k^{H_1} = \emptyset$. Dann ist aber wegen $B = s^H \subseteq s^{H_1}$ auch $B \cap t_k^{H_1} = \emptyset$. Die Behauptung gilt also für J .

Angenommen, J_{Alt} wird in Schritt 3) vergrößert. Hier wird ebenfalls das aktuelle H_{Alt} auf $H \leq H_1$ vergrößert. Das heißt wir haben $(J_{Alt} \setminus t_k^{H_{Alt}}) \cap t_k^{H_1} = \emptyset$ nach Induktionsvoraussetzung. Dann muss gelten $J_{Alt} \setminus t_k^{H_{Alt}} = J_{Alt} \setminus t_k^H$ und damit auch $(J_{Alt} \setminus t_k^H) \cap t_k^{H_1} = \emptyset$. Sei B eine Bahn von H mit $B \cap (J_{Alt} \setminus t_k^{H_{Alt}}) \neq \emptyset$, so gilt auch $B^{H_1} \cap (J_{Alt} \setminus t_k^{H_{Alt}}) \neq \emptyset$. Klar ist, dass B^{H_1} eine H_1 -Bahn ist und Elemente enthält, die nicht in $t_k^{H_1}$ liegen. Daraus folgt:

$$B^{H_1} \cap t_k^{H_1} = \emptyset$$

Insbesondere gilt dann auch $(J \setminus t_k^H) \cap t_k^{H_1} = \emptyset$ und es folgt die Behauptung.

Sei nun $g \in H_1$. Es bleibt zu zeigen, dass $g \in H$ für ein H der Iteration.

Falls $g^{-1}t_k g = t_k$, so sind wir fertig, da $g \in H_0 \leq H$.

Sei also $g^{-1}t_k g = t \neq t_k$. Wir betrachten den Schritt der Iteration, bei dem noch $t \in I$ gilt aber $t \in J$ im nächsten Schritt. Gilt nach der Iteration $t \in t_k^H \cap J$, so existiert ein $h \in H$ mit $h^{-1}th = t_k$, das heißt $gh \in H_0 \leq H$ und es folgt $g \in H_0 h^{-1} \subseteq H$ wie gewünscht.

Falls jedoch $t \in J \setminus t_k^H$, so folgt nach der Behauptung $t \notin t_k^{H_1}$, ein Widerspruch. \square

Definition 1.37.

Eine normierte Spread-Menge \mathbf{S} heißt **desarguesch**, falls die von ihr erzeugte Gruppe kommutativ ist. Eine durch diese Spread-Menge induzierte Translationsebene $\mathbb{T}(\mathbf{S})$ heißt ebenfalls **desarguesch**. Vergleiche mit [KLE, Kap. 9, Kor 21, S. 138].

Satz 1.38.

Sei \mathbb{T} eine Translationsebene der Ordnung q^n und es existiere eine zyklische Gruppe von Homologien der Ordnung $q^n - 1$, dann ist \mathbb{T} desarguesch.

Beweis.

Ist Z eine Gruppe von Kernhomologien, so ist $K(l_\infty) \cong GF(q^n)$ und die Ebene damit desarguesch, siehe [DEM, Kap. 7, Bem. 7.17, S. 68].

Sei also Z keine Gruppe von Kernhomologien. Da l_∞ eine Fixgerade ist, liegt das Zentrum von Z auf l_∞ und die Achse ist eine affine Gerade. Wir nehmen nun an, dass die Ebene durch eine Faserung auf dem Vektorraum $W = V \oplus V$, $V = V(n, q)$, definiert ist und dass $(0, 0)$ auf der Achse liegt, das heißt Z eine Untergruppe des üblichen Translationskomplementes ist. Wenn wir die Ebene koordinatisieren, können wir also (∞) als

Algorithmus 7 Automorphismengruppe, kurz *AUT*

Eingabe: Spread-Menge \mathbf{S}

Ausgabe: Struktur und Ordnung des Translationskomplementes \mathbf{G}

Initialisierung: $H := \emptyset$.

1) Berechne den Kern der Spread-Menge \mathbf{S} , also dem Zentralisator $C := C_{GL(V)}(\langle \mathbf{S} \rangle)$. Setze H als Menge der Erzeuger von C .

2) Bestimme den Stabilisator H_1 von $(\infty, 0, 1)$, dazu berechne alle $x \in GL(V)$ mit $x^{-1}\mathbf{S}x = \mathbf{S}$ und setze $H_1 := \langle x \mid x^{-1}\mathbf{S}x = \mathbf{S} \rangle$ (entspricht der Prozedur *STAB*).

Füge die Erzeuger von H_1 zu H hinzu.

3) Bestimme den Stabilisator H_2 von $(\infty, 0)$, dazu koordinatisiere \mathbf{S} bezüglich $(\infty, 0, i)$ mit $2 \leq i \leq 31$ und berechne via *STAB* alle Matrizen x_i mit $x_i^{-1}\mathbf{S}x_i = \mathbf{S}_i$. Setze $y_i = T \cdot \text{diag}(x_i, x_i)$, wobei T die Transformationsmatrix aus der Prozedur *KOORD* und $H_2 := \langle y_2, \dots, y_{31} \rangle$

Füge die Erzeuger von H_2 zu H hinzu.

4) Bestimme den Stabilisator H_3 von (∞) , dazu koordinatisiere \mathbf{S} bezüglich (∞, i, j) mit $1 \leq i \leq 31$, $j \in \{\infty, 0, 1, \dots, 31\} \setminus \{i\}$ und berechne via *STAB* alle x_{ij} mit $x_{ij}^{-1}\mathbf{S}x_{ij} = \mathbf{S}_{ij}$. Setze $y_{ij} = T \cdot \text{diag}(x_{ij}, x_{ij})$ mit T der Transformationsmatrix aus *KOORD* und $H_3 := \langle y_{ij} \mid i, j \text{ wie oben} \rangle$.

Füge die Erzeuger von H_3 zu H hinzu.

5) Koordinatisiere \mathbf{S} bezüglich (i, j, k) mit $0 \leq i \leq 31$, $j \in \{\infty, 0, 1, \dots, 31\} \setminus \{i\}$ und $k \in \{\infty, 0, 1, \dots, 31\} \setminus \{i, j\}$. Berechne via *STAB* ein x_{ijk} mit $x_{ijk}^{-1}\mathbf{S}x_{ijk} = \mathbf{S}_{ijk}$. Setze $y_{ijk} = T \cdot \text{diag}(x_{ijk}, x_{ijk})$ mit T der Transformationsmatrix aus *KOORD* und $H_4 := \langle y_{ijk} \mid i, j, k \text{ wie oben} \rangle$.

Füge die Erzeuger von H_4 zu H hinzu.

Setze $\mathbf{G} := \langle H \rangle$.

Ausgabe \mathbf{G} und H

Zentrum und $V(0)$ als Achse wählen. Ein Element $z \in Z$ lässt ferner die Gerade $V(\infty)$ fest. Damit operiert ein solches Element via

$$(x, y)z = (x, yD(z))$$

wobei $D : Z \rightarrow GL(V)$ ein Isomorphismus ist. Sei nun $V(T) \neq V(0), V(\infty)$ eine Faser. Dann gilt $V(T)z = V(TD(z))$, mit anderen Worten $\mathbf{S} = TD(Z) \cup 0$ ist eine Spread-Menge zu dieser Koordinatisierung. Damit ist $T^{-1}\mathbf{S} = D(Z) \cup 0$ eine normierte Spread-Menge für diese Ebene. Wir wissen, dass $D(Z)$ eine Singergruppe ist und somit ist $D(Z) \cup 0$ ein Körper der Ordnung q^n , die Ebene ist also desarguesch nach unserer Definition. \square

Definition 1.39.

- Eine nicht-leere Menge L zusammen mit einer Verknüpfung \circ und einem ausgezeichneten neutralen Element e heißt **Loop**, falls:
 1. $a \circ e = e \circ a = a$ für alle $a \in L$
 2. Für $a, b \in L$ existieren genau ein $x \in L$ mit $a \circ x = b$ und genau ein $y \in L$ mit $y \circ a = b$, also ein links- und ein rechtsinverses Element.
- Eine Menge $\{0, 1\} \subseteq Q$ zusammen mit zwei Verknüpfungen $+: Q \times Q \rightarrow Q$ und $\cdot: Q \times Q \rightarrow Q$ heißt ein **Quasikörper**, falls gilt:
 1. Das Paar $(Q, +)$ ist eine abelsche Gruppe mit neutralem Element 0.
 2. Das Paar $(Q \setminus \{0\}, \cdot)$ ist ein Loop mit neutralem Element 1.
 3. Es gilt das Distributivgesetz $(a + b) \cdot c = a \cdot c + b \cdot c$ für alle $a, b, c \in Q$.
 4. $a \cdot 0 = 0 \cdot a = 0$ für alle $a \in Q$
- Ein Quasikörper H ist ein **Halbkörper**, falls beide Distributivgesetze gelten.

Definition 1.40.

- Sei Q ein Quasikörper, so ist der **Kern** von Q definiert als

$$K(Q) := \{x \in Q \mid x(ab) = (xa)b, x(a + b) = xa + xb, a, b \in Q\}.$$

- Seien \mathbb{T} eine Translationsebene, $E = E(l_\infty)$ die Menge aller Elationen mit Achse l_∞ und $E(p)$ die Menge aller Elationen mit Zentrum p . Definiere den **Kern** von \mathbb{T} bezüglich l_∞ als die Menge

$$K(l_\infty) := \{\alpha \in \text{End}(E) \mid E(p)\alpha \subset E(p), \text{ für alle } p \in l_\infty\}$$

1. Grundlagen

In [DEM, Kap. 7, S.63-68] wird der Zusammenhang zwischen dem Kern eines Quasikörpers und dem Kern einer Translationsebene deutlich. Es wird gezeigt, dass eine Ebene genau dann eine Translationsebene ist, wenn sie durch einen Quasikörper koordinatisiert werden kann.

Definition 1.41.

Eine Translationsebene, die bei geeigneter Koordinatenwahl durch einen Halbkörper koordinatisiert werden kann, nennt man **Halbkörper-Ebene**.

Satz 1.42.

Für eine Halbkörper-Ebene gelten die äquivalenten Bedingungen:

- a) Die Spread-Menge \mathbf{S} bildet eine additive Gruppe.*
- b) Die Gruppe der Elationen mit Zentrum (∞) und Achse $V(\infty)$ operiert transitiv auf $l_\infty \setminus \{(\infty)\}$.*

Beweis.

Siehe [DEM, Kap. 7, Prop. 7.24, S. 72]. □

Bemerkung 1.43.

Aus dem vorangegangenen Satz folgt, dass der Vektorraum, der von einer Spread-Menge \mathbf{S} aus $n \times n$ -Matrizen erzeugt wird genau dann die Dimension n hat, wenn es sich bei $\mathbb{T}(\mathbf{S})$ um eine Halbkörper-Ebene handelt.

1.4. Die verwendete Software

Zum Programm:

GAP - Groups, Algorithms, Programming - ist ein freeware Computeralgebrasystem mit dem Berechnungen aus dem Gebiet der diskreten algorithmischen Gruppentheorie ausgeführt werden können. Die dazu nötige Software sowie Befehlsbeispiele in der Programmiersprache sind auf der Homepage www.gap-system.org zu finden. Die Programmiersprache selbst ist im intuitiven Stil gehalten und es existieren vorgefertigte Prozeduren, zum Beispiel zum Bilden einer Gruppe aus der Eingabe der Erzeuger. Des Weiteren kann man eigene Prozeduren definieren. Es stellte sich heraus, dass in unserem Fall GAP mit Permutationen schneller rechnen konnte als mit Matrizen, weshalb auf algorithmischer Ebene oftmals die Umwandlung einer Matrix zu einer Permutation und zurück stattfindet.

2. Die Translationsebenen der Ordnung 32

2.1. Hauptergebnis und elementare Beweise

Ziel dieses Kapitels ist es, das folgende Hauptergebnis dieser Arbeit zu zeigen:

Satz 2.1.

Sei \mathbb{T} eine Translationsebene der Ordnung 32 über $W = V(10, 2)$. Dann gilt eine der beiden Aussagen:

1. Entweder handelt es sich bei der Ebene um die desarguesche Ebene, eine Halbkörper-Ebene, die eindeutig bestimmte Fahnen-transitive Ebene oder eine der zwei nicht-isomorphen Ebenen, die einen Automorphismus der Ordnung 31 besitzen.
2. Das Translationskomplement ist isomorph zu der trivialen Gruppe, C_2 oder C_3 .

Wir werden nun zeigen, dass Kollineationen von Primzahlordnung nur die Ordnungen 31, 11, 7, 5, 3 oder 2 haben können, und alle Ordnungen der daraus resultierenden Translationskomplemente, bis auf die Fälle zwei und drei, untersuchen.

Die Ordnung von $GL(10, 2)$ ist

$$|GL(10, 2)| = 2^{45} \cdot 3^6 \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 17 \cdot 31^2 \cdot 73 \cdot 127.$$

Satz 2.2.

Gegeben sei eine Translationsebene der Ordnung 32. Ein Element von Primzahlordnung in einem Translationskomplement hat eine der Ordnungen aus $\{2, 3, 5, 7, 11, 31\}$.

Beweis.

Sei x eine Kollineation von Primzahlordnung. Jede Bahn auf \mathfrak{E} hat also die Länge 1 oder $|x|$.

Falls $|x| \nmid 33$, so existiert eine Faser $Y \in \mathfrak{E}$ mit $Yx = Y$. Damit induziert x auf Y und W/Y eine lineare Transformation.

Angenommen $x_Y = \mathbb{1}_Y$ und $x_{W/Y} = \mathbb{1}_{W/Y}$. Dann hat x die Ordnung 2, denn: $vx = v$, falls $v \in Y$ und $vx \in v + Y$, falls $v \in W \setminus Y$, also $vx = v + y$ für ein $y \in Y$. Daher gilt: $vx^2 = (v + y)x = vx + \underbrace{yx}_{=y} = v + y + y = v$ und damit $x^2 = \mathbb{1}$.

Seien also $x_Y \neq \mathbb{1}_Y$ oder $x_{W/Y} \neq \mathbb{1}_{W/Y}$ und $x_M \neq \mathbb{1}_Y$ für $M \in \{W, W/Y\}$, das heißt $|x_M| \neq 1$ und daher $|x_M| = |x|$, da x Primzahlordnung besitzt. Es folgt, dass $|x|$ ein Teiler ist von $|GL(5, 2)| = |GL(Y)| = |GL(W/Y)|$, also $|x| \in \{2, 3, 5, 7, 31\}$.

Sei nun $Yx \neq Y$ für alle $Y \in \mathfrak{E}$. Aus $|x| \mid |\mathfrak{E}| = 33$ folgt $|x| \in \{3, 11\}$. □

Satz 2.3.

Es sei G eine Gruppe der Ordnung $|G| = 2^a \cdot 3^b$ mit $a, b \in \mathbb{N}$, wobei $b > 1$ und $|G| > 3$. Dann enthält G eine Untergruppe, die zu einer der folgenden Gruppen isomorph ist:

$$\text{Alt}(4), C_9, C_3 \times C_3, C_6, \text{Sym}(3).$$

Beweis.

Sei $S \in \text{Syl}_3(G)$. Angenommen $|S| > 3$, so enthält S nach dem Satz von Cauchy [Hup, Kap. I, Satz 7.4, S. 34] Untergruppen der Ordnung 9. Nach [HUP, Kap. I, Satz 6.10, S. 31] sind Gruppen der Ordnung p^2 abelsch für p prim. Wir wissen aus dem Fundamentalsatz über abelsche Gruppen [HUP, Kap. I, Satz 13.12, S. 80], dass alle Gruppen der Ordnung 9 isomorph sind zu C_9 oder $C_3 \times C_3$.

Sei von nun an $|S| = 3$. Nach dem Satz von Burnside [HUP, Kap. V, Satz 7.3, S. 492] ist G auflösbar und ein minimaler Normalteiler N von G ist elementar-abelsch.

Sei zuerst $N = S$ und t ein Element der Ordnung 2 in G (existiert, da nach Voraussetzung und Annahme $|G|$ gerade ist). Falls $t^{-1}St = S$, so ist $\langle S, t \rangle \cong C_6$, falls $t^{-1}St = S^{-1}$, so ist $\langle S, t \rangle \cong \text{Sym}(3)$. Wir wissen aus der Gruppentheorie, dass dies die einzigen nicht-isomorphen Gruppen der Ordnung 6 sind.

Sei schließlich N ein 2-Normalteiler von G . Induktion nach $|G|$ zusammen mit unseren Voraussetzungen führt zu $G = NS$. Falls $C_N(S) \neq 1$, so $C_6 \leq G$. Also operiere S fixpunktfrei via Konjugation auf $N \setminus 1$ und sei $B := t^S$ mit $1 \neq t \in N$. Dann ist $|B| = 3$ und daher $|N| \leq |\langle B \rangle| \leq 8 = 2^3$. Wiederum aus der fixpunktfreien Operation von S auf $N \setminus 1$ und da die Bahnen von S die Länge 3 haben folgt aus $|N| \in \{1, 4, 7, 10, \dots\} \leq 8$, dass $|N| = 4$. Also ist $|G| = 12$ und $G \cong \text{Alt}(4)$, da G nach unserer Konstruktion keine Untergruppe der Ordnung 6 enthält. \square

Bemerkung 2.4.

In diesem Kapitel werden alle Translationsebenen der Ordnung 32 bestimmt, die eine Kollineationsgruppe besitzen, die isomorph ist zu einer der folgenden Gruppen:

1. $G \cong C_p$, mit p Primzahl ≥ 5
2. $G \cong C_3 \times C_3, C_9$
3. $G \cong C_6, \text{Sym}(3)$
4. $G \cong C_2 \times C_2, C_4$

Angenommen G sei eine Kollineationsgruppe, die keine Untergruppe aus 1-4 enthält. Nach Satz 2.2 ist G eine $\{2, 3\}$ -Gruppe. Aus Satz 2.3 folgt dann $|G| \leq 3$ und damit Satz 2.1.

Satz 2.5.

Eine Translationsebene der Ordnung 32 besitzt keine Kollineationsgruppe der Ordnung 9.

2. Die Translationsebenen der Ordnung 32

Beweis.

Angenommen E sei eine Kollineationsgruppe der Ordnung 9 auf $\mathbb{T} := \mathbb{T}(W, \mathfrak{S})$.

Angenommen $E \cong C_3 \times C_3$.

Sei $1 \neq e \in E$. Dann ist e entweder planar und $\mathbb{T}_e := \mathbb{T} |_e$ hat die Ordnung 2 oder e operiert fixpunktfrei auf L_∞ , d.h. $C_W(e) = 0$.

Falls e einen Fixpunkt auf L_∞ hat, dann offenbar sogar drei und $C_X(e) \neq 0$ für jede Fixfaser $X \in \mathfrak{S}$. Also ist \mathbb{T}_e eine Unterebene. Ist des Weiteren X eine Fixfaser, so gilt $0 \neq C_X(e) \neq X$. Sei $m := \dim(C_X(e))$, dann ist die Ordnung von \mathbb{T}_e gleich 2^m . Wegen $\dim(C_X(e)) \in \{1, 3\}$ und nach dem Satz von Baer [DEM, Kap. 4, S. 32ff] folgt $2^m \leq 2^2$ und damit $m = 1$. Es folgt die erste Aussage.

Falls e keinen Fixpunkt auf L_∞ hat, so gilt $X \neq Xe$ für alle $X \in \mathfrak{S}$ und somit $C_W(e) = 0$. Ferner gilt als Konsequenz aus [HUP, Kap. V, Hilfssatz 8.12, S. 502]:

$$W = \sum_{1 \neq e \in E} C_W(e).$$

Damit ist $E = \langle e_1, e_2 \rangle$ mit e_1, e_2 planar. Nach dem Satz von Maschke [HUP, Kap. I, Satz 17.6, S. 122] ist

$$X = [X, E] \oplus C_X(E) \text{ und } W = \bigoplus_{i=1}^n W_i$$

mit irreduziblen E -Moduln W_i . Sei weiterhin $U := C_W(e_1)$. Wäre $U = C_W(e_2)$, so existiert eine Fixfaser X , die invariant ist unter E , sodass für den Kommutator von E und X gilt: $[X, E] = \sum_{1 \neq e \in E} C_{[X, E]}(e)$. Also existiert ein $1 \neq e \in E$ mit $\dim(C_X(e)) > 1$,

was unmöglich ist, wie wir gezeigt haben. Daher operiert $\langle e_2 \rangle \cong E/\langle e_1 \rangle$ treu auf U .

Sei $D_i : E \rightarrow GL(W_i)$ die Darstellung von E auf W_i , dann ist $E/\ker(D_i)$ zyklisch, da E abelsch (Konsequenz aus dem Satz von Burnside, vgl. [HUP, Kap V.7, S. 490ff]). Es folgt $E/\ker(D_i) \cong C_3$, das heißt $n = 5$, $\dim(W_i) = 2$ und da $SL(2, 2) \cong Sym(3)$ nach [HUP, Kap II, Satz 6.14, S. 183] ist

$$e_i |_{W_j} \cong A^k, \quad k \in \{0, 1, 2\}, \quad A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Also existieren mindestens zwei j, j' mit

$$e_1 |_{W_j} = (e_2 |_{W_j})^\epsilon, \quad e_1 |_{W_{j'}} = (e_2 |_{W_{j'}})^\epsilon, \quad \epsilon = \pm 1.$$

Dann ist $C_W(e_1 \cdot e_2^{-\epsilon}) \supseteq W_j \oplus W_{j'}$. Ein Widerspruch.

Sei nun also $E \cong C_9$ zyklisch.

Wähle $e \in E$ mit $\langle e \rangle = E$. Da $9 \nmid 33$ gilt, dass $E_0 := \langle e^3 \rangle$ planar ist. Sei B eine Bahn der Länge drei von E auf L_∞ , so gilt nach unseren obigen Betrachtungen, dass B eine Teilmenge der Fixunterebene \mathbb{T}_{E_0} ist. Also hat E eine Bahn der Länge drei und sonst nur Bahnen der Länge 9 auf L_∞ . Aber $33 \not\equiv 3 \pmod{9}$. Ein Widerspruch.

Es folgt die Behauptung. □

Es sei W ein $2n$ -dimensionaler K -Raum, $K = GF(2)$ mit n ungerade.

Satz 2.6.

Sei $\mathbb{T} = \mathbb{T}(W, \mathfrak{S})$ eine Translationsebene. Dann enthält das Translationskomplement kein Element der Ordnung 4.

Beweis.

Angenommen y sei ein solches Element. Nach dem Satz von Baer ist y^2 entweder eine Zentralkollineation oder planar. In jedem Fall ist $\dim(C_W(y^2)) = n$. Setze $U := C_W(y^2)$. Sei also $w \in W \setminus U$ und $wy^2 = w + u$ mit $0 \neq u \in U$, dann ist

$$w = wy^4 = (w + u)y^2 = w + u + uy^2 \implies u = uy^2$$

Damit ist durch $W \ni w \mapsto w + wy^2 \in U$ ein Homomorphismus mit Kern U definiert, welcher sogar ein Epimorphismus ist, also $W/U \cong U$. Man kann eine Basis $B_U = \{e_1, \dots, e_n\}$ von U so zu einer Basis $B = \{e_1, \dots, e_{2n}\}$ von W ergänzen, dass y^2 bezüglich B folgende Matrixdarstellung besitzt:

$$y^2 = \begin{pmatrix} \mathbb{1}_{n \times n} & \\ \mathbb{1}_{n \times n} & \mathbb{1}_{n \times n} \end{pmatrix}$$

Da y und y^2 kommutieren, lässt y den Raum U invariant, die Matrixdarstellung von y hat also die Form:

$$y = \begin{pmatrix} A & \\ B & A \end{pmatrix}$$

Damit erhalten wir:

$$\begin{pmatrix} \mathbb{1}_{n \times n} & \\ \mathbb{1}_{n \times n} & \mathbb{1}_{n \times n} \end{pmatrix} = y^2 = \begin{pmatrix} A^2 & \\ AB + BA & A^2 \end{pmatrix}$$

Wir wissen aus der linearen Algebra, dass $Spur(AB + BA) = 0$, sodass

$$1 = Spur(\mathbb{1}_{n \times n}) = Spur(AB + BA) = 0$$

ein Widerspruch. Es folgt die Behauptung des Lemmas. □

2.2. Kollineationen der Ordnung 31

Im Folgenden soll gezeigt werden, dass es (bis auf Äquivalenz) zwei nicht-desarguesche Translationsebene der Ordnung 32 gibt, die einen Automorphismus der Ordnung 31 besitzen.

2.2.1. Theoretische Vorbereitung der Computersuche

Lemma 2.7.

Das Translationskomplement einer Translationsebene (W, \mathfrak{S}) der Ordnung 32 über W enthalte eine Gruppe $H \cong C_{31}$. Dann kann eine Basis von W so gewählt werden, dass

$$H := \left\langle \begin{pmatrix} A & \\ & D \end{pmatrix} \right\rangle, \quad A, D \in GL(V) \text{ mit } |A| = |D| = 31.$$

Beweis.

Da $33 \equiv 2 \pmod{31}$ existieren in \mathfrak{S} unter H zwei Fixfasern. Koordinatisiere so, dass $V(0)$ und $V(\infty)$ diese Fasern sind. Mit Bemerkung 1.35 folgt die Behauptung \square

Bemerkung 2.8.

Es ist bekannt:

1. Über $GF(2)$ sind nach Lemma 1.4 zu einer irreduziblen Matrix A nur deren Potenzen $A^2, A^4, A^8, A^{16}, \dots$ konjugiert.
2. Sei $|A| = 31$ in $GL(5, 2)$, dann ist A ein Singer-Zyklus. Aus Teil 1 zusammen mit Bemerkung 1.3c folgt, dass die Konjugiertenklassen der Elemente in $\langle A \rangle \setminus \mathbb{1}$ repräsentiert werden können durch die folgende Menge von Exponenten von A :
 $k_0 := \{1, 2, 4, 8, 16\}$, $k_1 := \{3, 6, 12, 17, 24\}$, $k_2 := \{5, 9, 10, 18, 20\}$,
 $k_3 := \{7, 14, 19, 25, 28\}$, $k_4 := \{11, 13, 21, 22, 26\}$ und $k_5 := \{15, 23, 27, 29, 30\}$.
 Die Exponentenmenge $\hat{k} = \{1, 3, 5, 7, 11, 15\}$ repräsentiert demnach die Konjugiertenklassen von Elementen der Ordnung 31 in $GL(5, 2)$.

3. Die Begleitmatrix der Ordnung 31 hat die Gestalt $B = \begin{pmatrix} . & 1 & . & . & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \\ 1 & . & 1 & . & . \end{pmatrix}$.

Lemma 2.9.

Sei $\text{diag}(A, D)$ eine Kollineation der Ordnung 31, dann kann eine Koordinatisierung so gewählt werden, dass gilt

1. $A = B$.

2. $D = B^k$, mit $k \in \hat{k}$.

Beweis.

zu 1: In $GL(5, 2)$ sind alle Singer-Gruppen konjugiert, da sie maximale 31-Untergruppen und somit 31-Sylowgruppen sind. Wähle also eine Basis von $V(0)$ so, dass A bezüglich dieser Basis gleich der Begleitmatrix ist.

zu 2: Wähle eine Basis von $V(\infty)$ so, dass D bezüglich dieser Basis in der Singer-Gruppe $\langle B \rangle$ liegt. Nach Bemerkung 2.8 ist also $D = B^k$ mit $k \in \hat{k}$ \square

Definition 2.10.

Seien H, K Untergruppen der Gruppe $G \ni g$. Die Menge

$$HgK = \{h \cdot g \cdot k \mid h \in H, k \in K\}$$

ist eine **Doppelnebenklasse**.

Bemerkung 2.11.

- Bekannt ist für Doppelnebenklassen, dass $|HgK| = \frac{|H| \cdot |K|}{|gKg^{-1} \cap H|} = \frac{|H| \cdot |K|}{|K^g \cap H|}$ (siehe [HUP, Kap. I, Satz 2.19, S. 11]).
- Ist $diag(B, B^k)$ eine Kollineation, so hat \mathfrak{S} nach Bemerkung 1.35 die Form

$$\mathfrak{S} = V(\infty) \cup V(0) \cup \{V(B^{-i}TB^{ik}) \mid 0 \leq i \leq 30\}$$

Satz 2.12.

Sei $\mathfrak{S} = V(\infty) \cup V(0) \cup \{V(B^{-i}TB^{ik}) \mid 0 \leq i \leq 30\}$. Es genügt, T als Repräsentant einer Doppelnebenklasse zu wählen. Die Größe dieser Menge ist 10410.

Beweis.

Sei $Z \in Syl_{31}(G)$ eine 31-Sylowgruppe in $G = GL(5, 2)$, also $Z \cong \langle B \rangle$. Damit operiert Z scharf transitiv auf $V(5, 2) \setminus \{0\}$. Des Weiteren können die Vertreter von Z in G_v , dem Stabilisator von v in G , gewählt werden. Es gilt

$$|G : G_v| = 31 = |V \setminus \{0\}|, \text{ d.h. } |G_v Z| = \frac{|G_v| \cdot |Z|}{|G_v \cap Z|} = |G|$$

Daraus folgt $G = G_v \cdot Z = Z \cdot G_v$. Mit anderen Worten ist G_v ein Nebenklassenvertretersystem von G modulo Z und vice versa Z ein NKVS von G modulo G_v . Schreibe also G in der Doppelnebenklassenzerlegung als

$$G = \bigcup_{r \in R} ZrZ$$

2. Die Translationsebenen der Ordnung 32

mit $ZrZ = \bigcup_{z \in Z} zrZ$ und $R \subseteq G_v$. Wir wissen nach Bemerkung 2.11: $|ZrZ| = \frac{|Z|^2}{|Z^r \cap Z|}$

Falls $r \notin N_G(Z)$ folgt, dass $Z^r \cap Z = 1$ und damit $|ZrZ| = |Z|^2$.

Sei nun also $r \in N_G(Z)$, dann ist $Z = Z^r$ und damit $|ZrZ| = |Z| = |rZ|$.

Schreibe $N_G(Z) = \langle Z \rangle \cdot \langle Y \rangle$ mit $|Y| = 5$ und somit

$$|N_G(Z)| = \bigcup_{0 \leq k \leq 4} y^k Z.$$

Sei n die Anzahl der Doppelnebenklassen der Größe $|Z|^2$, so ist

$$|G| = 5 \cdot |Z| + n \cdot |Z|^2 = |Z| \cdot |G_v|$$

Da $|G_v| = 5 + n \cdot |Z| = 5 + n \cdot 31$ ist $n = \frac{|G_v - 5|}{31} = \frac{|GL(4,2)| \cdot 16 - 5}{31} = 10405$.

Zusammen mit den fünf Wahlen für $r \in N_G(Z)$ ergibt sich wie behauptet eine Menge der Größe 10410 als mögliche Wahlen von T . \square

Folgerung 2.13.

Eine Spread-Menge, einer Translationsebene der Ordnung 32, die einen Automorphismus der Ordnung 31 besitzt, hat die Form:

$$S = \{B^{-i}TB^{ik} \mid 0 \leq i \leq 30\},$$

wobei $T \in GL(5, 2)$, $k \in \hat{k}$.

2.2.2. Praktische Durchführung

1. Schritt: Erstellen der Singer-Gruppe

Zu der Begleitmatrix B wird die Singer-Gruppe $\langle B \rangle$ in GAP erstellt und gespeichert.

2. Schritt: Finden der Repräsentanten der Doppelnebenklassen

Bemerkung 2.14.

Sei $v := (0, 0, 0, 0, 1)$. Wir wissen aus der linearen Algebra, dass die Menge

$$G_v := \{A \in GL(5, 2) \mid A_{1*} = v\}$$

der Stabilisator der ersten Matrixzeile ist.

Algorithmus 8 Spread-Mengen aus Repräsentanten der Doppelnebenklassen

Eingabe: Singer-Gruppe $\langle B \rangle$, Stabilisator G_v der ersten Matrixzeile

Ausgabe: Spread-Mengen

Initialisierung: $Reps := \emptyset$, $R := \emptyset$

for i in $[1..Size(G_v)]$ **do**

 Bilde die DNK $\langle B \rangle \cdot G_v[i] \cdot \langle B \rangle$

if Kein Element dieser Bahn ist schon in $Reps$ **then**

 Füge $G_v[i]$ zu $Reps$ hinzu und teste die Bahn mit Algorithmus 2 auf Spread-Mengen Eigenschaft

if Test positiv **then**

 Füge die Bahn zu R hinzu

end if

end if

end for

Ausgabe R

Ergebnis:

Von den 10410 Mengen der Form $\mathbf{S} = \{B^{-i}TB^{ik} \mid 0 \leq i \leq 30\}$, mit $T \in R$, $k \in \hat{k}$, fällt bei 165 der Spread-Mengen-Test aus Algorithmus 2 positiv aus. Diese werden zusammen mit dem dazugehörigen Exponent von B als Spread-Menge gespeichert.

3. Schritt: Nicht-desarguesche Spread-Mengen heraus filtern

Zur Identifizierung der desargueschen Spread-Mengen werden diese durch Multiplikation mit dem inversen eines beliebigen Elementes der Spread-Menge normiert und die Ordnung der durch diese Menge erzeugten Gruppe betrachtet. Dabei treten zwei Fälle auf:

2. Die Translationsebenen der Ordnung 32

1. Die Ordnung der Gruppe ist 31, die Gruppe ist also kommutativ
⇒ Die durch diese Spread-Menge induzierte Ebene ist desarguesch
2. Die Ordnung der Gruppe ist > 31 , die Gruppe ist nicht kommutativ
⇒ Die durch diese Spread-Menge induzierte Ebene ist nicht desarguesch

Die Rechnung zeigt:

Von den ursprünglich 165 Spread-Mengen sind nur noch 20 nicht-desarguesch.

4. Schritt: Test auf Äquivalenz

Nach Durchführung der Prozedur *EQUIV* verbleiben zwei nicht isomorphe Spread-Mengen, wie zu Beginn des Kapitels behauptet.

Resultat:

Es handelt sich um die in Kapitel 5 beschriebenen Ebenen \mathbb{T}_2 und \mathbb{T}_3 .

2.3. Kollineationen der Ordnung 11

Im Folgenden wollen wir zeigen, dass es bis auf Äquivalenz genau eine nicht-desarguesche Translationsebene der Ordnung 32 gibt, die einen Automorphismus der Ordnung 11 zulässt.

2.3.1. Theoretische Vorbereitung der Computersuche

Definition 2.15.

Es sei wieder W ein K -Raum. Die nichttrivialen Vektoren von W werden **1-Räume** genannt. Entsprechend nennen wir die Menge der nichttrivialen Vektoren eines d -dimensionalen Teilraumes von W einen **d -Raum**.

Für dieses Kapitel seien für ein Element x des Vektorraumes $GF(2^{10})$:

- $\Sigma : x \mapsto x^2$ die Frobenius-Abbildung und
- $\Theta : x \mapsto x\theta$ die Singer-Abbildung repräsentiert durch ein primitives Element θ (vgl. Definition 1.2).

Lemma 2.16.

Die Gruppe $\langle \Theta, \Sigma \rangle$ operiert transitiv auf $GF(2^{10})^*$.

Beweis.

Klar, da θ primitives Element und Θ bereits scharf transitiv auf $GF(2^{10})^*$ operiert. \square

Lemma 2.17.

Sei H das Translationskomplement einer Translationsebene der Ordnung 32, die einen Automorphismus der Ordnung 11 zulässt. Dann ist $\langle \Theta^{93} \rangle \in \text{Syl}_{11}(H)$.

Beweis.

Folgt unmittelbar aus dem Satz von Sylow. \square

2.3.2. Praktische Durchführung

Man stellt fest, dass die Rechenoperation „+“ in endlichen Körpern unter *GAP* länger dauert, als die Operation „·“. Zu diesem Zweck wird von uns zuerst eine Additionstabelle für das Rechnen in $GF(2^{10})^*$ angelegt, also eine symmetrische 1023×1023 Matrix, deren Einträge an der Stelle (i, j) die Position der Summe des i -ten mit dem j -ten Element aus $GF(2^{10})^*$ angeben. Wir rechnen von nun an also nicht mehr mit Körperelementen sondern mit deren Position-repräsentierenden Zahlen.

Der nächste Schritt ist das Erstellen der Gruppe $\langle \Sigma, \Theta \rangle$, wobei $\theta := Z(2^{10})$ das primitive Element bezeichnet. Für alle $x \in GF(2^{10})^*$ werden die Positionen der Elemente $x \cdot \theta$ und x^2 als Permutationslisten (wiederum von Zahlen) gespeichert. Aus diesem Erzeugendensystem wird nun die Gruppe $\langle \Sigma, \Theta \rangle$ gebildet.

Unser erstes Ziel ist die sukzessive Konstruktion eines 5-Raumes in $GF(2^{10})$ (also eine Faser der Translationsebene) durch Hinzunahme von 1-Räumen und testen auf die in Lemma 2.16 und 2.17 angeführten Kriterien. Wir können o.B.d.A. annehmen, dass diese erste Faser das Einselement unseres Vektorraumes enthält. Wähle also als Start-1-Raum das erste Element aus $GF(2^{10})^*$, repräsentiert durch die Zahl 1.

Algorithmus 9 Konstruktion der n -Räume

Eingabe: Additionstabelle A für $GF(2^{10})^*$, Teilmenge der $n - 1$ -Räume S_{n-1}

Ausgabe: Menge der n -Räume S_n , die Räume aus S_{n-1} als Teilräume enthalten

Initialisierung: $S_n = \emptyset$

for i in $[1..Size(S_{n-1})]$ **do**

$s_{n-1} := S_{n-1}[i]$, $N_n := \{1, 2, \dots, 1023\} \setminus \{s_{n-1}\}$

for j in $[1..Size(N_n)]$ **do**

Setze $L_y := \{A[y][N_n[j]] \mid y \in s_{n-1}\} \cup \{N_n[j]\}$

$s_n := s_{n-1} \cup L_y$

Füge s_n zu S_n hinzu

end for

end for

Ausgabe S_n

Lemma 2.18.

Der Algorithmus liefert alle zulässigen n -Räume.

Beweis.

Schritt 1) überprüft alle n -Räume nach Lemma 2.17 und Schritt 2) filtert die redundanten n -Räume heraus nach Lemma 2.16. □

Algorithmus 10 Überprüfung der n -Räume

Eingabe: Menge der n -Räume S_n , Gruppen $\langle \Sigma, \Theta \rangle$ und $\langle \Theta^{93} \rangle$ **Ausgabe:** Menge der n -Räume \hat{S}_n , die die Bedingungen einer partiellen Faser erfüllen*Initialisierung:* $S'_n := \emptyset$, $\hat{S}_n := \emptyset$

1)

for i in $[1..Size(S_n)]$ **do** Teste für alle Elemente $z \in S_n[i]$, ob die Bahn von z unter $\langle \Theta^{93} \rangle$ nur den Durchschnitt $\{z\}$ mit $S_n[i]$ hat. Falls dies für alle $z \in S_n[i]$ erfüllt ist, füge $S_n[i]$ zu S'_n hinzu.**end for**

2)

Finde Vertreter der Äquivalenzklassen der Elemente von S'_n , wobei $s, s' \in S'_n$ genau dann äquivalent sind, wenn sie in einer $\langle \Sigma, \Theta \rangle$ -Bahn liegen, dazu:**while** $Size(S'_n) > 0$ **do** Bilde die Bahn eines noch nicht überdeckten Elementes aus S'_n unter $\langle \Sigma, \Theta \rangle$, füge dieses Element zu \hat{S}_n hinzu und streiche alle Elemente der Bahn aus S'_n .**end while**Ausgabe \hat{S}_n

Jeder der 92 gefundenen zulässigen 5-Räume wird nun um zwei weitere 5-Räume erweitert. Dies geschieht durch dasselbe Vorgehen wie in Algorithmus 9. Das Testprinzip auf Zulässigkeit beziehungsweise Redundanz ist äquivalent zu demjenigen in Algorithmus 10.

Ergebnis: 21 Tripel aus zulässigen 5-Räumen.

Zu Beginn des Kapitels wurden die affinen Punkte unserer Translationsebene mit den Körperelementen aus $GF(2^{10})$ identifiziert. Um aus drei 5-Räumen eine Matrix-Spread-Menge bezüglich eines Referenztripels aus drei Fasern zu erhalten, werden die 5-Räume in Vektorräume über $GF(2)$ überführt. Dazu werden die Zahlen, die die 5-Räume repräsentieren zunächst wieder mit den Körperelementen identifiziert. Aus den so erhaltenen Vektoren können mit einer GAP-Prozedur direkt drei fünfdimensionale Vektorräume erstellt werden. Das Bilden einer Bahn unter $\langle \Theta^{93} \rangle$ liefert eine komplette Faserung der Mächtigkeit 33 von W . Aus dieser Faserung kann wie in Algorithmus 1 angegeben eine Spread-Menge konstruiert werden.

Der anschließende Äquivalenztest aus Algorithmus 5 zeigt, dass alle gefundenen Spread-Mengen äquivalent sind. Somit ist die Behauptung zu Beginn des Kapitels gezeigt.

Resultat:

Es handelt sich um die in Kapitel 5 beschriebene fahnentransitive Ebene \mathbb{T}_4 .

2.4. Kollineationen der Ordnung 7

Im Folgenden soll gezeigt werden, dass es **keine** Translationsebene der Ordnung 32 mit Automorphismus der Ordnung 7 gibt.

2.4.1. Theoretische Vorbereitung der Computersuche

Die Überlegungen im Fall der Automorphismen der Ordnung 7 können teilweise auf die von uns vorgenommenen Beobachtungen im Falle der Ordnung 31 übertragen werden.

Lemma 2.19.

1. Die Begleitmatrix der Ordnung 7 ist eine Matrix der $GL(3, 2)$, die auf natürliche Weise mit einer Matrix der $GL(5, 2)$ identifiziert werden kann.

$$B := \begin{pmatrix} \cdot & 1 & \cdot \\ \cdot & \cdot & 1 \\ 1 & 1 & \cdot \end{pmatrix} \mapsto \begin{pmatrix} \mathbb{1}_{2 \times 2} & 0 \\ 0 & B \end{pmatrix} =: A$$

2. $\langle A \rangle$ ist konjugiert zu jeder 7-Sylowgruppe von $GL(5, 2)$.
3. A ist konjugiert zu A^2 und A^4 , ebenso sind A^3, A^5 und A^6 zueinander konjugiert.

Beweis.

zu 1: Siehe Folgerung 1.5.

zu 2: Folgt direkt aus den Sylow-Sätzen.

zu 3: Nach Bemerkung 2.8 Teil 1 ist B in $GL(3, 2)$ nur zu $B^2, B^4, B^8 = B^1$ konjugiert und B^3 nur zu $B^6, B^{12} = B^5$ sowie $B^{10} = B^3$. Zusammen mit Teil 1 des Lemmas folgt die Behauptung. \square

Da $|\mathfrak{C}| = 33 \equiv 5 \pmod{7}$ gibt es bei einem Automorphismus der Ordnung 7 genau fünf Fixfasern, die eine Fixunterebene der Ordnung 4 enthalten. Diese Fasern seien $V(0), V(\infty), V(t_1), V(t_2), V(t_3)$ mit $t_1, t_2, t_3 \in GL(5, 2)$. Zusätzlich enthält eine Spread-Menge noch vier disjunkte 7-Spread-Mengen, die als Bahnen des Automorphismus bezüglich eines Repräsentanten aufgefasst werden können.

Satz 2.20.

1. Sei $e \in GF(2)^3 \setminus \{0\}$ beliebig, dann ist $e\langle B \rangle = GF(2)^3 \setminus \{0\}$
2. Sei $\langle x \rangle$ eine Kollineationsgruppe der Ordnung 7 mit $V(0), V(\infty)$ als Fixfasern. Dann können Basen von $V(0)$ und $V(\infty)$ so gewählt werden, dass gilt:

$$x = \begin{pmatrix} A & \\ & A \end{pmatrix}$$

Beweis.

zu 1: Wir wissen, dass $|e \cdot \langle B \rangle| = |\langle B \rangle : C_{\langle B \rangle}(e)|$. Aber $C_{V(3,2)}(\langle B \rangle) = 0$, das bedeutet $C_{\langle B \rangle}(e) = 1$, woraus folgt

$$|e \cdot \langle B \rangle| = |\langle B \rangle| = 7 = |V(3,2) \setminus \{0\}|$$

zu 2: Nach Bemerkung 2.8 ist $B \sim B^2, B^4$ und $B \approx B^{-1}, B^{-2}, B^{-4}$. Daher auch $A \sim A^2 \sim A^4$ und $A \approx A^{-1}, A^{-2}, A^{-4}$. Also existieren Basen von $V(0)$ und $V(\infty)$, so dass $x_{V(0)} = A$ und $x_{V(\infty)} \in \langle A \rangle$. Ist dabei $x_{V(\infty)} \in \{A, A^2, A^4\}$ so kann man sogar $x_{V(\infty)} = A$ annehmen, da $A \sim A^2 \sim A^4$ in $N_{GL(5,2)}(\langle A \rangle)$.

Ist $x_{V(\infty)} \in \{A^{-1}, A^{-2}, A^{-4}\}$ so kann man analog $x_{V(\infty)} = A^{-1}$ annehmen.

Angenommen $V(t)$ ist fix unter $y := \begin{pmatrix} A^{-1} & 0 \\ 0 & A \end{pmatrix}$, dann ist $V(t)y = V(AtA)$ und damit $t = AtA$ was aber äquivalent ist zu $t^{-1}A^{-1}t = A$. Wir wissen jedoch, dass A in $GL(5,2)$ nicht zu ihrer Inversen A^6 konjugiert ist nach Lemma 1.4. Ein Widerspruch. Es folgt die Behauptung. \square

Folgerung 2.21.

Eine 7-Spread-Menge enthält eine Matrix, deren erste Zeile in

$R := \{r_1, \dots, r_4\} = \{(0, 0, 0, 0, 1), (0, 1, 0, 0, 1), (1, 0, 0, 0, 1), (1, 1, 0, 0, 1)\}$ *liegt.*

Beweis.

Sei M eine Matrix aus einer 7-Spread-Menge. Es sind $M_{1*} = (a, b)$ mit $a \in GF(2)^2$, $b \in GF(2)^3$ und $x = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$.

Dann ist $V(M)x = V(A^{-1}MA)$, wobei klar ist, dass $(A^{-1}M)_{1*} = M_{1*}$.

Daraus folgt $(A^{-1}MA)_{1*} = M_{1*}A = (a, bB)$. Wegen $\det(M - A^{-1}MA) \neq 0$ ist $bB \neq b$, also $b \neq 0$.

Nach Satz 2.20 existiert eine Matrix M' mit $V(M') \in B(M) \cdot \langle x \rangle$ und $M'_{1*} = (a, e)$, wobei $e = (0, 0, 1)$.

Es folgt die Behauptung. \square

Notation 2.22.

Sei $r \in V$. Setze

$$Pot(r) = \{M \in GL(V) \mid M_{1*} = r\} = \{M \in GL(V) \mid (1, 0, \dots, 0)M = r\}.$$

Eine solche Menge bezeichnen wir mit **Topf** bezüglich einer ersten Matrixzeile r .

2. Die Translationsebenen der Ordnung 32

Lemma 2.23.

Sei R wie in Folgerung 2.21 und $r \in R$. Dann gilt

$$Pot(r) = G_v \cdot E$$

wobei E ein beliebiges Element in $Pot(r)$ und $v = (0, 0, 0, 0, 1)$ ist.

Beweis.

Aus der Gruppentheorie wissen wir:

Falls eine Gruppe H transitiv auf der Menge $\Omega \ni \omega_0, \omega_1$ operiert und H_0 der Stabilisator von ω_0 in H ist, dann gilt:

$$\{h \in H \mid \omega_0 h = \omega_1\} = H_0 h_0,$$

wobei h_0 ein beliebiges Element mit $\omega_0 h_0 = \omega_1$ ist.

Anwenden auf $H = GL(5, 2)$, $\Omega = V \setminus \{0\}$, $\omega_0 = v$ und $\omega_1 = r$ liefert die Behauptung. \square

Folgerung 2.24.

Eine Spread-Menge mit Automorphismus der Ordnung 7 hat die Form:

$$\mathcal{S} = \{t_1, t_2, t_3\} \cup \bigcup_{i=1}^4 \{A^{-j} T_i A^j \mid 1 \leq j \leq 7\}$$

für $T_i \in Pot(r_i)$.

2.4.2. Praktische Durchführung

1. Schritt: Erstellen der Sylow-7-Untergruppe

Zu der Begleitmatrix B bilden wir die Matrix $A = \begin{pmatrix} \mathbb{1}_{2 \times 2} & \\ & B \end{pmatrix}$ sowie die durch A erzeugte Sylow-7-Gruppe $\langle A \rangle$.

2. Schritt: Einteilen von Töpfen

Zu den in Folgerung 2.21 aufgeführten ersten Matrixzeilen R werden die Töpfe $Pot(r_i)$ mit $r_i \in R$ und $i \in \{1, \dots, 4\}$ konstruiert und gespeichert.

$$Pot(r_i) = G_v \cdot g, \text{ für ein } g \in Pot(r_i)$$

Die Größe jedes Topfes beträgt 322560 Matrizen.

3. Schritt: Herstellen der 7-Spread-Mengen

Alle Elemente aus jedem Topf werden mit den Potenzen von A konjugiert, sodass eine Bahn der Länge sieben entsteht, die mit der Spread-Mengen Bedingung aus Algorithmus 2 überprüft wird.

Hierbei stellt sich heraus, dass es in keinem der Töpfe eine 7-Spread-Menge gibt, was unsere anfängliche Behauptung zeigt.

2.5. Kollineationen der Ordnung 5

Im Folgenden soll gezeigt werden, dass es bis auf Äquivalenz sechs nicht-desarguesche Translationsebenen der Ordnung 32 gibt, die einen Automorphismus der Ordnung 5 zulassen.

2.5.1. Theoretische Vorbereitung der Computersuche

Ähnlich wie im Fall der Ordnung 7 ergibt sich:

Lemma 2.25.

1. Die Begleitmatrix der Ordnung 5 ist eine Matrix der $GL(4, 2)$, die auf natürliche Weise mit einer Matrix der $GL(5, 2)$ identifiziert werden kann.

$$B := \begin{pmatrix} \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix} =: A$$

2. $\langle A \rangle$ ist konjugiert zu jeder 5-Sylowgruppe von $GL(5, 2)$.
3. A ist konjugiert zu A^i für alle $i = 1, \dots, 5$

Beweis.

Siehe Beweis zu Lemma 2.19. □

Da $|\mathfrak{E}| = 33 \equiv 3 \pmod{5}$ gibt es bei einem Automorphismus der Ordnung 5 genau drei Fixfasern, die eine Fixunterebene der Ordnung 2 enthalten. Diese Fasern seien bei geeigneter Basenwahl $V(0), V(\infty), V(1)$. Zusätzlich enthält eine Spread-Menge noch sechs disjunkte 5-Spread-Mengen, die wie im Fall der Ordnung 7 als Bahnen des Automorphismus bezüglich eines Repräsentanten aufgefasst werden können.

Folgerung 2.26.

Repräsentanten der 5-Spread-Mengen sind Matrizen, deren erste Zeile in der Menge $R := \{(1, 1, 0, 0, 0), (0, 1, 0, 0, 0), (1, 1, 0, 0, 1), (0, 1, 0, 0, 1), (1, 1, 1, 0, 0), (0, 1, 1, 0, 0)\} = \{r_1, \dots, r_6\}$ enthalten ist.

Beweis.

Die $\langle B \rangle$ -Bahnen auf $V(4, 2)$ können repräsentiert werden durch die Vektoren $(1, 0, 0, 0)$, $(1, 0, 0, 1)$ und $(1, 1, 0, 0)$. Des Weiteren siehe Beweis zu Folgerung 2.21. □

Folgerung 2.27.

Eine Spread-Menge mit Automorphismus der Ordnung 5 hat die Form:

$$\mathbf{S} = \mathbb{1}_{5 \times 5} \cup \bigcup_{i=1}^6 \{A^{-j}T_iA^j \mid 1 \leq j \leq 5\},$$

wobei $T_i \in \text{Pot}(r_i)$.

2.5.2. Praktische Durchführung

1. Schritt Erstellen der Sylow-5-Untergruppe

Wie im Fall der Ordnung 7.

2. Schritt: Einteilen von Töpfen

Zu den in Folgerung 2.26 aufgeführten ersten Matrixzeilen R werden die Töpfe $Pot(r_i)$ mit $r_i \in R$ und $i \in \{1, \dots, 6\}$ konstruiert und gespeichert.

$$Pot(r_i) = G_v \cdot g, \text{ für ein } g \in Pot(r_i)$$

Die Größe jedes Topfes beträgt 322560 Matrizen.

3. Schritt: Herstellen der 5-Spread-Mengen

Algorithmus 11 5-Spread-Mengen Töpfe

Eingabe: Töpfe $Pot(r_i)$ mit $r_i \in R$

Ausgabe: 5-Spread-Mengen Töpfe

Initialisierung: $Pots := \emptyset$ als 5-Spread-Mengen Töpfe

for i in $[1..Size(R)]$ **do**

for j in $[1..Size(Pot(r_i))]$ **do**

 Bilde die Bahn $U := \{A^{-k} \cdot Pot(r_i)[j] \cdot A^k \mid k = 1, \dots, 5\}$

 Teste $U \cup \mathbb{1}$ auf Spread-Mengen-Bedingung

if Test positiv **then**

 Füge U zu $Pots[i]$ hinzu

end if

end for

end for

Ausgabe $Pots$

Ergebnis:

In jedem der sechs Töpfe befinden sich nun 6818 der 5-Spread-Mengen.

4. Schritt: Sukzessiver Aufbau der nicht-desargueschen Spread-Mengen

Algorithmus 12 Spread-Mengen

Eingabe: 5-Spread-Mengen Töpfe $Pots$ **Ausgabe:** Spread-Mengen*Initialisierung:* $5er := \emptyset$ als Menge der 5-Spread-Mengen**for** i in $[1..Size(Pots[1])]$ **do** $P := Pots[1][i] \cup \mathbb{1}$ **while** $2 \leq j \leq 6$ **do****for** k in $[1..Size(Pots[j])]$ **do****if** $P := P \cup Pots[j][k]$ ist partielle Spread-Menge = true **then** $j := j + 1$ **end if****end for****end while**Füge P zu $5er$ hinzu**end for**Ausgabe $5er$

Ergebnis:

Wir erhalten 276 nicht-desarguesche Spread-Mengen

5. Schritt: Test auf ÄquivalenzNach der Durchführung des Äquivalenztestes *EQUIV* erhalten wir sechs nicht-äquivalente Spread-Mengen.*Resultat:*Es handelt sich um die in Kapitel 5 beschriebenen Ebenen $\mathbb{T}_2, \mathbb{T}_3, \mathbb{T}_4, \mathbb{T}_5, \mathbb{T}_6$ und \mathbb{T}_7 .

2.6. Kollineationsgruppen der Ordnung 6

2.6.1. Theoretische Vorbereitung der Computersuche

Im Folgenden soll gezeigt werden, dass es keine nicht-desarguesche Translationsebene der Ordnung 32 gibt, die einen Automorphismus der Ordnung 6 zulässt.

1. Fall: Zyklische Gruppe

Lemma 2.28.

Das Translationskomplement einer Translationsebene (W, \mathfrak{C}) der Ordnung 32 über W enthalte eine Gruppe $H \cong C_3 \times C_2 = \langle s, t \rangle$ mit $|s| = 3$ und $|t| = 2$. Dann kann eine Basis von W so gewählt werden, dass

$$s = \begin{pmatrix} \hat{A} & \\ & \hat{A} \end{pmatrix}, t = \begin{pmatrix} \mathbb{1} & \\ & \mathbb{1} \end{pmatrix},$$

wobei $|\hat{A}| = 3$.

Beweis.

Da $33 = 1 \pmod{2}$ existiert eine Faser, die unter t fix bleibt, diese sei X . Da H abelsch ist lässt s ebenfalls die Faser X fix. Daraus folgt, dass s planar ist, was bedeutet, dass zwei weitere Fasern Y und Z unter s fix bleiben. Diese drei Fasern enthalten eine Fixunterebene der Ordnung 2. Identifiziere bei geeigneter Basenwahl X, Y, Z mit $V(0), V(\infty), V(1)$, so hat s nach Folgerung 1.35 die Form

$$s = \begin{pmatrix} A & \\ & A \end{pmatrix}, \quad \text{mit } |A| = 3$$

und t die Form:

$$t = \begin{pmatrix} D & \\ & D \end{pmatrix},$$

wobei $D = \mathbb{1}$ gilt, da t eine Elation ist.

Sei weiterhin $\hat{Z} = \begin{pmatrix} Z & \\ & Z \end{pmatrix} \in C_{GL(W)}(y)$, dann ist $\hat{H} := \langle \hat{Z}^{-1}x\hat{Z}, \hat{Z}^{-1}y\hat{Z} \rangle$ eine Gruppe, die die Fasern $V(0), V(\infty)$ und $V(1)$ fix lässt. Wähle \hat{Z} so, dass

$$\hat{A} := Z^{-1}AZ = \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}.$$

$$\implies H = \left\langle \begin{pmatrix} \hat{A} & \\ & \hat{A} \end{pmatrix}, \begin{pmatrix} \mathbb{1} & \\ & \mathbb{1} \end{pmatrix} \right\rangle$$

□

Folgerung 2.29.

Repräsentanten der 6-Spread-Mengen sind Matrizen, deren erste Zeile in der Menge $R := \{r_1, \dots, r_5\} = \{(0, 0, 0, 1, 0), (0, 0, 1, 1, 1), (1, 0, 1, 0, 1), (0, 1, 0, 0, 0), (1, 1, 0, 1, 1)\}$ enthalten ist.

Beweis.

Siehe Beweis zu Folgerung 2.21. □

Folgerung 2.30.

Für eine Matrix $T \in GL(V)$ definiere $T_A^{(1)} := A^{-1} \cdot T \cdot A + \mathbb{1}$ und entsprechend $T_A^{(2)} := A^{-1} \cdot T_A^{(1)} \cdot A + \mathbb{1}$ et cetera.

Dann hat eine Spread-Menge mit Automorphismus der Ordnung 6 die Form:

$$\mathcal{S} = \mathbb{1}_{5 \times 5} \cup \bigcup_{i=1}^5 \{T_A^{(j)} \mid 1 \leq j \leq 6\},$$

wobei $T_i \in \text{Pot}(r_i)$.

2. Fall: Symmetrische Gruppe**Lemma 2.31.**

Das Translationskomplement einer Translationsebene (W, \mathfrak{S}) der Ordnung 32 über W enthalte eine Gruppe $H \cong \text{Sym}(3) = \langle s, t \rangle$ mit $|s| = 3$ und $|t| = 2$. Dann ist s nicht planar und es kann eine Basis von W so gewählt werden, dass

$$s = \begin{pmatrix} & A \\ A & A \end{pmatrix}, t = \begin{pmatrix} & D \\ D & D \end{pmatrix},$$

wobei $A^3 = \mathbb{1} = D^2$ und $DAD = A^2$.

Beweis.

Angenommen s sei planar, X, Y, Z sei die Fixunterebene der Ordnung 2. Nun wissen wir, dass t die Menge der Fixfasern invariant lässt, da t die von s erzeugte Gruppe normalisiert. Jedoch ist t eine Elation, das heißt eine der Fixfasern, etwa X , ist Achse von t . Sei $x \in X \setminus C_X(s)$. Wir wissen, dass $|C_X(s)| = 2$ und da auch xs in X liegt gilt:

$$xs^{-1} = xt = xst = xs \implies xs = x$$

ein Widerspruch.

Also operiert s fixpunktfrei. Da t genau eine Fixfaser hat, gibt es folglich genau eine

2. Die Translationsebenen der Ordnung 32

H -Bahn auf \mathbf{S} der Länge 3. Wähle die Koordinatisierung so, dass diese Bahn gleich $\{V(0), V(\infty), V(1)\}$ ist und dass $V(0)t = V(0)s = V(\infty)$ gilt und somit auch

$$s = \begin{pmatrix} & C \\ A & B \end{pmatrix}, t = \begin{pmatrix} & E \\ D & \end{pmatrix}$$

Da $V(\infty)s = V(1)$ und $V(1)s = V(0)$ folgt $A = B = C$ sowie $A^3 = \mathbb{1}$, da $|s| = 3$. Äquivalente Überlegungen zeigen, dass aus $V(1)t = V(1)$ folgt, dass $E = D^{-1}$. Schließlich zeigt die Gleichung $s^2 = tst$, dass $D^{-1}AD = DAD = A^2$ und so $D^2 = \mathbb{1}$. \square

Bemerkung 2.32.

- Da eine Faser $V(T) \in \mathbf{S}$ unter H die Bahn

$$\begin{aligned} \text{Orb}(T) := \{ & V(T), V(D^{-1}T^{-1}D), V(\mathbb{1} + A^{-1}TA), V([\mathbb{1} + ATA^{-1}]^{-1}), \\ & V([\mathbb{1} + (AD)^{-1}TAD]^{-1}), V(\mathbb{1} + (DA)^{-1}TDA)\} \end{aligned}$$

bildet, ist es nicht möglich, eine Einteilung in Bahnen von Töpfen zu treffen, wie in den übrigen Fällen. Das Invertieren lässt keine Vorhersage über das Verhalten der ersten Zeile einer Matrix zu.

- Wir wissen aus der linearen Algebra und unseren vorherigen Überlegungen aus Lemma 2.8, dass es nur drei Konjugiertenklassen von Matrizen der Ordnung 3 gibt. Daher

$$A \in \tilde{A} := \{A_1, A_2, A_3\} = \left\{ \mathbb{1}_{5 \times 5}, \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}, \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix} \right\}$$

- Ebenso ist bekannt, dass es genau drei Konjugiertenklassen von Matrizen der Ordnung 2 gibt, diese sind

$$\tilde{D} := \{D_1, D_2, D_3\} = \left\{ \mathbb{1}_{5 \times 5}, \begin{pmatrix} 1 & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix} \right\}$$

Aufgrund dieser einfachen Blockstruktur folgt direkt, dass D in Abhängigkeit von A gewählt werden kann als

$$\tilde{D}(A_1) = \tilde{D}(\mathbb{1}) = \tilde{D}, \quad \tilde{D}(A_2) = \tilde{D} \setminus \mathbb{1}, \quad \tilde{D}(A_3) = D_3$$

Folgerung 2.33.

Eine Spread-Menge mit symmetrischer Kollineationsgruppe der Ordnung 6 hat die Form:

$$\mathbf{S} = \mathbb{1}_{5 \times 5} \cup \bigcup_{i=1}^5 \{Orb(T_i)\},$$

wobei $T_i \in GL(5, 2)$, $A \in \tilde{A}$, $D \in \tilde{D}(A)$.

3. Fall: Kollineationsgruppen der Ordnung 12 – Alternierende Gruppe

Da $C_2 \times C_2 \leq Alt(4)$, siehe 2.7.1 Fall 2.

2.6.2. Praktische Durchführung

1. Fall:

Die Suche im Fall der zyklischen Kollineationsgruppe der Ordnung 6 verläuft äquivalent wie im Falle der Ordnung 5 mit R wie oben und einer Substitution der Bahn U aus Algorithmus 11 zu $U := \{Pot(r_i)_A^{(1)}, \dots, Pot(r_i)_A^{(6)}\}$.

Bei Schritt 4 der Suche stellt sich heraus, dass in diesem Fall keine vollständigen Spread-Mengen existieren.

2. Fall:

1. Schritt: Erstellen des Topfes $Pot(v)$, wobei $v := (0, 0, 0, 0, 1)$

$$Pot(v) = G_v \cdot g, \quad \text{für ein } g \in Pot(v)$$

Des Weiteren wurden zu jeder Matrix $T \in Pot(v)$ die Bahnen $Orb(T)$ für alle Wahlen von D und A gebildet.

Ergebnis:

Je 64512 Bahnen (6-Spread-Mengen), die Matrizen T mit $T_{1*} = v$ enthalten.

2. Schritt: Reduktion der Bahnen

Um die 6-Spread-Mengen auf Äquivalenz zu prüfen, reicht ein Test unter der Operation $op_0(g)$ aus Satz 1.30 für $g \in GL(5, 2)$. Da diese Gruppe den internen Speicher des Programms GAP übersteigt, wird die Gruppe dargestellt als

$$GL(5, 2) = \langle B \rangle \cdot G_v$$

wobei B die Begleitmatrix der Ordnung 31 ist. Es stellt sich heraus, dass es schon genügt nur mit Elementen von G_v zu operieren, um zu zeigen, dass alle 6-Spread-Mengen für alle Wahlen von D und A äquivalent sind.

Wir erhalten also lediglich je eine Startermenge der Größe 6.

3. Schritt: Erstellen weiterer Töpfe und Bildung der Spread-Mengen

Da das Erstellen sämtlicher Töpfe, die alle die Größe 64512 haben, ebenfalls den Speicherplatz übersteigen würde, haben wir folgende Vorüberlegungen zu treffen:

- Es sind nur solche Töpfe zu betrachten, deren Matrizen *keine* erste Zeile aus $Orb(T)$ enthalten.
- Aufgrund der Struktur von $Orb(T)$ sind nur solche Töpfe $Pot(w)$ zu generieren, mit $w = (0, *, *, *, *)$ und $* \in \{0, 1\}$.

Für jede Startermenge werden nun also nur noch ≤ 8 Töpfe notwendig. Aus diesen werden wie in Algorithmus 11 die partiellen Spread-Mengen sukzessive vervollständigt.

Ergebnis:

Alle 6 auf diese Weise gefundenen Spread-Mengen sind desarguesch.

2.7. Kollineationsgruppe der Ordnung 4

2.7.1. Theoretische Vorbereitung der Computersuche

Da wir zu Beginn des Kapitels gezeigt haben, dass es keine zyklische Kollineationsgruppe der Ordnung 4 gibt, bleibt nur die Untersuchung einer Kleinschen Vierergruppe von Kollineationen.

Lemma 2.34.

Das Translationskomplement einer Translationsebene (W, \mathfrak{S}) der Ordnung 32 über W enthalte eine Gruppe $H \cong C_2 \times C_2 = \langle s, t \rangle$. Dann kann eine Basis von W so gewählt werden, dass H erzeugt wird von Elationsmatrizen (siehe [JOH, Kap. 23.2, S. 340ff]) der Form

$$s = \begin{pmatrix} \mathbb{1} & \mathbb{1} \\ & \mathbb{1} \end{pmatrix}, t = \begin{pmatrix} \mathbb{1} & D \\ & \mathbb{1} \end{pmatrix},$$

wobei $D \in GL(5, 2)$ nicht den Eigenwert 1 hat.

Beweis.

Da $33 \equiv 1 \pmod{4}$ gibt es genau eine Fixfaser. Koordinatisiere so, dass $V(\infty)$ diese Faser ist und eine H -Bahn die Fasern $V(0)$ und $V(1)$ enthält, die von s vertauscht werden. Dann folgt ähnlich zu den obigen Beweisen zu Lemma 2.28 und 2.31 für die Matrixschreibweise von s und t :

$$s = \begin{pmatrix} A & A \\ & A \end{pmatrix}, \quad t = \begin{pmatrix} C & D \\ & C \end{pmatrix}, \quad \text{mit } |A| = |C| = 2$$

Sei $V(T)$ eine beliebige Faser von \mathfrak{S} , dann hat $V(T)$ unter H die Bahn

$$V(T), V(\mathbb{1} + A^{-1}TA), V(C^{-1}D + C^{-1}TC), V(\mathbb{1} + C^{-1}D + C^{-1}TC), V(\mathbb{1} + C^{-1}D + A^{-1}TA)$$

und da $|H| = 4$ folgt $C = A$. Normiere nun s und erhalte:

$$H = \left\langle \begin{pmatrix} \mathbb{1} & \mathbb{1} \\ & \mathbb{1} \end{pmatrix}, \begin{pmatrix} \mathbb{1} & D \\ & \mathbb{1} \end{pmatrix} \right\rangle$$

Zu klären bleibt nun noch der Eigenwert von D . Da t eine Elation ist, ist D nicht singulär.

Für eine Faser $V(T)$ mit $T \in GL(5, 2)$ ergibt sich die Bahn:

$$V(T), V(T + \mathbb{1}), V(T + D), V(T + D + \mathbb{1}).$$

Da $V(\infty)$ unter H fix bleibt und $V(0)$ in der Bahn

$$V(0), V(1), V(D), V(D + \mathbb{1})$$

2. Die Translationsebenen der Ordnung 32

liegt, folgt $\det(D + \mathbb{1}) \neq 0$. Aus der linearen Algebra wissen wir:

$$\begin{aligned} \det(D + \mathbb{1}) &\neq 0 \\ \iff (D + \mathbb{1})v &\neq 0, \quad \text{für alle } 0 \neq v \in V \\ \iff Dv &\neq v, \quad \text{für alle } 0 \neq v \in V \\ \iff 1 &\text{ ist kein Eigenwert von } D \end{aligned}$$

□

Lemma 2.35.

Sei D wie oben, dann ist $|D| \in \{21, 31\}$

Beweis.

Falls $|D| = 2^k$ für ein $k \in \mathbb{N}$, so gibt es ein $v \in V = V(5, 2)$ mit $Dv = v$, also ist nach obiger Beobachtung $\det(D + \mathbb{1}) = 0$. Ein Widerspruch.

Sei nun $|D|$ ungerade. Ist D irreduzibel, so ist $\langle D \rangle \subseteq \text{End}(V)$ ein Körper genau dann, wenn $|D| = 31$, siehe [JOH, App. II, Bem. II.7].

Sei also D reduzibel. Nach dem Satz von Maschke [JOH, App. II, Satz II.5] lässt sich eine disjunkte Zerlegung von V in D -invariante Räume $V = V_1 \oplus \dots \oplus V_n$ für ein $n \in \mathbb{N}$ finden. Für alle $1 \leq i \leq n$ gilt stets $\dim(V_i) > 1$, da sonst D einen nichttrivialen Fixpunkt hat. Die einzige Möglichkeit einer solchen Zerlegung ist $V = V_1 \oplus V_2$ mit $\dim(V_1) = 2$ und $\dim(V_2) = 3$. Da D irreduzibel auf V_1, V_2 ist, hat die Einschränkung auf V_1 die Ordnung 3, diejenige auf V_2 die Ordnung 7. Daraus folgt $|D| = 21$

Angenommen $|D| = 2k$ für ein $k \in \mathbb{N}$, dann ist $\hat{D} := D^k$ eine Involution. Sei $v := w \cdot (\hat{D} + \mathbb{1}) \in \text{Im}(\hat{D} + \mathbb{1})$, dann gilt

$$v \cdot (\hat{D} + \mathbb{1}) = w \cdot (\hat{D} + \mathbb{1})^2 = w \cdot (\hat{D}^2 + \mathbb{1}) = 0.$$

Daraus folgt $\text{Im}(\hat{D} + \mathbb{1}) \subseteq \ker(\hat{D} + \mathbb{1})$ und somit können folgende Möglichkeiten auftreten:

1. Fall: $\dim(\text{Im}(\hat{D} + \mathbb{1})) = 1$ und $\dim(\ker(\hat{D} + \mathbb{1})) = 4$:

Dann ist $\text{Im}(\hat{D} + \mathbb{1})$ ein D -Modul der Dimension 1, womit D einen nicht-trivialen Fixpunkt besitzt.

2. Fall: $\dim(\text{Im}(\hat{D} + \mathbb{1})) = 2$ und $\dim(\ker(\hat{D} + \mathbb{1})) = 3$:

Sei $1 \neq U = D^{2^s}$ mit $s \in \mathbb{N}$ der 2-Anteil von D . Dann wird $\ker(\hat{D} + \mathbb{1})$ unter D fix gelassen und somit auch $\text{Im}(\hat{D} + \mathbb{1})$. Wiederum nach dem Satz von Maschke existiert ein 1-dimensionaler, U -invarianter Teilraum Y mit $Y \oplus \text{Im}(\hat{D} + \mathbb{1}) = \ker(\hat{D} + \mathbb{1})$. Falls nun U trivial auf $\ker(\hat{D} + \mathbb{1})$ operiert, so induziert D auf $\ker(\hat{D} + \mathbb{1})$ ein Element von 2-Potenz-Ordnung, das heißt es existiert ein nicht-trivialer Fixpunkt von D . Falls U nichttrivial operiert, induziert U auf $\text{Im}(\hat{D} + \mathbb{1})$ ein Element der Ordnung 3 und $C_{\ker(\hat{D} + \mathbb{1})}(U) = Y$. Dann ist Y somit D -invariant, es existiert also wieder ein nicht-trivialer Fixpunkt. □

Bemerkung 2.36.

Da D irreduzibel ist, kann man ohne Einschränkung D auf Normalform bringen. Nach dem obigen Lemma gibt es die folgenden Wahlen für D :

$$D_1 := \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & 1 & \cdot & \cdot \end{pmatrix}, D_2 := \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot & 1 \end{pmatrix}$$

Mit $|D_1| = 31$ und $|D_2| = 21$. Analog zu Bemerkung 2.8 sind die Potenzen $\hat{k}_1 = \{1, 3, 5, 7, 11, 15\}$ von D_1 , sowie $\hat{k}_2 = \{1, 3, 5, 7, 9\}$ von D_2 zu betrachten.

Folgerung 2.37.

Eine Spread-Menge mit Automorphismengruppe der Ordnung 4 hat die Form:

$$\mathbf{S} = \{\mathbb{1}_{5 \times 5}, D, D + \mathbb{1}_{5 \times 5}\} \cup \bigcup_{i=1}^7 \{T_i, T_i + \mathbb{1}, T_i + D, T_i + D + \mathbb{1}\},$$

wobei $T_i \in GL(5, 2)$.

2.7.2. Praktische Durchführung

Die durch D_i und deren Potenzen induzierten 4–Spread-Mengen Töpfe lassen sich nicht so allgemein wie in Folgerung 2.21 angeben, sondern werden für jede Wahl durch folgenden Algorithmus erzeugt:

Algorithmus 13 Repräsentantensystem der 4–Spread-Mengen Töpfe

Eingabe: Matrix D

Ausgabe: Repräsentantensystem R der ersten Matrixzeilen

Initialisierung: $e := \{v \mid v \in V(5, 2) \setminus \{0\}\}$, $R := \emptyset$, $w := (1, 0, 0, 0, 0)$

while $Size(e) > 0$ **do**

 Füge $e[1]$ zu R hinzu

$B := [e[1], e[1] + D[1], e[1] + w, e[1] + D[1] + w]$

 Setze $e := e \setminus B$

end while

Ausgabe R

Ergebnis:

Es befinden sich etwa 8000 Matrizen in jedem der 4–Spread-Mengen Töpfe. Aus diesen werden durch sukzessiven Aufbau 126 nicht-desarguesche Spread-Mengen erstellt von denen nach dem Äquivalenztest noch 5 nicht-isomorphe Spread-Mengen verbleiben.

Resultat:

Es handelt sich um die in Kapitel 5 beschriebenen Halbkörperebenen $\mathbb{T}_5, \mathbb{T}_6, \mathbb{T}_7, \mathbb{T}_8$ und \mathbb{T}_9 .

3. Symplektische Spread-Mengen

Ziel dieses Kapitels ist es zu zeigen, dass es bis auf Äquivalenz zwei nicht-desarguesche Translationsebenen gibt, deren Spread-Menge aus symmetrischen Matrizen besteht.

3.1. Theoretische Vorbereitung der Computersuche

Motivation:

Symplektische Faserungen (und Spread-Mengen) sind eng verwandt mit den von Kantor untersuchten orthogonalen Faserungen (und Spread-Mengen), daher unterziehen wir diesen Fall einer genaueren Betrachtung. Für Details siehe [KAN] oder [DEM, Kap. 12, S. 120-124].

Bemerkung 3.1.

Seien W ein Vektorraum über einem Körper K und $w, w' \in W$ sowie

$$\beta : W \times W \rightarrow K, \quad (w, w') \mapsto \beta(w, w')$$

eine Bilinearform. Zur Erinnerung: Eine Bilinearform heißt

- *nicht-entartet*, falls für alle $w \in W \setminus \{0\}$ ein $w' \in W$ existiert mit $\beta(w, w') \neq 0$
- *alternierend*, falls $\beta(w, w) = 0$ für alle $w \in W$
- *symmetrisch*, falls $\beta(w, w') = \beta(w', w)$ für alle $w, w' \in W$

Definition 3.2.

Seien W und β wie oben

1. β heißt **symplektische Form**, falls β eine nicht-entartete alternierende Bilinearform ist
2. W zusammen mit β ist ein **symplektischer Raum**
3. Eine Faserung \mathfrak{S} heißt **symplektisch**, falls für alle Fasern $X \in \mathfrak{S}$ gilt: X ist isotrop, das heißt $\beta(x, y) = 0$ für alle $x, y \in X$
4. Die Menge $Sp(W) = \{T \in GL(W) \mid \beta(wT, w'T) = \beta(w, w') \text{ mit } w, w' \in W\}$ ist eine Untergruppe von $GL(W)$ und heißt **symplektische Gruppe** auf W bezüglich β . Ist $K = GF(q)$ und $\dim(W) = 2m$, so schreibt man auch $Sp_{2m}(q)$ für $Sp(W)$.
5. Sei (W, β) ein symplektischer Raum. Ein Paar $\{w_1, w_2\} \subset W$ mit $\beta(w_1, w_2) = 1$ heißt ein **hyperbolisches Paar**. Vergleiche [HUP, Kap II, Def. 9.5, S. 217].
6. Ein zweidimensionaler symplektischer Raum, der von einem hyperbolischen Paar erzeugt wird heißt eine **hyperbolische Ebene**.
7. Seien W ein $2n$ -dimensionaler symplektischer Raum und β wie oben. Eine Menge $\{v_1, \dots, v_n, w_1, \dots, w_n\}$ heißt **symplektische Basis** von W , falls für alle $1 \leq i \leq n$ gilt $\beta(v_i, w_j) = \delta_{ij}$ und $H_i := \langle v_i, w_i \rangle$ eine hyperbolische Ebene ist.

3. Symplektische Spread-Mengen

Bemerkung 3.3.

- $Sp_4(2) \cong Sym(6)$, siehe [HUP, Kap. II, Satz 9.21, S. 227].
- Sei β eine alternierende Bilinearform über K . Ist $char(K) = 2$, so ist β offenbar auch symmetrisch, denn für $x, y \in W$ gilt:

$$\underbrace{\beta(x+y, x+y)}_{=0} = \underbrace{\beta(x, x)}_{=0} + \beta(x, y) + \beta(y, x) + \underbrace{\beta(y, y)}_{=0}$$

$$\implies \beta(x, y) = -\beta(y, x) \stackrel{char(K)=2}{=} \beta(y, x)$$

Lemma 3.4.

Sei \mathfrak{S} eine symplektische Faserung über dem symplektischen Raum W der Dimension $2m$, dann wird \mathfrak{S} bei geeigneter Koordinatisierung durch eine Spread-Menge symmetrischer $m \times m$ -Matrizen repräsentiert.

Beweis.

Seien $X, Y \in \mathfrak{S}$ zwei Fasern. Nach Voraussetzung sind alle Fasern isotrop. Es können Basen $B_X = \{v_1, \dots, v_m\}$ und $B_Y = \{w_1, \dots, w_m\}$ mit $\beta(v_i, w_j) = \delta_{ij}$ gewählt werden, denn:

Angenommen $0 \neq x \in X$, dann existiert ein $y \in Y$ mit $\beta(x, y) \neq 0$. Andernfalls ist $\beta(x, y) = 0$ für alle $y \in Y$ und damit $Y \oplus \langle x \rangle$ isotrop. Damit ist $X \perp \langle x \rangle \perp Y$ und folglich $\langle x \rangle \in Rad(\beta) = 0$. Ein Widerspruch.

Also existiert ein $y \in Y$ mit $\beta(x, y) \neq 0$ und o.B.d.A. (nach Skalarmultiplikation) sogar mit $\beta(x, y) = 1$.

Schreibe X und Y nun als $X = \langle x \rangle \oplus (X \cap \langle x, y \rangle^\perp)$, $Y = \langle y \rangle \oplus (Y \cap \langle x, y \rangle^\perp)$, mit $\dim(\langle x, y \rangle^\perp) = m - 1$. Induktion nach der Dimension auf $\langle x, y \rangle^\perp$ angewendet liefert schließlich die symplektische Basis $\{v_1, \dots, v_m, w_1, \dots, w_m\}$.

Identifiziere nun X mit $V(0)$ und Y mit $V(\infty)$. Setze $\mathfrak{S} = \{V(\infty)\} \cup \{V(T) \mid T \in \mathbf{S}\}$, dann ist

$$\beta((v_i, 0), (0, w_j)) = \delta_{ij} \implies \beta((0, w_j), (v_i, 0)) = -\delta_{ij}$$

Sei $T = (t_{ij})$ für alle $T \in \mathbf{S}$. Da $V(T)$ isotrop ist, folgt:

$$0 = \beta((v_k, w_k T), (v_l, w_l T)) = \beta\left((v_k, \sum_{i=1}^m t_{ki} w_i), (v_l, \sum_{j=1}^m t_{lj} w_j)\right)$$

$$= \underbrace{\beta((v_k, 0), (w_l, 0))}_{=0} + \underbrace{\beta\left((0, \sum_{i=1}^m t_{ki} w_i), (0, \sum_{j=1}^m t_{lj} w_j)\right)}_{=0} + \underbrace{\beta((v_k, 0), (0, \sum_{j=1}^m t_{lj} w_j))}_{=t_{lk}}$$

3.1. Theoretische Vorbereitung der Computersuche

$$+ \underbrace{\beta\left(\left(0, \sum_{i=1}^m t_{ki} w_i\right), (v_l, 0)\right)}_{=-t_{kl}} = t_{lk} - t_{kl}$$

Es ist also jede Matrix $T \in \mathbf{S}$ gleich ihrer Transponierten T^t und damit symmetrisch. \square

Lemma 3.5.

Sei V ein m -dimensionaler Vektorraum über $GF(2)$ mit nicht-entarteter symmetrischer Bilinearform β . Dann gilt eine der folgenden Aussagen:

1. Es ist $m = 2d$ und die Form ist symplektisch.
2. Es ist $m = 2d$ und $V = Z \oplus Z^\perp$, so dass Z symplektisch ist. Z^\perp hat die Dimension 2 und besitzt eine Orthonormalbasis.
3. Es ist $m = 2d + 1$ und $V = Z \oplus Z^\perp$, so dass Z symplektisch ist und Z^\perp die Dimension 1 hat.

Beweis.

Wir wissen nach [HUP, Kap II, Satz 9.6a, S. 217], dass eine Zerlegung $V = V_0 \oplus V_1$ existiert mit V_0 symplektisch und $V_0^\perp = V_1$ besitzt eine Orthonormalbasis $\{v_1, \dots, v_k\}$. Angenommen $k \geq 3$. Setze $u_1 = v_1 + v_2$, $u_2 = v_2 + v_3$. Dann gilt $\beta(u_i, u_i) = 0$ für $i = 1, 2$ und $\beta(u_1, u_2) = 1$. Setze $H = \langle u_1, u_2 \rangle$. Dann ist H eine hyperbolische Ebene. Setze $V'_0 = V_0 \oplus H$ und V'_1 sei das orthogonale Komplement von H in V_1 . Dann ist V'_0 symplektisch und $V'_1 = V'_0{}^\perp$.

Induktion liefert die Behauptung. \square

Bemerkung 3.6.

Sei V der 5-dimensionale Vektorraum über $GF(2)$. Bezeichne

$$J_0 = \begin{pmatrix} \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \end{pmatrix}, \quad J = \begin{pmatrix} 1 & \\ & J_0 \end{pmatrix}.$$

Offenbar ist J_0 die Gramsche Matrix einer symplektischen Form auf $V(4, 2)$. Daher gilt für die symplektische Gruppe auf $V(4, 2)$:

$$Sp_4(2) = \{N_0 \in GL(4, 2) \mid N_0^t J_0 N_0 = J_0\}.$$

Sei $C \in GL(5, 2)$ symmetrisch. Dann definiert C via $(x, y) = xCy^t$ eine symmetrische Bilinearform. Nach Lemma 3.5 existiert nun eine Matrix (genauer eine Basistransformationsmatrix) $N \in GL(5, 2)$ mit der Eigenschaft, dass $N^t C N = J$.

3. Symplektische Spread-Mengen

Des Weiteren können wir eine Untergruppe der $GL(5, 2)$ erzeugen, deren Elemente via der natürlichen Operation die Gram-Matrix J invariant lassen und die eingeschränkt auf $V(4, 2)$ isomorph zur symplektischen Gruppe $Sp_4(2)$, also der Isomorphiegruppe der zu J gehörigen Bilinearform β ist. $|Sp_4(2)| = |Q|$, wobei

$$Q := \left\langle \begin{pmatrix} 1 & . & . & . & . \\ . & 1 & 1 & . & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & . & . & . & . \\ . & 1 & . & . & . \\ . & 1 & 1 & . & . \\ . & . & . & 1 & 1 \\ . & . & . & . & 1 \end{pmatrix}, \begin{pmatrix} 1 & . & . & . & . \\ . & 1 & . & 1 & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ . & . & . & . & 1 \end{pmatrix}, \begin{pmatrix} 1 & . & . & . & . \\ . & 1 & . & . & . \\ . & . & 1 & . & . \\ . & 1 & . & 1 & . \\ . & . & . & . & 1 \end{pmatrix} \right\rangle$$

Definition 3.7.

Es seien J wie oben, \mathfrak{S} eine symplektische Faserung mit drei Fasern X, Y, Z , wobei die Basen von X und Y so gewählt sind, dass die folgenden beiden Aussagen zutreffen:

- Die assoziierte Spread-Menge \mathbf{S} besteht aus symmetrischen Matrizen
- Die Faser $V(0)$ repräsentiert X , die Faser $V(\infty)$ repräsentiert Y und $V(J)$ repräsentiert Z .

Dann nennen wir \mathbf{S} eine **normierte symmetrische Spread-Menge** bezüglich des Referenztripels (X, Y, Z) .

Bemerkung 3.8.

Eine normierte symmetrische Spread-Menge ist im Allgemeinen, aufgrund der vorhandenen Freiheit in den Basiswahlen (von X und Y), nicht eindeutig bestimmt.

Bemerkung 3.9.

(Umkoordinatisieren von normierten symmetrischen Spread-Mengen)

Sei \mathbf{S} eine normierte Spread-Menge der Faserung \mathfrak{S} über V bezüglich des Referenztripels (X, Y, Z) mit $X, Y, Z \in \mathfrak{S}$. Definiere weiterhin J wie oben, $N \in GL(5, 2)$ und

$$\delta_N = \begin{pmatrix} (N^t)^{-1} & 0 \\ 0 & N \end{pmatrix}, \quad \tau_J = \begin{pmatrix} \mathbb{1}_{5 \times 5} & J \\ 0 & \mathbb{1}_{5 \times 5} \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & \mathbb{1}_{5 \times 5} \\ \mathbb{1}_{5 \times 5} & 0 \end{pmatrix}$$

- Sei $V(T) = Z' \in \mathfrak{S} \setminus \{X, Y, Z\}$. Wähle $N \in GL(5, 2)$ so, dass $N^t T N = J$. Dann ist $X = X \delta_N$, $Y = Y \delta_N$ und $\mathbf{S}' = N^t \mathbf{S} N$ ist die normierte symmetrische Spread-Menge bezüglich (X, Y, Z') .

Bezeichne diese Operation mit $op_N : \mathbf{S} \mapsto N^t \mathbf{S} N$ (Vergleiche mit Definition 1.30).

- Aus der Rechnung $V(0)\tau_J = V(J)$, $V(J)\tau_J = V(0)$, $V(\infty)\tau_J = V(\infty)$ folgt, dass $\mathbf{S} + J$ eine normierte symmetrische Spread-Menge bezüglich des Referenztripels (Z, Y, X) ist.

Bezeichne diese Operation mit $op_1 : \mathbf{S} \mapsto \mathbf{S} + J$.

- c) Aus $V(0)\tau = V(\infty)$, $V(\infty)\tau = V(0)$, $V(T) = \{(vT^{-1}, v) \mid v \in V\}$ und $J = J^{-1}$ folgt, dass $\mathbf{S}^{-1} = \{T^{-1} \mid T \in \mathbf{S} \setminus 0\} \cup 0$ eine normierte symmetrische Spread-Menge bezüglich des Referenztripels (Y, X, Z) ist.
 Bezeichne diese Operation mit $op_2 : \mathbf{S} \mapsto \mathbf{S}^{-1}$.

Algorithmus 14 Koordinatisierung symplektischer Spread-Mengen, kurz $KOORD_{Sym}$

Eingabe: Normierte symmetrische Spread-Menge bezüglich $(\infty, 0, J)$, Koordinaten $a, b \in \{\infty, 0, J, \dots\}$

Ausgabe: Symmetrische Spread-Menge bezüglich (a, b, X) mit $(X) \in l_\infty$. Zum anschließenden normieren dieser Spread-Menge kann die Operation op_N verwendet werden, siehe Algorithmus 18.

if $a = \infty, b = 0$ **then**

$$\mathbf{S}' = \mathbf{S}, T = \mathbb{1}_{\dim(W)}$$

end if

if $a = 0, b = \infty$ **then**

$$\mathbf{S}' = \mathbf{S}^{-1}, T = \begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix}$$

end if

if $a = \infty, b > 0$ **then**

$$\mathbf{S}' = \mathbf{S} + \mathbf{S}[b], T = \begin{pmatrix} \mathbb{1} & \mathbf{S}[b] \\ 0 & \mathbb{1} \end{pmatrix}$$

end if

if $a > 0, b = 0$ **then**

$$\mathbf{S}' = (\mathbf{S}^{-1} + \mathbf{S}[a])^{-1}, T = \begin{pmatrix} \mathbb{1} & 0 \\ \mathbf{S}[a] & \mathbb{1} \end{pmatrix}$$

end if

if $a = 0, b > 0$ **then**

$$\mathbf{S}' = (\mathbf{S}^{-1} + \mathbf{S}[b])^{-1}, T = \begin{pmatrix} \mathbb{1} & 0 \\ \mathbf{S}[b] & \mathbb{1} \end{pmatrix}$$

end if

if $a > 0, b = \infty$ **then**

$$\mathbf{S}' = (\mathbf{S} + \mathbf{S}[a])^{-1}, T = \begin{pmatrix} \mathbf{S}[a] & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix}$$

end if

if $a > 0, b > 0$ **then**

$$\mathbf{S}' = ((\mathbf{S} + \mathbf{S}[b])^{-1} + \mathbf{S}[a])^{-1}, T = \begin{pmatrix} \mathbf{S}[b] \cdot \mathbf{S}[a] + \mathbb{1} & \mathbf{S}[b] \\ \mathbf{S}[a] & \mathbb{1} \end{pmatrix}$$

end if

Ebenso wie im Fall der Spread-Mengen nicht-symmetrischer Matrizen wollen wir im Folgenden einen Test vorstellen, der es uns erlaubt (partielle) symmetrische Spread-Mengen auf Äquivalenz zu untersuchen. Dazu konstruieren wir aus den Spread-Mengen jeweils einen Graphen, die wir dann auf Isomorphie untersuchen.

3. Symplektische Spread-Mengen

Definition 3.10.

Sei $t \in GL(V)$ eine symmetrische Matrix, dann heißt

- $a(t)$ die **Achse** von t , wobei $V \ni v \in a(t) \Leftrightarrow vtvt = 0$, also die Menge der isotropen Vektoren
- $c(t)$ das **Zentrum** von t , wobei $V \ni v \in c(t) \Leftrightarrow vtwt = 0$ mit $w \in a(t)$

Die Konstruktion des gerichteten Graphen zu einer gegebenen Spread-Menge erfolgt durch folgende Inzidenzvorschrift:

Definition 3.11.

Sei $\mathbf{S} = \{t_1, \dots, t_m\}$ eine partielle Spread-Menge symmetrischer Matrizen in $GL(5, 2)$. Dann sind

- $D = (d_{ij})$ die **Inzidenzmatrix**, wobei $d_{ij} = \begin{cases} 1, & c(t_j) \in a(t_i) \\ 0, & c(t_j) \notin a(t_i) \end{cases}$
- $S = (s_{ij})$ die **symmetrische Adjazenzmatrix**, wobei $s_{ij} = 1$ genau dann, wenn $d_{ij} = d_{ji} = 1$.
- Fasse S als Adjazenzmatrix eines Graphen mit der Eckenmenge $\{1, \dots, m\}$ auf. Der ij -te Eintrag der **Pfad-2-Matrix** $Q = (q_{ij}) = S^2$ gibt die Anzahl der (ungerichteten) Pfade der Länge 2 von i nach j an. Die Multimenge $\{q_{i1}, \dots, q_{im}\}$ ist der so genannte **Pfad-2-Typ** von t_i .

Lemma 3.12.

Seien $A \in GL(5, 2)$ und \mathbf{S} wie oben mit $ASA^t = \mathbf{S}$. Dann gilt:

1. Für $t \in \mathbf{S}$ ist $a(AtA^t) = a(t)A^{-1}$ und $c(AtA^t) = c(t)A^{-1}$
2. Für $t \in \mathbf{S}$ haben t und AtA^t den gleichen Pfad-2-Typ

Beweis.

Zu 1: Seien $v, w \in GF(2)^5$ dann ist:

$$v \in a(AtA^t) \Leftrightarrow vAtA^tv^t = 0 \Leftrightarrow vA \in a(t) \Leftrightarrow v \in a(t)A^{-1}$$

Außerdem folgt aus der Definition von Zentrum und Achse von t , dass $v(AtA^t)(zA^{-1})^t = (vA)tz^t = 0$ für alle $z \in a(t)$ und damit die Behauptung.

Zu 2: Sei (i, k, j) ein Pfad der Länge 2 von i nach j . Dann ist $c(t_i), c(t_j) \in a(t_k)$ und $c(t_k) \in a(t_i) \cap a(t_j)$. Seien $At_iA^t =: t_{i'}$, $At_jA^t =: t_{j'}$ und $At_kA^t =: t_{k'}$, dann folgt aus Teil 1:

$$c(t_{i'}) = c(t_i)A^{-1}, \quad c(t_{j'}) = c(t_j)A^{-1} \in a(t_k)A^{-1} = a(t_{k'})$$

Algorithmus 15 Achse und Zentrum von Matrizen, Normierung

Eingabe: Matrix $A \in GL(V)$

Ausgabe: $D := [T, a(A), c(A)]$, wobei T Transformationsmatrix mit $T^t A T = J$

Initialisierung: $a(A) := \emptyset, c(A) := \emptyset, T := 0$

for x in V **do**

 Teste, ob x isotrop, d.h. ob $(x \cdot A) \cdot x = 0$ und falls ja füge x zu $a(A)$ hinzu

end for

Setze $B := [a(A)[1], \emptyset, \emptyset, \emptyset]$ als die Basis der Achse

for j in $[1..Size(I)]$ **do**

 Teste, ob $(I[1] \cdot A) \cdot a(A)[j] = 1$ und falls ja setze $B[3] := a(A)[j]$

end for

Definiere die hyperbolische Ebene $H := \{v \in a(A) \mid (B[1] \cdot A) \cdot v = 0 \text{ und } (B[3] \cdot A) \cdot v = 0\}$ und setze $B[2] := H[1], B[4] := H[2]$.

$c := \{w \in GF(2)^5 \setminus a(A) \mid (B[k] \cdot A) \cdot v = 0 \text{ für } 1 \leq k \leq 4\}$ ist die Menge aller anisotropen Vektoren, die senkrecht auf den isotropen Vektoren der Basis stehen

$c(A) := c[1], T := \begin{pmatrix} c(A) \\ B \end{pmatrix}, D := [T, a(A), c(A)]$

Ausgabe D

ebenso wie die zweite Inklusion. Also ist $(i', k'j')$ ebenfalls ein Pfad der Länge 2 von i nach j . □

Definition 3.13.

Für $m \in \mathbb{N}^+$ setze $[m] = \{1, 2, \dots, m\}$. Eine Abbildung $p : [m] \rightarrow [m]$ heißt **Partition**.

Bemerkung 3.14.

Klar ist, dass $[m] = p^{-1}(1) \sqcup \dots \sqcup p^{-1}(m)$, das heißt $(p^{-1}(1), \dots, p^{-1}(m))$ ist eine Partition im üblichen Sinn. Konventionsweise sei $Im(p) = [k]$ für ein $k \leq m$.

Definition 3.15.

Sei $G = (V, E)$ ein Graph mit Kantenmenge E , Eckenmenge $V = [n]$ und $p : [n] \rightarrow [n]$ eine Partition. Des Weiteren sei $V(i) = p^{-1}(i)$. Für $v \in V$ definiere den i -ten **Relativgrad** d_i bezüglich p als $d_i(v) = |\{w \in V(i) \mid w \sim v\}|$. Setze $d(v) = (d_1(v), \dots, d_n(v))$.

Bemerkung 3.16. *Exkurs über naives Labelling* (vgl. [COR])

Es seien $p : [n] \rightarrow [n]$ eine Partition und $V(i) = p^{-1}(i)$. Ordne die Menge $\mathcal{L}(i) =$

3. Symplektische Spread-Mengen

$\{d(v) \mid v \in V(i)\}$ lexikographisch. Definiere eine Partition von $V(i) = V(i)_1 \sqcup \dots \sqcup V(i)_k$ gemäß der **Label-Menge** $\mathcal{L}(i)$ via

$$v, w \in V(i)_k \iff d(v) = d(w)$$

Resultat: Man erhält eine neue Partition $p' : [n] \rightarrow [n]$, die feiner ist als p , das heißt

$$p'(v) = p'(w) \implies p(v) = p(w)$$

Dieser Schritt wird nun mit p' anstelle von p so lange iteriert, bis eine stabile Partition auftritt das heißt $p' = p$ gilt.

Anwendung: Sei p eine Partition mit der Eigenschaft $p(v) = p(v^\alpha)$, für jedes $\alpha \in \text{Aut}(G)$, $v \in [n]$. Sei p' die Verfeinerung von p , dann gilt auch $p'(v) = p'(v^\alpha)$ für alle $\alpha \in \text{Aut}(G)$, $v \in [n]$. Ist nämlich $v \in p^{-1}(i)$, $w \in p^{-1}(j)$ und $v \sim w$, so ist $v^\alpha \in p^{-1}(i)$, $w^\alpha \in p^{-1}(j)$ und $v^\alpha \sim w^\alpha$.

Fazit: Seien p' die Partition, die aus p durch naives Labelling entsteht und $\alpha \in \text{Aut}(G)$, so gilt $p'(v^\alpha) = p'(v)$. Gilt insbesondere $p'^{-1}(i) = \{v\}$, so muss v Fixpunkt des Automorphismus sein. Mit anderen Worten das Labelling liefert Einschränkungen für die Gestalt möglicher Automorphismen. Mit offensichtlichen Anpassungen kann ein Labelling auch zur Konstruktion von Isomorphismen verwendet werden.

Algorithmus 16 Naives Labelling

Eingabe: Graph $G = (V, E)$, mit $|V| = n$

Ausgabe: Stabiles Labelling

Initialisierung: $p : V \rightarrow \{1\}$ und $d(v) = \text{Grad von } v \in V$

1) Definiere das Label von $v \in [n]$ als $l(v) = (p(v), d_1(v), \dots, d_k(v))$

2) Ordne die Menge $\mathcal{L} = \{l(v) \mid v \in [n]\}$ lexikographisch. Sei $|\mathcal{L}| = k'$

3) Definiere $p' : [n] \rightarrow [k']$ durch $p'(v) = i$, falls $l(v) = l_i$ für $\mathcal{L} = \{l_1, \dots, l_{k'}\}$

4) Iteriere die Schritte 1) bis 3) mit p' anstelle von p so lange bis $p' = p$

while $|(p')^{-1}(m)| > 1$ für ein $m \in [n]$ **do**

 Verfeinere $(p')^{-1}(m)$ künstlich durch ein ausgezeichnetes Element \hat{m} und sein Komplement

 Definiere das Label $l(w)$ von $w \in (p')^{-1}(m) \setminus \{\hat{m}\}$ und iteriere die Schritte 1) bis 4)

end while

Ausgabe p'

Bemerkung 3.17.

In Schritt 1) von Algorithmus 16 ist es wichtig, die Partition $p(v)$ in das Label zu integrieren, um sicherzugehen, dass es sich wirklich um eine Verfeinerung der Partition handelt und nicht um eine Neuordnung.

Die letzte Schleife stellt in offensichtlicher Weise sicher, dass es sich bei der Ausgabe p' um eine Permutation handelt.

3.2. Praktische Durchführung

1. Schritt: Erzeugen der symplektischen Gruppe

Erzeuge Q aus Bemerkung 3.6. Bezeichne mit Q_w den Stabilisator von $w \in V(5, 2)$.

2. Schritt: Einteilen der symmetrischen Matrizen in Töpfe

$$1. \text{ Bilde die Menge } R := \left\{ \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & v_1 & v_2 & v_3 & v_4 \\ \cdot & v_2 & v_5 & v_6 & v_7 \\ \cdot & v_3 & v_6 & v_8 & v_9 \\ \cdot & v_4 & v_7 & v_9 & v_{10} \end{pmatrix} \mid (v_1, \dots, v_{10}) \in V(10, 2) \right\}$$

2. Für alle $v \in V(5, 2) \setminus \{0\}$ setze $Pot(v) = \emptyset$ und erweitere die symmetrischen 5×5 -Matrizen aus R um die erste Zeile (beziehungsweise Spalte) mit den Einträgen von v und füge sie zu $Pot(v)$ hinzu, falls die Determinante $\neq 0$ ist.

Ergebnis: 30 Töpfe mit je 448 symmetrischen, invertierbaren Matrizen.

3. Schritt: Erstellen der Startermengen der Größe 3

Nach Definition 3.7 ist J in jeder normierten symmetrischen Spread-Menge enthalten, daher bildet J eine Startermenge der Größe 1.

Wir reduzieren alle Töpfe über den Spread-Mengen-Test aus Algorithmus 2 und erhalten in jedem der 30 Töpfe 192 symmetrische Matrizen.

Für einen beliebigen Topf, in unserem Falle $Pot(v_1)$ mit $v_1 = (0, 0, 0, 0, 1)$ bilde Q_{v_1} und finde eine Überdeckung von $Pot(v_1)$ mit Bahnen der Form $\{Q_{v_1}[i]^t \cdot P_j \cdot Q_{v_1}[i] \mid 1 \leq i \leq Size(Q_{v_1})\}$ wobei $P_j \in Pot(v_1)$, da J unter dieser Operation invariant gelassen wird.

Rechnung zeigt: Es gibt vier solcher P_j und damit vier Startermengen der Größe 2 der Form $\{J, P_j\}$ wobei $1 \leq j \leq 4$.

Es folgt eine erneute Reduktion der Töpfe nach jeder dieser 2-Startermengen. Dies führt zu einer Mächtigkeit von 80 Matrizen pro Topf. Die Matrizen eines weiteren beliebigen Topfes etwa $Pot(v_2)$ mit $v_2 = (0, 0, 0, 1, 0)$ werden mit den vier 2-Startermengen zu Startermengen der Größe 3 verbunden.

Resultat: 320 Startermengen der Größe 3.

4. Schritt: Ergänzung der 3-Startermengen zu Spread-Mengen

Definition 3.18.

Sei $G = (V, E)$ ein Graph, C eine Teilmenge der Knotenmenge V .

- a) Man nennt C eine **Clique** von G , falls für alle Knotenpaare $c_1, c_2 \in C$ eine Kante in G existiert, die c_1 mit c_2 verbindet

3. Symplektische Spread-Mengen

- b) Sei $r \geq 2$. Dann heißt G **r-partit**, falls eine Partition von V in r Teile existiert, so dass die Endknoten jeder Kante von G in verschiedenen Partitionsklassen liegen, vergleiche [DIE, Kap. 0.6, S.15]. Ist r nicht bekannt oder redundant, so sprechen wir von einem **multipartiten Graphen**.

Zum Erstellen sämtlicher m -Cliques eines Graphen, dessen Teile unsere oben konstruierten Töpfe sind, wenden wir Algorithmus 17 an. Dabei wird eine Zeiger z uns anzeigen, an welchem Ort des Graphen wir suchen und ein Level l gibt an, in welchem Iterationsschritt wir uns befinden.

Es ist leicht einzusehen, dass der Algorithmus das gewünschte Ergebnis liefert. Dies sind in unserem Fall 4652 Spread-Mengen, von denen zwei desarguesch sind.

Algorithmus 17 Erstellen von m -Cliques, kurz *MPG*

Eingabe: m -partiter Graph G und dessen Adjazenzmatrix A **Ausgabe:** Sämtliche m -Cliques

Initialisierung: $M := [[\text{Size}(\text{Pot}(1)), \dots, \text{Size}(\text{Pot}(m))], \overbrace{[0, \dots, 0], \dots, [0, \dots, 0]}^{m-1}]$, die Größe der Töpfe in jedem Level, $N := [[\text{Pot}(1), \dots, \text{Pot}(m)], [\emptyset, \dots, \emptyset], \dots, [\emptyset, \dots, \emptyset]]$, die Cliques in jedem Level, $z := [1, \dots, 1]$, Level $l := 1$, $f := \text{false}$, $w := \text{true}$, $C := \emptyset$.

while $f = \text{false}$ **do** $j := l + 1$ **while** $j \leq m$ und $w = \text{true}$ **do** **for** k in $[1..M[l][j]]$ **do** **if** $A[N[l][l][z[l]]][N[l][j][k]] = 1$ **then** Füge $N[l][j][k]$ zu $N[l+1][j]$ hinzu. **end if** **end for** Setze $M[l+1][j] := \text{Size}(N[l+1][j])$ und $w := M[l+1][j] > 0$ $j := j + 1$ **end while****if** $w = \text{true}$ **then** **if** $l = m - 1$ **then** $c := \emptyset$ **for** i in $[1..m - 1]$ **do** Füge $N[i][i][z[i]]$ zu c hinzu. **end for** **for** i in $[1..M[m][m]]$ **do** Füge $c \cup N[m][m][i]$ zu C hinzu. **end for** **else if** $l < m - 1$ **then** $l := l + 1$ **end if****else if** $w = \text{false}$ **then** Setze $z[l] := z[l] + 1$ und $z[x] := 1$ für alle $l + 1 \leq x \leq m$. **while** $z[l] > M[l][l]$ und $l > 1$ **do** Setze $z[l] := 1$, $l := l - 1$ und $z[l] := z[l] + 1$. **end while** **if** $l = 1$ und $z[1] > M[1][1]$ **then** $f := \text{true}$ **else if** $l > 1$ oder $z[1] \leq M[1][1]$ **then** $w := \text{true}$ **end if** **end if****end while**Ausgabe C

3. Symplektische Spread-Mengen

5. Schritt: Test auf Äquivalenz

Algorithmus 18 Äquivalenz von symmetrischen Spread-Mengen, kurz $EQUIV_{Sym}$

Eingabe: Zwei symmetrische Spread-Mengen \mathbf{S} und \mathbf{S}' , Gruppe Q

Ausgabe: „true“ falls \mathbf{S} äquivalent zu \mathbf{S}' , „false“ falls nicht.

0) *Initialisierung:* $w := \text{false}$

for i in $[1..\text{Size}(\mathbf{S})]$ **do**

 Normiere $\mathbf{S}[i]$ mit Algorithmus 15 und erhalte die Achse $a(t_i)$ und das Zentrum $c(t_i)$

end for

1) Bilde die Inzidenzmatrix, sowie die dazugehörige symmetrische Adjazenzmatrix und damit den Pfad-2-Typ aller $t_i \in \mathbf{S}$

Bestimme auf dieselbe Weise den Pfad-2-Typ aller $t'_i \in \mathbf{S}'$ (siehe Definition 3.11)

if Die Größe beider Pfad-2-Typen stimmt überein **then**

 2) Führe für die Graphen G und G' , definiert durch die Inzidenzmatrizen, das naive Labelling aus Algorithmus 16 durch und erhalte zwei Permutationen P und P'

 3) Finde m, m' mit $P[m] = 1$ und $P'[m'] = 1$ sowie N, N' aus Schritt 0) mit $N \cdot \mathbf{S}[m] \cdot N^t = J = N' \cdot \mathbf{S}'[m'] \cdot (N')^t$. Setze $\mathbf{S} := N \cdot \mathbf{S} \cdot N^t$ sowie $\mathbf{S}' := N' \cdot \mathbf{S}' \cdot (N')^t$

 4) Finde n und n' mit $P[n] = 2$ und $P'[n'] = 2$

if $\mathbf{S}[n][1][1] = \mathbf{S}'[n'][1][1] := a$ **then**

 5) Finde zwei Matrizen $R, R' \in Q$ mit $\mathbf{S}[n][1] \cdot R = (a, 0, 0, 0, 1) = \mathbf{S}'[n'][1] \cdot R'$ und setze $\mathbf{S} := R \cdot \mathbf{S} \cdot R^t$ und $\mathbf{S}' := R' \cdot \mathbf{S}' \cdot (R')^t$

 Setze $k := 1$, $Q_v := Q_{a,0,0,0,1}$

while $k \leq \text{Size}(Q_v)$ und $w = \text{false}$ **do**

 6) $\mathbf{S}'' = (Q_v[k])^t \cdot \mathbf{S} \cdot Q_v[k]$

$w := \mathbf{S}'' = \mathbf{S}'$

end while

end if

end if

Ausgabe w

Lemma 3.19.

Lautet die Ausgabe von Algorithmus 18 „true“, so sind die beiden Ebenen äquivalent.

Beweis.

In Schritt 1) werden wie oben beschrieben die durch die Spread-Mengen \mathbf{S} und \mathbf{S}' induzierten Graphen erstellt. Das Problem der Äquivalenz der Spread-Mengen wird also auf das Problem der Isomorphie zweier Graphen reduziert. Notwendigerweise muss bei zwei isomorphen Graphen die Größe der Pfad-2-Typen übereinstimmen, siehe [COR, Kap. 4].

Wir haben schon gezeigt, dass bei Durchführung eines naiven Labellings eine Permutation wie in Schritt 2) gefordert zustande kommt.

Da die Spread-Mengen durch die vorangegangene Koordinatisierung noch nicht notwendigerweise normiert sind, wird in Schritt 3) o.B.d.A. nach der Transformation, welche

die 1 in der Permutation repräsentiert, normiert.

Wir wissen, dass für alle $x \in Q_v$ gilt: $x \cdot J \cdot x^t = J$. Seien

$$T := \begin{pmatrix} a & b \\ c & D \end{pmatrix}, T' := \begin{pmatrix} a' & b' \\ c' & D' \end{pmatrix}$$

zwei Matrizen der normierten Spread-Mengen \mathbf{S} und \mathbf{S}' , die in den Permutationen durch die 2 repräsentiert werden. Ein Element in Q_v hat die Form:

$$x = \begin{pmatrix} 1 & \\ & X \end{pmatrix}, X \in GL(4, 2)$$

Damit \mathbf{S} in \mathbf{S}' überführt werden kann, muss für T und T' gelten:

$$x \cdot T \cdot x^t = \begin{pmatrix} 1 & \\ & X \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & D \end{pmatrix} \cdot \begin{pmatrix} 1 & \\ & X^t \end{pmatrix} = \begin{pmatrix} a & bX \\ Xc & XDX^t \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} a' & b' \\ c' & D' \end{pmatrix} = T'$$

Es muss also $a = a'$ und $bX = b'$ gelten. Daher werden in Schritt 5) die beiden Spread-Mengen auf diese zweite Bedingung normiert.

In Schritt 6) werden schließlich sämtliche Transformationen mit Elementen aus Q_v von \mathbf{S} in \mathbf{S}' getestet. \square

Bemerkung 3.20.

Wir haben *nicht* gezeigt, dass durch den Algorithmus 18 alle Äquivalenzen gefunden werden können, da nicht gesichert ist, dass das naive Labelling aufgrund der künstlichen Verfeinerung eindeutig ist. Da sich jedoch alle Ebenen unter den schwachen Voraussetzungen auf zwei reduzieren, ist dies auch nicht nötig.

Die Prozedur *AUTOM* zeigt, dass es sich dabei wirklich um zwei nicht-isomorphe Spread-Mengen handelt.

Resultat:

Es handelt sich um die in Kapitel 5 beschriebenen Ebenen \mathbb{T}_4 und \mathbb{T}_7 .

4. Identifikation der Ebenen

4.1. Kollineationen der Ordnung 31

Die zwei nicht-desargueschen Translationsebenen \mathbb{T}_2 und \mathbb{T}_3 der Ordnung 32, die einen Automorphismus der Ordnung 31 zulassen gehen aus Transposition der Spread-Mengen auseinander hervor. Nach [POL, Satz 3.2, S. 5] existieren genau zwei Translationsebenen, die einen Automorphismus der Ordnung 31 zulassen. Demzufolge handelt sich bei unseren Ebenen um eben diese beiden.

4.2. Kollineationen der Ordnung 11

Bei der nicht-desargueschen Translationsebene \mathbb{T}_4 der Ordnung 32, die einen Automorphismus der Ordnung 11 zulässt, handelt es sich um die von Prince [PRI, Kap. 4, Beweis zu Satz 4.1] beschriebene Fahnen-transitive Translationsebene. Es ist zu bemerken, dass diese Ebene isomorph zu der aus Transposition der Spread-Mengen hervorgehenden Ebene ist.

4.3. Kollineationen der Ordnung 5

Zwei der sechs Translationsebenen der Ordnung 32, die einen Automorphismus der Ordnung 5 zulassen, lassen zusätzlich einen Automorphismus der Ordnung 31 zu, es handelt sich also um \mathbb{T}_2 und \mathbb{T}_3 .

Eine der Ebenen lässt zusätzlich einen Automorphismus der Ordnung 11 zu, ist also isomorph zu \mathbb{T}_4 .

Bei den übrigen drei Translationsebenen $\mathbb{T}_5, \mathbb{T}_6$ und \mathbb{T}_7 erzeugen die Spread-Mengen bei geeigneter Koordinatisierung einen Vektorraum der Dimension 5, sind also nach Bemerkung 1.43 Halbkörper-Ebenen. Sämtliche Halbkörper mit 32 Elementen wurden von Walker in [WAL] aufgelistet. Somit gehen unsere Ebenen aus den Halbkörpern *III*, *IV* und *VI* hervor, vergleiche [WAL, Abschnitt 3, S. 85]. Des Weiteren sind die Spread-Mengen aller Halbkörper-Ebenen in [SEM] aufgelistet.

4.4. Kollineationsgruppe der Ordnung 4

Bei allen Translationsebenen der Ordnung 32 mit einer Kollineationsgruppe der Ordnung 4 erzeugen die Spread-Mengen einen Vektorraum der Dimension 5, es handelt sich also um Halbkörper-Ebenen. Da drei der fünf Ebenen einen Automorphismus der Ordnung 5 zulassen, wurden sie oben schon beschrieben.

Folglich sind die übrigen zwei von uns gefundenen Translationsebenen \mathbb{T}_8 und \mathbb{T}_9 äquivalent zu den aus den Halbkörpern *I* und *II* von Walker hervorgehenden Ebenen.

4.5. Symplektische Spread-Mengen

Die beiden Translationsebenen der Ordnung 32, die aus einer symplektischen Spread-Menge hervorgeht, können mit Hilfe der Prozeduren *AUT* und *EQUIV* identifiziert werden mit der Fahnen-transitiven Ebene \mathbb{T}_4 von Prince und der Halbkörperenebene \mathbb{T}_7 .

5. Die neun Translationsebenen der Ordnung 32

In diesem Kapitel bezeichne \mathbf{G} das Translationskomplement der Ebenen und B_m die Begleitmatrix der Ordnung m . Wir geben zusammenfassend für jede Ebene an:

1. Die Ordnung der Automorphismengruppe
2. Erzeuger des Translationskomplementes bei geeigneter Koordinatisierung
3. Die formale Spread-Menge als Vereinigung von Bahnen
4. Konkrete Repräsentanten der einzelnen Bahnen

Die desarguesche Ebene \mathbb{T}_1

1. $|\text{Aut}(\mathbb{T}_1)| = |PGL(3, 32)|$
2. $\mathbf{G}(\mathbb{T}_1) = \left\langle \left(\begin{array}{cc} B_{31} & \\ & \mathbb{1} \end{array} \right), \left(\begin{array}{cc} \mathbb{1} & \\ & \mathbb{1} \end{array} \right), \left(\begin{array}{cc} & \mathbb{1} \\ \mathbb{1} & \end{array} \right), \left(\begin{array}{cc} N & \\ & N \end{array} \right) \right\rangle \cong GL(2, 32),$
wobei $N \in N_{GL(5,2)}(B_{31}) \setminus \langle B_{31} \rangle$
3. $\mathbf{S}(\mathbb{T}_1) = \{B_{31}^i \mid 0 \leq i \leq 30\}$

Die Ebenen $\mathbb{T}_2, \mathbb{T}_3$ mit Automorphismus der Ordnung 31 [POL]

1. $|\text{Aut}(\mathbb{T}_2)| = |\text{Aut}(\mathbb{T}_3)| = 155$
2. $\mathbf{G}(\mathbb{T}_2) = \left\langle \left(\begin{array}{cc} B_{31} & \\ & B_{31}^{14} \end{array} \right), \left(\begin{array}{cc} C & \\ & D \end{array} \right) \right\rangle, \quad \mathbf{G}(\mathbb{T}_3) = \left\langle \left(\begin{array}{cc} B_{31} & \\ & B_{31}^5 \end{array} \right), \left(\begin{array}{cc} C & \\ & E \end{array} \right) \right\rangle$ mit

$$C = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & 1 & \cdot \\ 1 & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & 1 \\ \cdot & 1 & \cdot & 1 & \cdot \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & 1 & \cdot \end{pmatrix}, \quad E = \begin{pmatrix} \cdot & 1 & 1 & \cdot & 1 \\ \cdot & \cdot & 1 & 1 & 1 \\ 1 & \cdot & \cdot & 1 & \cdot \\ 1 & \cdot & 1 & 1 & 1 \\ \cdot & 1 & \cdot & \cdot & 1 \end{pmatrix}$$

3. $\mathbf{S}(\mathbb{T}_2) = \{B_{31}^{-i} S B_{31}^{5i} \mid 0 \leq i \leq 30\}, \quad \mathbf{S}(\mathbb{T}_3) = \{B_{31}^{-i} T B_{31}^{14i} \mid 0 \leq i \leq 30\}$

4. $S = \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & 1 \\ \cdot & 1 & \cdot & 1 & \cdot \\ \cdot & 1 & 1 & \cdot & \cdot \end{pmatrix}, \quad T = \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & 1 \end{pmatrix}$

Die Fahnen-transitive Ebene \mathbb{T}_4 [PRI]

1. $|\text{Aut}(\mathbb{T}_4)| = 165$

$$2. \mathbf{G}(\mathbb{T}_4) = \left\langle A, \begin{pmatrix} B_5 & \\ & B_5 \end{pmatrix} \right\rangle, \text{ wobei } A := \begin{pmatrix} 1 & 1 & 1 & . & . & . & . & 1 & . & . \\ . & 1 & 1 & 1 & . & . & . & . & . & 1 \\ . & 1 & . & 1 & 1 & . & . & 1 & 1 & . \\ 1 & . & . & . & 1 & 1 & . & 1 & . & . \\ 1 & . & . & 1 & 1 & . & 1 & 1 & 1 & 1 \\ . & . & 1 & . & . & 1 & 1 & . & . & . \\ . & . & . & . & 1 & . & 1 & 1 & 1 & 1 \\ . & . & 1 & 1 & . & . & 1 & 1 & . & 1 \\ 1 & . & 1 & . & . & . & . & 1 & . & 1 \\ . & 1 & 1 & 1 & 1 & 1 & 1 & 1 & . & . \end{pmatrix}$$

$$3. \mathbf{S}(\mathbb{T}_5) = \mathbb{1} \cup \bigcup_{i=1}^6 \{B_5^{-j} T_i B_5^j \mid 1 \leq j \leq 5\}$$

$$4. T_i \in \left\{ \begin{pmatrix} . & . & . & . & 1 \\ 1 & . & . & 1 & . \\ 1 & 1 & . & 1 & 1 \\ . & . & . & 1 & 1 \\ . & . & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} . & . & . & 1 & 1 \\ . & . & 1 & 1 & 1 \\ 1 & . & 1 & . & 1 \\ . & 1 & . & . & . \\ . & 1 & 1 & . & 1 \end{pmatrix}, \begin{pmatrix} . & . & 1 & . & 1 \\ 1 & . & . & . & 1 \\ 1 & . & . & 1 & . \\ . & 1 & 1 & . & . \\ 1 & . & . & . & . \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & . & . & . & 1 \\ 1 & . & . & 1 & 1 \\ 1 & 1 & 1 & . & 1 \\ . & . & 1 & 1 & 1 \\ . & 1 & . & . & . \end{pmatrix}, \begin{pmatrix} 1 & . & . & 1 & 1 \\ . & . & 1 & . & 1 \\ 1 & 1 & . & . & 1 \\ . & 1 & . & 1 & 1 \\ . & 1 & . & . & 1 \end{pmatrix}, \begin{pmatrix} 1 & . & 1 & . & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & . & 1 & . \\ . & . & . & . & 1 \\ 1 & . & 1 & 1 & 1 \end{pmatrix} \right\}$$

Die Halbkörpererebenen $\mathbb{T}_5, \mathbb{T}_6, \mathbb{T}_7$ mit Automorphismus der Ordnung 5 [WAL]

$$1. |\text{Aut}(\mathbb{T}_5)| = |\text{Aut}(\mathbb{T}_6)| = |\text{Aut}(\mathbb{T}_7)| = 160$$

$$2. \mathbf{G}(\mathbb{T}_i) = \left\langle \begin{pmatrix} B_5 & \\ & B_5 \end{pmatrix}, \begin{pmatrix} B_5 & D_i \\ & B_5 \end{pmatrix} \right\rangle, \quad i = \{5, 6, 7\} \text{ und } \mathbb{1} \neq D_i \in \mathbf{S}(\mathbb{T}_i).$$

$$3. \mathbf{S}(\mathbb{T}_5) = \mathbb{1} \cup \bigcup_{i=1}^6 \{B_5^{-j} R_i B_5^j \mid 1 \leq j \leq 5\}, \quad \mathbb{T}_6, \mathbf{S}(\mathbb{T}_6) = \mathbb{1} \cup \bigcup_{i=1}^6 \{B_5^{-j} S_i B_5^j \mid 1 \leq j \leq 5\},$$

$$\mathbf{S}(\mathbb{T}_7) = \mathbb{1} \cup \bigcup_{i=1}^6 \{B_5^{-j} T_i B_5^j \mid 1 \leq j \leq 5\}$$

$$4. R_i \in \left\{ \begin{pmatrix} . & . & . & . & 1 \\ 1 & . & 1 & 1 & 1 \\ 1 & 1 & . & . & . \\ 1 & . & 1 & . & 1 \\ . & 1 & . & . & . \end{pmatrix}, \begin{pmatrix} . & . & . & 1 & 1 \\ . & 1 & 1 & . & 1 \\ . & . & 1 & . & 1 \\ 1 & 1 & . & 1 & . \\ 1 & 1 & . & 1 & . \end{pmatrix}, \begin{pmatrix} . & . & 1 & . & 1 \\ . & . & . & . & 1 \\ 1 & . & 1 & 1 & 1 \\ . & 1 & . & 1 & . \\ 1 & . & . & . & . \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 1 & . & . & . & 1 \\ 1 & 1 & . & . & . \\ 1 & 1 & . & . & 1 \\ 1 & . & 1 & 1 & 1 \\ . & . & . & 1 & . \end{pmatrix}, \begin{pmatrix} 1 & . & . & 1 & 1 \\ . & . & . & 1 & 1 \\ . & 1 & 1 & . & 1 \\ 1 & . & . & . & 1 \\ 1 & . & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & . & 1 & . & 1 \\ . & 1 & 1 & 1 & . \\ 1 & . & 1 & 1 & . \\ . & . & 1 & 1 & . \\ 1 & 1 & . & . & 1 \end{pmatrix} \right\}$$

5. Die neun Translationsebenen der Ordnung 32

$$\begin{aligned}
 S_i \in & \left\{ \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & 1 & 1 & \cdot & \cdot \\ 1 & 1 & 1 & 1 & \cdot \\ \cdot & 1 & 1 & \cdot & 1 \\ \cdot & \cdot & 1 & 1 & \cdot \end{pmatrix}, \begin{pmatrix} \cdot & \cdot & \cdot & 1 & 1 \\ \cdot & 1 & 1 & 1 & 1 \\ 1 & 1 & \cdot & 1 & 1 \\ \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & 1 & 1 \end{pmatrix}, \begin{pmatrix} \cdot & \cdot & 1 & \cdot & 1 \\ 1 & \cdot & 1 & 1 & \cdot \\ 1 & 1 & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot \end{pmatrix}, \right. \\
 & \left. \begin{pmatrix} 1 & \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & 1 & \cdot & \cdot \\ 1 & 1 & \cdot & 1 & \cdot \\ \cdot & 1 & 1 & 1 & 1 \\ \cdot & \cdot & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \cdot & \cdot & 1 & 1 \\ \cdot & \cdot & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ \cdot & \cdot & \cdot & 1 & 1 \\ \cdot & 1 & \cdot & 1 & \cdot \end{pmatrix}, \begin{pmatrix} 1 & \cdot & 1 & \cdot & 1 \\ 1 & 1 & 1 & 1 & \cdot \\ 1 & 1 & 1 & \cdot & 1 \\ \cdot & 1 & \cdot & 1 & \cdot \\ 1 & 1 & \cdot & \cdot & 1 \end{pmatrix} \right\} \\
 T_i \in & \left\{ \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & 1 & 1 & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 \\ 1 & 1 & 1 & \cdot & 1 \end{pmatrix}, \begin{pmatrix} \cdot & \cdot & \cdot & 1 & 1 \\ 1 & \cdot & 1 & 1 & 1 \\ \cdot & 1 & 1 & 1 & \cdot \\ \cdot & 1 & \cdot & 1 & 1 \\ \cdot & 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} \cdot & \cdot & 1 & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & 1 & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot \end{pmatrix}, \right. \\
 & \left. \begin{pmatrix} 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & 1 & \cdot \\ 1 & 1 & \cdot & \cdot & 1 \\ 1 & \cdot & 1 & 1 & 1 \\ \cdot & \cdot & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \cdot & \cdot & 1 & 1 \\ 1 & 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & 1 & \cdot \\ 1 & 1 & 1 & \cdot & 1 \\ \cdot & 1 & \cdot & \cdot & \cdot \end{pmatrix}, \begin{pmatrix} 1 & \cdot & 1 & \cdot & 1 \\ \cdot & 1 & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & \cdot & 1 & \cdot & \cdot \end{pmatrix} \right\}
 \end{aligned}$$

Die übrigen Halbkörpererebenen $\mathbb{T}_8, \mathbb{T}_9$ [WAL]

1. $|\text{Aut}(\mathbb{T}_8)| = |\text{Aut}(\mathbb{T}_9)| = 32$
2. $\mathbf{G}(\mathbb{T}_i) = \left\langle \begin{pmatrix} \mathbb{1} & \\ & \mathbb{1} \end{pmatrix}, \begin{pmatrix} \mathbb{1} & D_i \\ & \mathbb{1} \end{pmatrix} \right\rangle, \quad i = \{8, 9\} \text{ und } \mathbb{1} \neq D_i \in \mathbf{S}(\mathbb{T}_i)$
3. $\mathbf{S}(\mathbb{T}_8) = \bigcup_{i=1}^8 \{S_i, S_i + \mathbb{1}, S_i + B_{31}, S_i + B_{31} + \mathbb{1}\},$
 $\mathbf{S}(\mathbb{T}_9) = \bigcup_{i=1}^8 \{T_i, T_i + \mathbb{1}, T_i + B_{31}, T_i + B_{31} + \mathbb{1}\}$

$$\begin{aligned}
 4. S_i \in & \left\{ \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & 1 & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ 1 & 1 & 1 & \cdot & \cdot \end{pmatrix}, \begin{pmatrix} \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 & 1 \\ 1 & 1 & 1 & \cdot & 1 \\ 1 & 1 & 1 & \cdot & 1 \\ 1 & \cdot & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} \cdot & \cdot & \cdot & 1 & 1 \\ \cdot & \cdot & 1 & \cdot & 1 \\ 1 & 1 & 1 & 1 & \cdot \\ 1 & 1 & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & 1 & 1 \end{pmatrix}, \begin{pmatrix} \cdot & \cdot & 1 & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & 1 & \cdot \\ 1 & 1 & \cdot & 1 & \cdot \end{pmatrix}, \right. \\
 & \left. \begin{pmatrix} \cdot & \cdot & 1 & \cdot & 1 \\ 1 & 1 & 1 & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & 1 & 1 & 1 & \cdot \\ \cdot & \cdot & 1 & 1 & \cdot \end{pmatrix}, \begin{pmatrix} \cdot & \cdot & 1 & 1 & \cdot \\ 1 & 1 & \cdot & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & \cdot & 1 & 1 & 1 \\ \cdot & 1 & 1 & \cdot & 1 \end{pmatrix}, \begin{pmatrix} \cdot & \cdot & 1 & 1 & 1 \\ 1 & \cdot & 1 & 1 & 1 \\ \cdot & 1 & 1 & 1 & 1 \\ 1 & \cdot & \cdot & 1 & 1 \\ 1 & \cdot & \cdot & \cdot & 1 \end{pmatrix}, B_{31} \right\}
 \end{aligned}$$

$$T_i \in \left\{ \begin{array}{l} \left(\begin{array}{cccccc} \cdot & \cdot & \cdot & \cdot & 1 & \\ \cdot & \cdot & \cdot & 1 & \cdot & \\ 1 & \cdot & \cdot & \cdot & \cdot & \\ 1 & 1 & 1 & \cdot & 1 & \\ 1 & 1 & \cdot & \cdot & \cdot & \end{array} \right), \left(\begin{array}{cccccc} \cdot & \cdot & \cdot & 1 & \cdot & \\ \cdot & 1 & 1 & 1 & 1 & \\ \cdot & 1 & \cdot & 1 & 1 & \\ 1 & \cdot & \cdot & 1 & \cdot & \\ 1 & \cdot & \cdot & \cdot & \cdot & \end{array} \right), \left(\begin{array}{cccccc} \cdot & \cdot & \cdot & 1 & 1 & \\ \cdot & 1 & 1 & \cdot & 1 & \\ 1 & 1 & \cdot & 1 & 1 & \\ \cdot & 1 & 1 & 1 & 1 & \\ 1 & \cdot & \cdot & \cdot & \cdot & \end{array} \right), \left(\begin{array}{cccccc} \cdot & \cdot & 1 & \cdot & \cdot & \\ 1 & 1 & \cdot & \cdot & \cdot & \\ 1 & \cdot & \cdot & \cdot & 1 & \\ 1 & 1 & \cdot & 1 & 1 & \\ 1 & \cdot & \cdot & 1 & 1 & \end{array} \right), \\ \left. \begin{array}{l} \left(\begin{array}{cccccc} \cdot & \cdot & 1 & \cdot & 1 & \\ 1 & 1 & \cdot & 1 & \cdot & \\ \cdot & \cdot & \cdot & \cdot & 1 & \\ \cdot & \cdot & 1 & 1 & \cdot & \\ \cdot & 1 & \cdot & 1 & 1 & \end{array} \right), \left(\begin{array}{cccccc} \cdot & \cdot & 1 & 1 & \cdot & \\ 1 & \cdot & 1 & 1 & 1 & \\ 1 & 1 & \cdot & 1 & \cdot & \\ \cdot & 1 & \cdot & \cdot & 1 & \\ 1 & 1 & \cdot & 1 & 1 & \end{array} \right), \left(\begin{array}{cccccc} \cdot & \cdot & 1 & 1 & 1 & \\ 1 & \cdot & 1 & \cdot & 1 & \\ 1 & \cdot & 1 & \cdot & \cdot & \\ 1 & \cdot & 1 & \cdot & \cdot & \\ \cdot & \cdot & \cdot & 1 & 1 & \end{array} \right), B_{31} \end{array} \right\}$$

6. Fraktional-Dimensionale Unterebenen

Definition 6.1.

Sei $\mathbb{T}(\mathfrak{S})$ eine Translationsebene bezüglich der Faserung \mathfrak{S} über $W = V(2n, p)$ mit p prim und sei $U = V(2k, p)$ eine Unterebene von $\mathbb{T}(\mathfrak{S})$. Dann existieren Fasern $X_0, \dots, X_{p^{k+1}}$, sodass $\mathfrak{S}_U := \{X_0 \cap U, \dots, X_{p^{k+1}} \cap U\}$ eine Faserung von U ist. Man nennt $\frac{n}{k}$ die **fraktionale Dimension** der Ebene im Bezug auf U .

Bemerkung 6.2.

- In [DIM, Abschnitt 1, S. 463] werden solche Fälle untersucht, in denen $k \nmid n$, die fraktionale Dimension der Ebene also nicht ganzzahlig ist. Uns interessieren also solche $1 \leq k \leq n = 5$, mit $k \nmid n$ und $U = V(2k, 2)$ ist eine Unterebene. Mit dem Satz von Baer folgt in diesem Fall $k = 2$.
- Im Falle der Desargueschen Ebene ist bekannt, dass es keine Unterebenen der Ordnung 2^2 gibt, siehe [DIM, Abschnitt 1, S. 463].

Beobachtung:

Seien \mathfrak{S} eine Faserung über W und U eine vierdimensionale Unterebene von $\mathbb{T}(\mathfrak{S})$. Bezeichne die Faserung von U mit

$$\mathfrak{S}_U := \{X \cap U \mid X \in \mathfrak{S}\}.$$

Koordinatisiere so, dass $V(\infty), V(0) \in \mathfrak{S}_U$. Des Weiteren sei $V(T) \in \mathfrak{S}_U$. Bezeichne mit $U(T) := U \cap V(T)$ den U -Anteil der Faser $V(T)$. Klar ist, dass

$$(u, uT) \in U(T) \subset U(0) \oplus U(\infty) \implies u \in U(0), uT \in U(\infty),$$

wobei $V(0)$ und $V(\infty)$ jeweils mit dem Vektorraum V identifiziert werden. Es folgt

$$U(0)T = U(\infty), \text{ für alle } V(T) \in \mathfrak{S}_U$$

Bei der Wahl der Koordinatisierung ist die Operation des Translationskomplementes auf L_∞ zu beachten. Es genügt, nur solche Koordinatisierungen zu betrachten, die durch diese Operation nicht ineinander überführt werden können.

Es ist also hinreichend bei einer gegebenen Koordinatisierung alle zweidimensionalen Unterräume \hat{U} sowie alle Tripel $\{T_1, T_2, T_3\} \in \mathbf{S}$ zu durchlaufen und zu testen, ob

$$\hat{U}T_1 = \hat{U}T_2 = \hat{U}T_3$$

gilt für $\mathfrak{S}_U = \{U(0), U(\infty), U(T_1), U(T_2), U(T_3)\}$. Siehe den folgenden Algorithmus.

Algorithmus 19 Existenz einer fraktional-dimensionalen Unterebene

Eingabe: Spread-Menge \mathbf{S} mit gegebener Koordinatisierung, wobei $\mathbb{T}(\mathfrak{S}) = \mathbb{T}(\mathbf{S})$

Ausgabe: „true“, falls bei dieser Koordinatisierung eine Unterebene der Ordnung 4 existiert, „false“, falls nicht.

Initialisierung: $\mathbf{U} := \emptyset$, $w := \text{false}$, $E := \{v \mid v \in GF(2)^5 \setminus \{0\}\}$.

Schritt 1: Erstellen der 2-dimensionalen Unterräume

for i in $[1..Size(\mathbf{E})-1]$ **do**

for j in $[i+1..Size(\mathbf{E})]$ **do**

$u := \{E[i], E[j], E[i] + E[j]\}$ ein 2-dimensionaler Unterraum

 Füge u zu \mathbf{U} hinzu

end for

end for

Schritt 2: Test auf hinreichende Bedingung

$i := 1$

while $i \leq Size(\mathbf{U})$ und $w = \text{false}$ **do**

$j := 1$

while $j \leq Size(\mathbf{S}) - 2$ und $w = \text{false}$ **do**

$k := j + 1$

while $k \leq Size(\mathbf{S}) - 1$ und $w = \text{false}$ **do**

$l := k + 1$

while $l \leq Size(\mathbf{S})$ und $w = \text{false}$ **do**

$U_j := \mathbf{U}[i] \cdot \mathbf{S}[j]$, $U_k := \mathbf{U}[i] \cdot \mathbf{S}[k]$, $U_l := \mathbf{U}[i] \cdot \mathbf{S}[l]$

if $U_j = U_k = U_l$ **then**

$w := \text{true}$

end if

$l := l + 1$

end while

$k := k + 1$

end while

$j := j + 1$

end while

$i := i + 1$

end while

Ausgabe w

6. Fraktional-Dimensionale Unterebenen

Ergebnis:

Insgesamt gibt es 155 der 2-dimensionalen Unterräume, die pro Koordinatisierung mit $\begin{pmatrix} 31 \\ 3 \end{pmatrix}$ Matrix-Tripeln zu prüfen sind. Folgende Tabelle war das Ergebnis unserer Rechnung:

Ebene	Besitzt Unterebene der Ordnung 4	Koordinatisierung
\mathbb{T}_1	Nein	—
\mathbb{T}_2	Ja	$(1, 2, \infty)$
\mathbb{T}_3	Ja	$(1, 2, \infty)$
\mathbb{T}_4	Ja	$(\infty, 0, 1)$
\mathbb{T}_5	Ja	$(\infty, 0, 1)$
\mathbb{T}_6	Ja	$(\infty, 0, 1)$
\mathbb{T}_7	Ja	$(\infty, 0, 1)$
\mathbb{T}_8	Ja	$(\infty, 0, 1)$
\mathbb{T}_9	Ja	$(\infty, 0, 1)$

A. Anhang

A.1. Originalvortrag von Prof. Rudolf Mathon

Translation planes

of order 32

R. MATHON *

Outline

1. Basic facts

2. The search

3. Isomorph rejection

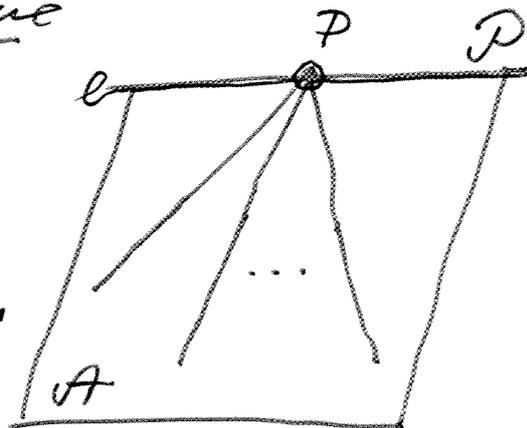
4. Algorithms

* U of Toronto, Toronto, CANADA

Translation plane

(finite)

nice automorphism
group



collineation π

axis l : if it fixes l pointwise

centre P : — " — P line wise

π is an elation if P is incident with l
 elations with axis l form group T
 (translation). If T is transitive
 [regular] on affine pts ($P-l$) then
 P is called a translation plane

Spreads and translation planes

Translation group T - elementary abelian

$T \iff$ vector space V of
dim. $2d$ over $GF(q)$

($|A|$ is square and T is regular on A)

P_i : points of \mathcal{L}

E_i : elations with centre P_i

\iff d -dim. subspaces of $GF(q)^{2d}$

E_i intersect in O only \implies
form a spread of $GF(q)^{2d}$

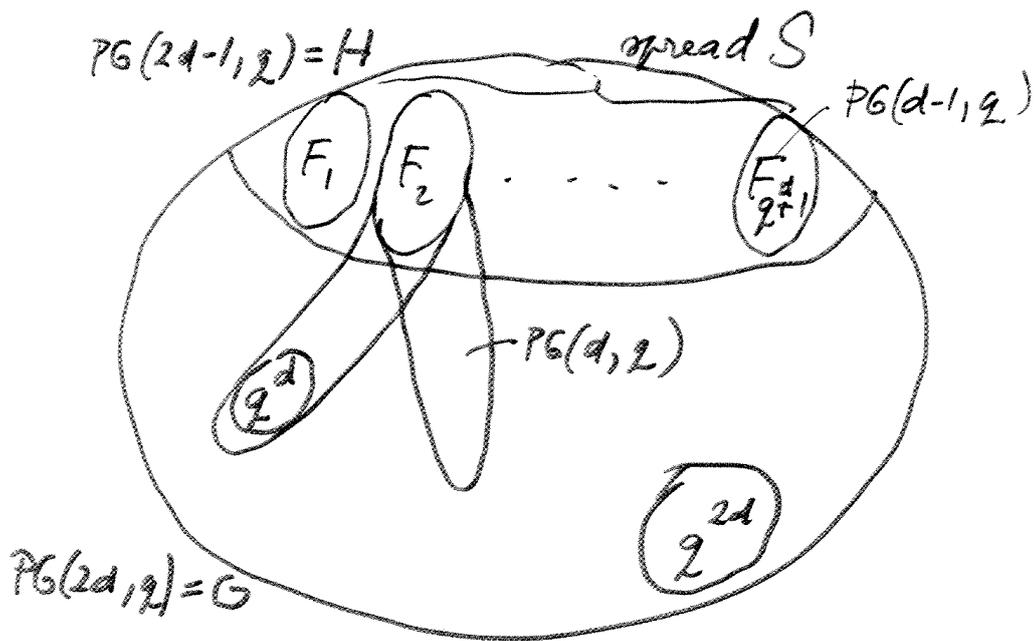
Conversely, spread of d -subspaces of V
form affine tr. plane \mathcal{A}

points : vectors in V

lines : cosets of the subspaces

To get \mathcal{P} add a line at infinity

Geometric construction (André, Bruck, Bose)



A: points - points of $G \setminus H$

lines - d -dim. subspaces of G
intersecting H in F_i 's

incidence - natural

P: line at infinity: F_1, \dots, F_{q+1}

\Rightarrow classification of S_{d-1} spreads in H

Translation planes of
small order

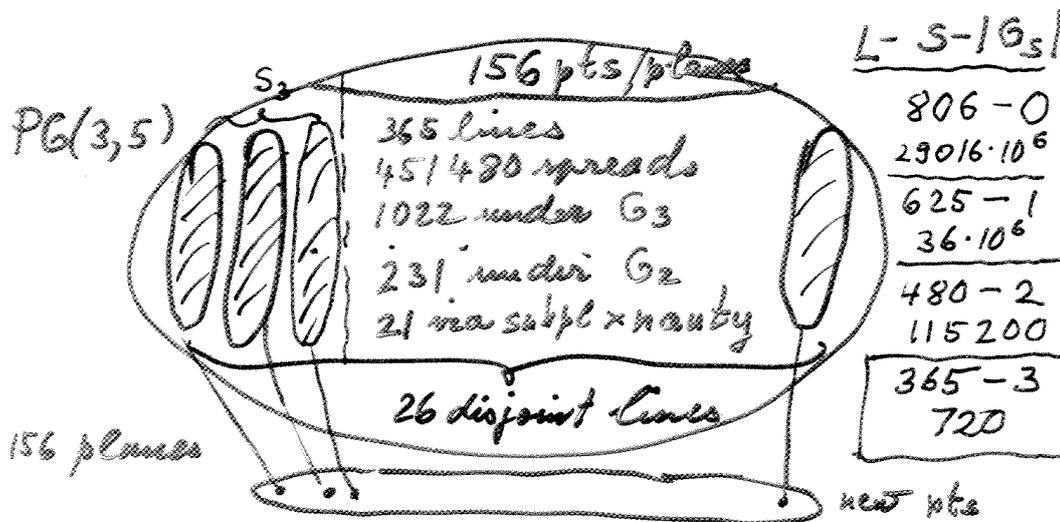
order	#	Reference
9	2	well known
16	8	Dempwolff, Reifart 83
25	21	Czerwinski, Oakden 82
27	7	Dempwolff 94 (M, R 95)
32	≥ 9	Mathon 85
49	1347	Mathon, Royle 95 (Charnes, Dempwolff 82)

Search plan for spreads

Example:

TRANSLATION PLANES OF ORDER 25

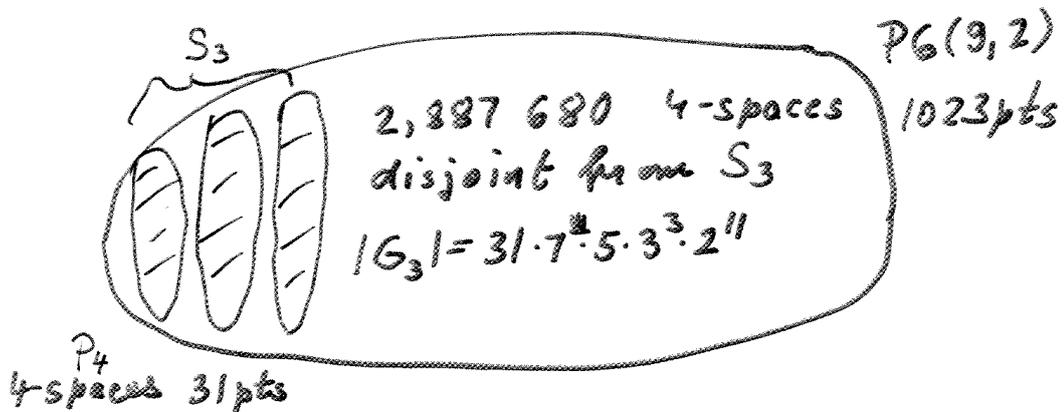
No	rk5	fano subplanes	F	G	Com
1	226	33*0	0	187200	Des
2	261	16*850000+10*1440000	28000000	1920	
3	251	20*690000+ 6*600000	17400000	1440	
4	255	24*280000+ 2*480000	7680000	1152	
5	239	20*510000+ 6*950000	15900000	720	
6	253	25*820000+ 1*500000	21000000	600	
7	258	24*700000+ 2*720000	18240000	576	
8	260	24*715000+2*1380000	19920000	288	
9	259	18*640000+ 8*585000	16200000	288	
10	259	12*535000+8*585000+6*700000	15300000	144	
11	262	12*405000+8*615000+6*580000	13260000	144	
12	260	20*570000+ 6*600000	15000000	120	
13	261	16*740000+6*640000+4*670000	18360000	96	
14	256	18*490000+6*400000+2*570000	12360000	72	
15	262	33*550000	14300000	52	P16
16	258	33*550000	14300000	52	P15
17	258	24*515000+ 2*480000	13320000	48	
18	257	24*500000+ 2*600000	13200000	48	
19	264	18*620000+6*680000+2*480000	16200000	36	
20	262	16*640000+8*580000+2*700000	16280000	32	
21	259	12*530000+6*650000+4*690000+4*600000	15420000	24	



Translation planes of order 32

Spreads of 4-spaces in $P_6(9,2)$

P_4	S	$ G_s $
109, 221 651	0	$127 \cdot 73 \cdot 31^2 \cdot 17 \cdot 11 \cdot 7^3 \cdot 5^2 \cdot 3^6 \cdot 2^{45}$
33, 554 432	1	$31^2 \cdot 7^2 \cdot 5^2 \cdot 3^4 \cdot 2^{45}$
9, 999 360	2	$31^2 \cdot 7^2 \cdot 5^2 \cdot 3^4 \cdot 2^{21}$



2 orbits of P_4 disjoint from S_3 under G_3

S_4^A stabilizer G_A of order 252
 S_4^B — " — G_B — " — 124

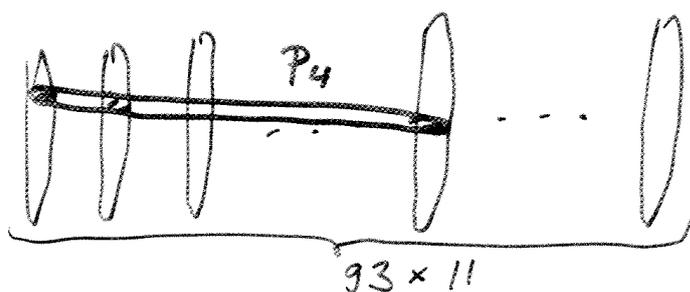
There are 2070 non-iso sets of 5 disjoint 4-sp.

Aut. orders for spreads: $\boxed{31, 11, 7, 5, 3, 2, 1}$
 (possible)

Sample automorphisms

order 11 single class

93 pt. orbits, no fixed pts
 stabilizer G_{11} of order 10230



288 519 transversal P_4 's
 (sets of 11 disjoint 4-spaces)

partitioning into 30 orbits under G_{11}

$$1 \cdot 33 + 1 \cdot 2046 + 28 \cdot 10230$$

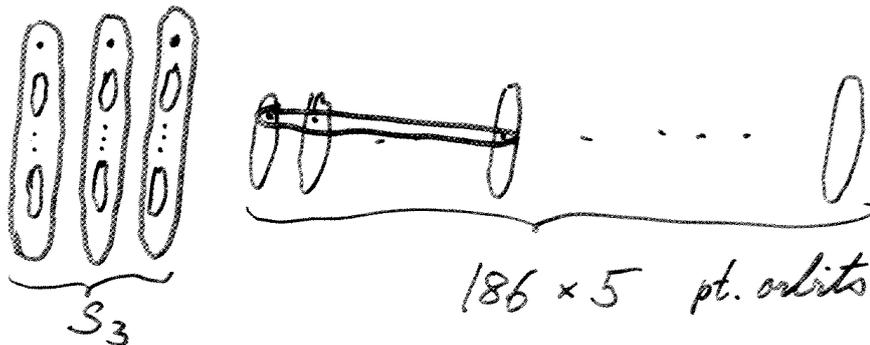
Complete search ("spreads") from orbit
 representatives yields exactly 2 solutions

Dis	No. 4	\emptyset
Stab.	5074080	165

(Can use clique finder: # of disj. 4-sp is from 0 to 110)

order 5 single class ζ_5

(at least 3 fixed P_4 's, pick any 3 and examine stabilizer in $PTL(10,2)$)

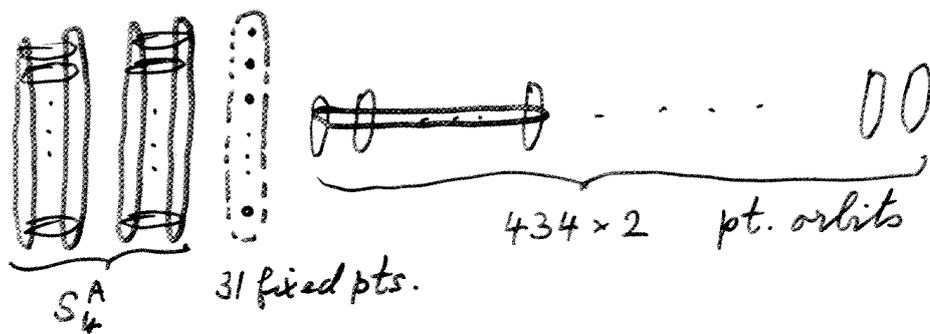


40896 transversal P_4 's or
sets of 5 disjoint 4-spaces

Complete search via "spreads" yields
288 solutions. Using the stabilizer
of $S_3 + \zeta_5$ of order 360 these partition
into 7 orbits representing 7 non-iso.
spreads (planes No. 1-7).

order 2 single class \mathcal{C}_2^A

assuming spread contains S_4^A with stabilizer of order 252



Any spread must contain P_4 formed by the fixed points (computer proof)

108,864 transversal P_4 's
(sets of 2 disjoint 4-spaces)

Complete search via "spreads" yields 6804 solutions (11 hours on a 2.6Hz G5). Using the stabilizer of $S_4^A + \mathcal{C}_2^A$ of order 84 partitions them into 324 orbits representing 5 non-iso spreads (planes No. 5-9) (~5 hours via "nauty")

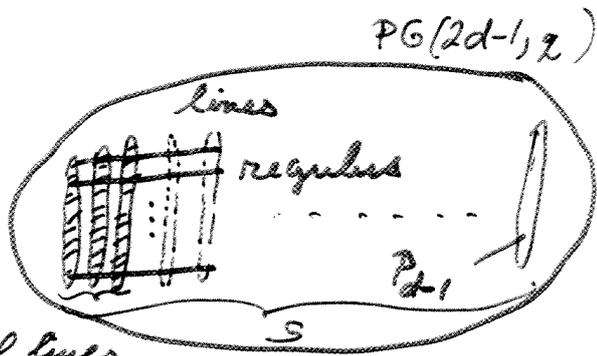
[Similar search with S_4^B yields 9146 solutions, 296 orbits and 6 non-iso spreads (No. 1, 5-9).]

Isomorphism invariants

SPREADS:

Regulus profile

regulus
 $\{q+1$ disjoint P_{d-1} with
 $|P_{d-1}|$ disjoint transversal lines



Any 3 disjoint P_{d-1} determine a unique regulus
 ($d=2$ is ordinary regulus).

For each of the $\binom{q^d+1}{3}$ triples of P_{d-1} 's in S
 find the # of subspaces the induced regulus
 shares with S .

short profile : (x_3, \dots, x_{q+1}) where
 $x_i = \#$ of reguli meeting S in $\binom{2}{i} P_{d-1}$'s

long profile : $(y^{(1)}, \dots, y^{(q^d+1)})$

$$y^{(j)} = (y_3^{(j)}, \dots, y_{q+1}^{(j)})$$

$y_i^{(j)} = \#$ of triples (reguli) through S_j
 meeting S in $\binom{2}{i}$ subspaces

Does not work for $q=2$. Use transversal P_{d-1} 's.

Fingerprints

view as d -dim subspaces in $V = GF(q)^{2d}$

$$W_\infty = \{ (0, \dots, 0, x_1, \dots, x_d) \mid x_i \in GF(q) \}$$

$$W_0 = \{ (x_1, \dots, x_d, 0, \dots, 0) \mid x_i \in GF(q) \}$$

$$W_A = \{ (\underline{x}, \underline{x}A \mid \underline{x} \in GF(q)^d \}$$

A - non singular $d \times d$ matrix

Spread set $\{ W_{A_i} \mid i=1, \dots, q^d, A_i = 0$

W_{A_i}, W_{A_j} disjoint $\Leftrightarrow A_i - A_j$ non singular

Matrix B ($q^d \times q^d$), 0 diagonal

$$b_{ij} = \pm 1 \Leftrightarrow \det(A_i - A_j) = \prod_{\alpha \in GF(q)} \alpha$$

$Q = BB^T$ (product over rationals)

Fingerprint is the multiset of absolute values of entries in Q from $\{1, \dots, q^d\}$

Can be used for partial spreads.

Very good if $d=2$ (orders 25, 49, ...).

PLANES

$$q = p^m$$

p-rank of pt \times line incidence matrix

{ duality preserves p-rank
polarity - does not nec. preserve

distribution of Fano subplanes

$\#$ of subplanes incident with
pts (lines) of a plane

for translation planes only pts of
translation line. For order 32 this
is a fast and strong invariant
distinguishes duality but not polarity.

These work on any finite projective plane.
Most difficult are translation planes
with transitive spreads - no help from
invariants - improve "nauty".

TRANSLATION PLANES OF ORDER 32

No	fano subplanes	F	rk2	G	D	P	TS4	x*Cm
1	33*43298816	1342263296	244	5074080	1	1	65472	N*33
2	31*5395456+5682176+5206016	91549696	344	155	3	3	2573	62*11
3	31*5410816+5047296+4729856	90914816	344	155	2	2	2573	62*11
4	33*6445056	126089216	349	165	4	4	990	330*9
5	32*5395456+43298816	129355776	328	160	6	7	1952	9*32
6	32*6547456+43298816	166219776	328	160	5	6	1344	640*9
7	32*5364736+43298816	128372736	342	160	7	5	1952	9*32
8	32*5342208+43298816	127651840	344	32	9	9	1664	5*32
9	32*5387264+43298816	129093632	344	32	8	8	1664	5*32

Invariants:

translation line L contains x points incident with y fano planes (sum x*y)

F is the total number of fano planes incident with translation line

rk2 is the 2-rank of the incidence matrix

|G| is the order of the translation complement G
 group of plane is 1024 times larger except for Des (#1)
 which is 1024*1057 times bigger

D,P are planes dual and polar to a given plane, respectively

TS4 number of 4-subspaces transversal to spread in PG(9,2)

x*Cm number of maximum sets of m disjoint transversal 4-subspaces

B. Literatur

- JOH Biliotti, M; Jha, V; Johnson, N: *Foundation of Translation Planes*, Marcel Dekker Inc., 2001.
- BON Bongartz, K: *Normalformen von Matrizen*, Vorlesung Lineare Algebra 2, Uni Wuppertal, SS2006.
- BRA Braun, M: *Konstruktion diskreter Strukturen unter Verwendung von Operationen linearer Gruppen auf dem linearen Verband*, Doktorarbeit der Universität Bayreuth, 2003. ftp://ftp.mathe2.uni-bayreuth.de/DIPLOM/diss_braun_michael.pdf
- COR Corneil, D. G; Gotlieb, C. C: *An Efficient Algorithm for Graph Isomorphism*, Journal of the Association for Computing Machinery, 17 (1970), S. 51-64.
- COS Cossidente, A; Resmini, M.J: *Remarks on Singer Cyclic Groups and Their Normalizers*, Designs, Codes and Cryptography, 32 (2004), 97-102.
- DBR Dembowski, P: *Finite Geometries*, Springer-Verlag, 1997.
- SEM Dempwolff, U: *Files for Semifield Planes of Order 32*, http://www.mathematik.uni-kl.de/~dempw/dempw_32_semi.html.
- GRP Dempwolff, U: *Gruppentheorie*, Vorlesungsmitschrift, SS 2009.
- DEM Dempwolff, U: *Introduction to Finite Projective Planes*, Vorlesungsskript.
- POL Dempwolff, U; Müller, P: *Permutation Polynomials and Translation Planes of Even Order*, Preprint, 2011.
- CTP Dempwolff, U; Reifart, A: *The Classification of the Translation Planes of Order 16*, Geometriae Dedicata, 17 (1984), S. 1-9.
- TRA Dempwolff, U: *Translation Planes of Order 27*, Designs, Codes and Cryptography, 4 (1994), 105-121.
- DIE Diestel, R: *Graphentheorie*, Elektronische Ausgabe, Springer-Verlag, Heidelberg, 2000.
- HUG Hughes, D.R; Piper, F.C: *Projective Planes*, Springer, 1973.
- HUP Huppert, B: *Endliche Gruppen I*, Springer-Verlag, 1976.
- DIM Jha, V; Johnson, N: *The dimension of a subplane of a translation plane*, Bulletin of the Belgian Mathematical Society - Simon Stevin, 3 (2010), Soc., Brussels, S. 463 - 479.
- KAL Kallaher, M.J: *Affine Planes with Transitive Collineation Groups*, North Holland, 1982.
- KAN Kantor, W.M: *Orthogonal spreads and translation planes*, Advanced Studies in Pure Mathematics, 24 (1996), Mathematical Society Japan, S. 227-242.
- KLE Klein, H: *Geometrie I*, Universität Kiel, Skript zum Wintersemester 2000/2001.
- KNA Knarr, N: *Translation Planes*, Springer, 2009.
- GRA Krumke, S.O; Noltemeier, H; Schwarz, S; Wirth, H.C: *Graphentheoretische Konzepte und Algorithmen*, Vorlesungsskript, 2000.
- LÜN Lüneburg, H: *Lectures on Projective Planes*, University of Illinois, Lecture Notes, 1969.
- MAD Maduram, D.M: *Matrix Representation of Translation Planes*, Geometriae Dedicata, 4 (1975), S. 485 - 492.

B. Literatur

- MAT Mathon, R: *Translation planes of order 32 with non-trivial translation complement*, Abstract eines Vortrages der ALCOMA 2005, Bayreuth, http://www.mathe2.uni-bayreuth.de/ALCOMA05/mathon_alcoma.pdf.
- MOR Moorhouse, G.E: *On projective planes of order less than 32*, Finite Geometries, Groups, and Computation, Berlin 2006, S. 149-162.
- PIC Pickert, M: *Projektive Ebenen*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen Band LXXX Springer,1955.
- PRI Prince, A: *Flag-Transitive Affine Planes of Order at Most 125*, Journal of Geometry, 67 (2000), Birkhäuser Verlag, Basel, S. 208-216.
- WAL Walker, R.J: *Determination of Division Algebras with 32 Elements*, Proceedings of symposia in applied mathematics, 15 (1962), S. 83-85.
- WIL Wilhelm, L: *Die Suche nach einer Translationsebene der Ordnung 64*, Diplomarbeit am Fachbereich Mathematik der Universität Kaiserslautern, 1991.

C. Erklärung

Hiermit erkläre ich, dass ich diese Arbeit selbst verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Kaiserslautern, den 23.09.2011

Robert Rockenfeller