

OVOIDE 8-DIMENSIONALER QUADRATISCHER RÄUME

Andrea Mindnich

Vom Fachbereich Mathematik der Technischen Universität Kaiserslautern zur
Verleihung des akademischen Grades Doktor der Naturwissenschaften (Doctor
rerum naturalium, Dr. rer. nat.) genehmigte Dissertation

1. Gutachter: Prof. Dr. U. Dempwolff
2. Gutachter: Prof. Dr. K. Metsch

Vollzug der Promotion: 23. April 2007

D386

Inhaltsverzeichnis

Einleitung	3
1 Grundlagen	6
1.1 Quadratische Räume	6
1.2 Ovoide	8
1.3 Die Kleinkorrespondenz	10
2 Die bekannten Ovoide in $V^+(8, q)$	16
2.1 Unitäre Ovoide	16
2.2 Ree-Tits Ovoide	17
2.3 Desarguessche Ovoide	18
2.4 Das Ovoid von Dye	18
2.5 Ovoide aus dem Wurzelsystem E_8	18
3 Normalformen orthogonaler Abbildungen	21
3.1 Orthogonale Zerlegungen	21
3.2 Quadratische Formen	28
3.2.1 Moduln vom Typ $\text{II}_{(x\pm 1)^n}$	29
3.2.2 Moduln vom Typ $\text{I}_{(x\pm 1)^n}$	32
3.2.3 Moduln vom Typ III_{pp^*}	34
3.2.4 Moduln vom Typ II_{p^n}	34
3.3 Typen orthogonaler Zerlegungen	36
4 Invarianten und Äquivalenz	42
4.1 Der Fingerprint	42
4.2 Der Footprint	44
4.3 Die Dimensionsinvariante	46
4.4 Äquivalenztest	48
4.5 Stabilisatoren von Ovoiden	52
5 Ovoidsuche in $V^+(2n, q)$	54
5.1 Partition der singulären Punkte	54
5.2 Äquivalenz von Teilovoiden	55

5.3	Ein Algorithmus zur Ovoidsuche	56
6	Ergebnisse der Ovoidsuche	64
6.1	Ovoide von $V^+(8, 7)$	64
6.2	Ovoide von $V^+(8, 8)$	67
6.3	Ovoide von $V^+(8, 9)$	68
7	Anwendung der Algorithmen in $V^+(6, 8)$	69
7.1	Die Projektionen des Dye-Ovoids	69
7.2	Semifields und Ovoide	69
7.3	Weitere Ovoide von $V^+(6, 8)$	72
A	Ergebnistabellen	74
A.1	$V = V^+(8, 7)$	74
A.2	$V = V^+(8, 8)$	77
A.3	$V \simeq V^+(8, 9)$	79
B	Ein Beispielprogramm in GAP	80

Einleitung

Diese Arbeit beschäftigt sich mit Ovoiden in 8-dimensionalen quadratischen Räumen von maximalem Wittindex.

Sei V ein endlicher nicht ausgearteter quadratischer $\text{GF}(q)$ -Raum. Ein Ovoid $\mathcal{O}$ von V ist eine Menge singulärer Punkte, das heißt singulärer eindimensionaler Teilräume von V , so dass $\mathcal{O}$ mit jedem maximalen total singulären Teilraum von V genau einen Punkt gemeinsam hat. Wir sagen, dass ein quadratischer $\text{GF}(q)$ -Raum V vom Typ $V^+(2n, q)$ ist, falls $\dim(V) = 2n$ ist und V maximalen Wittindex hat.

Außer in Räumen vom Typ $V^+(6, q)$, deren Ovoide über die Kleinkorrespondenz den Spreads von $\text{GF}(q)^4$ entsprechen, sind nur wenige Beispiele für Ovoide bekannt. Es wird vermutet, dass es in nicht ausgearteten quadratischen Räumen der Dimension größer 8 keine Ovoide gibt. Dazu sind die folgenden Nichtexistenzaussagen bekannt:

Nach Thas [Tha81] gibt es keine Ovoide, falls V nicht maximalen Wittindex hat und $\dim(V) \geq 6$ ist. Weiterhin gibt es keine Ovoide, wenn $\dim(V) \geq 9$ und ungerade ist, siehe [Tha81, GM97]. Ist $V = V(n, p^e)$ ein n -dimensionaler quadratischer $\text{GF}(p^e)$ -Raum mit p prim und $e \in \mathbb{N}$, so haben Blockhuis und Moorhouse [BM95] gezeigt, dass V keine Ovoide enthält, falls

$$p^{\lfloor \frac{n-1}{2} \rfloor} > \binom{n-2+p}{n-1} - \binom{n-4+p}{n-1}.$$

Das heißt, zu gegebener Primzahl p existiert eine Schranke n_p , so dass es keine Ovoide von $V(n, p^e)$ gibt, falls $n \geq n_p$ ist. Eine tabellarische Übersicht zu weiteren Existenz- bzw. Nichtexistenzaussagen von Ovoiden in verschiedenen Räumen findet sich in [Tha01].

Sei nun V ein quadratischer Raum vom Typ $V^+(8, q)$. In diesem Fall bildet die so genannte „Trialität“ die Ovoide von V bijektiv auf orthogonale Spreads von V ab. Die Ovoide von V sind bisher nur für $q \leq 5$ klassifiziert [CD00]. Weiterhin ist zu den Automorphismengruppen der Ovoide von V folgendes bekannt:

Alle Ovoide von V , die eine 2-transitive bzw. primitive Automorphismengruppe besitzen sind klassifiziert, vgl. [Kle88, Gun00]. Für die Fälle $q = 7$ und $q = 25$ zeigt ein Computerresultat von B. Williams [Wil99], dass es keine Ovoide mit transitiver Automorphismengruppe gibt.

Die vorliegende Arbeit entstand aus der Idee, für $q \geq 7$ neue Ovoide in 8-dimensionalen quadratischen $\text{GF}(q)$ -Räumen zu finden. Mit Hilfe des Computeralgebrasystems GAP wurde speziell für $q \in \{7, 8, 9\}$ systematisch nach Ovoiden gesucht. Dabei sind leider keine neuen Ovoide aufgetreten. Jedoch erlaubt die Systematik, Aussagen über die Stabilisatoren von Ovoiden zu treffen, die nicht aus einer der bekannten Konstruktionen stammen.

Bei der Ovoidsuche in dieser Arbeit wurden vorwiegend zyklische Gruppen $G \leq \text{PO}(V)$ bestimmter Ordnungen vorgeben und alle Ovoide von V bestimmt, die invariant unter einer solchen Gruppe G sind. Dadurch ergeben sich Abschätzungen für die Ordnung von Gruppen und deren Elemente, die als Stabilisatoren solcher Ovoiden auftreten können, die nicht zu den bisher bekannten zählen. Diese Arbeit gliedert sich nun wie folgt.

Im ersten Kapitel werden zunächst grundlegende Begriffe und Notationen zur Theorie der quadratischen Räume angegeben. Dann werden Ovoide eingeführt und schließlich wird aufgezeigt, wie sich mit Hilfe der Kleinkorrespondenz Spreads von $\text{GF}(q)^4$ bijektiv auf Ovoide von $V^+(6, q)$ abbilden lassen.

Danach werden im zweiten Kapitel die bekannten Ovoide von $V^+(8, q)$ vorgestellt.

Kapitel 3 beschäftigt sich mit Normalformen orthogonaler Abbildungen mit dem Ziel bis auf Konjugation die zyklischen Untergruppen bestimmter Ordnungen in $\text{O}(V^+(8, q))$ bestimmen zu können. Wir erhalten dadurch eine Beschreibung der zyklischen Gruppen, die als Automorphismengruppen von Ovoiden in Frage kommen. Da die Berechnung der Konjugiertenklassen von $\text{O}(V^+(8, q))$ sehr aufwändig ist, werden viele der späteren Rechnungen durch diese theoretische Betrachtung erst ermöglicht oder zumindest stark vereinfacht. Außerdem ergibt sich so eine übersichtlich strukturierte Aufzählung der betrachteten Fälle.

Die folgenden Kapitel konzentrieren sich dann auf die Suche nach Ovoiden mit Hilfe des Computers.

In Kapitel 4 werden zunächst Invarianten für Ovoide behandelt, die die Ovoidsuche deutlich erleichtern. Sie werden sowohl verwendet um während der Ovoidsuche Äquivalenzklassen von Teilovoiden zu bilden, als auch um Äquivalenztests für volle Ovoide durchzuführen. Im Anschluss an die Beschreibung des Äquivalenztests wird dessen Anwendung zur Berechnung von Automorphismengruppen von Ovoiden besprochen.

Im nachfolgenden Kapitel 5 wird dann ein Suchalgorithmus für Ovoide in $V^+(2n, q)$ entwickelt. Zu einzelnen Schritten des Algorithmus werden kurz Variationsmöglichkeiten besprochen und dann einige Beispiele zu dessen Laufzeitverhalten angegeben.

In Kapitel 6 sind die Ergebnisse der Ovoidsuche, die für $q = 7, 8, 9$ in $V^+(8, q)$ durchgeführt wurde, zusammengefasst. Die einzelnen Ergebnisse der Suche mit vorgegeben zyklischen Automorphismengruppen sind im Anhang A in tabellarischer Form angegeben.

Kapitel 7 demonstriert die Anwendungsmöglichkeiten der entwickelten Me-

thoden auf Ovoide von $V^+(6, q)$, das heißt auf Translationsebenen der Ordnung q^2 mit Kern $\text{GF}(q)$. Es werden hier einige Beispiele für $q = 8$ gerechnet. Konkret berechnen wir die Stabilisatoren der Ovoide von $V^+(6, 8)$, die sich durch Projektion aus dem Ovoid von Dye ergeben. Dann werden die Ovoide bestimmt, die über die Kleinkorrespondenz den Semifieldebenen der Ordnung 64 mit Kern $\text{GF}(8)$ entsprechen und auch hier die Stabilisatoren berechnet. Schließlich verwenden wir den Suchalgorithmus aus Kapitel 5 um alle Ovoide von $V^+(6, 8)$ zu finden, die invariant unter einer zyklischen Gruppe $G \leq \text{PO}(V^+(6, 8))$ der Ordnung 5, 7, 8, 9, 13 oder 73 sind. Wir stellen fest, welches die Ovoide von $V^+(6, 8)$ mit nicht auflösbarem Stabilisator sind.

In Anhang B findet sich als Beispiel für die Implementierung der Algorithmen dieser Arbeit ein GAP-Programm zur Berechnung des Stabilisators eines Ovoids.

Ich danke meinem Betreuer Herrn Dempwolff für seine Hilfe beim Erstellen dieser Arbeit. Außerdem danke ich meinen Freunden für ihre Unterstützung und hilfreiche Diskussionen.

Kapitel 1

Grundlagen

1.1 Quadratische Räume

In diesem Abschnitt führen wir die verwendeten Notationen für quadratische Räume ein. Einzelheiten zu quadratischen Räumen finden sich beispielsweise in [Tay92] und [Gro02].

Definition 1.1.1. Sei K ein Körper und V ein K -Vektorraum. Eine Abbildung $Q: V \rightarrow K$ heißt *quadratische Form* auf V genau dann, wenn

- (i) Für alle $x \in V$ und alle $a \in K$ ist $Q(ax) = a^2Q(x)$.
- (ii) Durch $(x, y) := Q(x + y) - Q(x) - Q(y)$ ist eine Bilinearform auf V definiert.

(V, Q) heißt *quadratischer Raum*.

Wenn nur eine quadratische Form auf einem Vektorraum V betrachtet wird, nennen wir auch V quadratischen Raum, ohne die Form explizit zu benennen.

Definition 1.1.2. Sei V ein quadratischer K -Raum. V heißt

- (i) *ausgeartet*, falls es ein $v \in V \setminus \{0\}$ gibt mit $(v, w) = 0$ für alle $w \in V$,
- (ii) *total ausgeartet*, wenn $(v, w) = 0$ für alle $v, w \in V$,
- (iii) *singulär*, falls es ein $v \in V \setminus \{0\}$ gibt mit $Q(v) = 0$,
- (iv) *total singulär*, falls $Q(v) = 0$ für alle $v \in V$ ist.

Man sieht leicht, dass jeder total singuläre Raum total ausgeartet ist. Falls $\text{Char}(K)$ gerade ist, gilt die Umkehrung jedoch nicht.

Je zwei maximale total singuläre Teilräume eines quadratischen Raums V haben die gleiche Dimension. Diese Dimension heißt *Wittindex* von V .

Definition 1.1.3. Sei V ein quadratischer Raum.

- (i) Ist $U \subseteq V$ ein Teilraum, so ist $U^\perp := \{v \in V \mid (v, u) = 0 \text{ für alle } u \in U\}$ das *orthogonale Komplement* von U in V .
- (ii) Die Menge $\text{Rad}(V) := V^\perp = \{v \in V \mid (v, w) = 0 \text{ für alle } w \in V\}$ wird als *Radikal* von V bezeichnet.

Definition 1.1.4. Sei (V, Q) ein quadratischer Raum und $v \in V \setminus \{0\}$. Falls $Q(v) = 0$ ist, so heißt v *singulär* und $\langle v \rangle$ wird als *singulärer Punkt* von V bezeichnet. Wir bezeichnen mit $I(V)$ die Menge der singulären Punkte von V .

Sind $v, w \in V \setminus \{0\}$ singulär und $(v, w) = 1$, so heißt das Paar $\{v, w\}$ *hyperbolisches Paar* und $\langle v, w \rangle$ heißt *hyperbolische Ebene*.

Sei $B = (v_1, \dots, v_{2n})$ eine Basis von V , so dass $V = \langle v_1, v_{n+1} \rangle \perp \dots \perp \langle v_{n-1}, v_{2n} \rangle$ ist und die Paare $\{v_i, v_{n+i}\}$ für alle $1 \leq i \leq n$ hyperbolische Paare sind. Dann heißt B *hyperbolische Basis* von V .

Lemma 1.1.5 ([Tay92, S. 138]). *Ist V ein endlicher nicht ausgearteter quadratischer Raum, dann gibt es hyperbolische Ebenen $V_1, \dots, V_n$ von V und einen Teilraum W von V , der keine singulären Vektoren enthält, so dass $V = V_1 \perp \dots \perp V_n \perp W$ ist. Dabei ist $\dim W \leq 2$, und V ist bis auf Isomorphie eindeutig durch n und W bestimmt. Die Zahl n ist der Wittindex von V .*

Lemma 1.1.6 ([Tay92, S. 139]). *Sei $V = V_1 \perp \dots \perp V_n \perp W$ ein quadratischer Raum über $\text{GF}(q)$ mit hyperbolischen Ebenen V_i und nicht singulärem W .*

Für $1 \leq i \leq n$ sei $\{e_i, e_{n+i}\}$ ein hyperbolisches Paar von V_i . Nach Lemma 1.1.5 ist $\dim W \leq 2$, es ergeben sich somit die folgenden drei Fälle:

(i) *Falls $\dim(W) = 0$, so ist $V = V_1 \perp \dots \perp V_n$ und $(e_1, \dots, e_{2n})$ eine hyperbolische Basis von V . Es gilt*

$$Q\left(\sum_{i=1}^{2n} x_i e_i\right) = \sum_{i=1}^n x_i x_{i+n}.$$

Wir schreiben in diesem Fall $V^+(2n, q)$ für (V, Q) .

(ii) *Im Fall $\dim(W) = 1$ sei $W = \langle e_{2n+1} \rangle$. Dann ist die quadratische Form gegeben durch*

$$Q\left(\sum_{i=1}^{2n+1} x_i e_i\right) = \sum_{i=1}^n x_i x_{i+n} + Q(e_{2n+1}) x_{2n+1}^2.$$

Wir schreiben $V(2n+1, q)$ für (V, Q) .

(iii) *Falls $\dim(W) = 2$ ist, so gibt es $e_{2n+1}, e_{2n+2} \in W$ mit $Q(e_{2n+1}) = 1$ und $(e_{2n+1}, e_{2n+2}) = 1$, so dass $W = \langle e_{2n+1}, e_{2n+2} \rangle$. Für die quadratische Form gilt*

$$Q\left(\sum_{i=1}^{2n+2} x_i e_i\right) = \sum_{i=1}^n x_i x_{i+n} + x_{2n+1}^2 + x_{2n+1} x_{2n+2} + Q(e_{2n+2}) x_{2n+2}^2.$$

Da W keine singulären Punkte enthält, ist das Polynom $X^2 + X + Q(e_{2n+2})$ irreduzibel über $\text{GF}(q)$.

Wir schreiben $V^-(2n+2, q)$ für (V, Q) in diesem Fall.

Definition 1.1.7. Ist V ein K -Vektorraum, $f: V \rightarrow V$ eine Abbildung und $\sigma \in \text{Aut}(K)$, so heißt f genau dann σ -semilinear, wenn

$$f(u + v) = f(u) + f(v) \text{ für alle } u, v \in V, \text{ und}$$

$$f(av) = a^\sigma f(v) \text{ für alle } v \in V, a \in K.$$

f heißt *semilinear*, falls es ein $\sigma \in \text{Aut}(K)$ gibt, so dass f eine σ -semilineare Abbildung ist.

Definition 1.1.8. Sei V ein quadratischer Raum, $f: V \rightarrow V$ eine bijektive, semilineare Abbildung auf V und $s \in K \setminus \{0\}$.

- (i) f heißt *Semiähnlichkeit* mit Multiplikator s , wenn es einen Körperautomorphismus σ gibt, so dass $Q(f(x)) = sQ(x)^\sigma$ für alle $x \in V$.
- (ii) Ist $\sigma = 1$, so heißt f *Ähnlichkeit*.

Sei V ein quadratischer Raum. Dann bezeichne $O(V)$ die Gruppe der orthogonalen Abbildungen von V , das heißt

$$O(V) = \{f \in \text{GL}(V) \mid Q(f(v)) = Q(v) \text{ für alle } v \in V\}$$

Des Weiteren sei $GO(V)$ die Gruppe der Ähnlichkeiten von V und $\Gamma O(V)$ die Gruppe der Semiähnlichkeiten von V . Für $G \in \{O(V), GO(V), \Gamma O(V)\}$ bezeichnet zudem $PG = G/Z(G)$ die zugehörige projektive Gruppe.

1.2 Ovoids

Definition 1.2.1. Sei V ein endlicher nicht ausgearteter quadratischer Raum und $\mathcal{O}$ eine Menge singulärer Punkte von V .

- (i) $\mathcal{O}$ heißt *Ovoid*, wenn es zu jedem maximalen total singulären Teilraum W von V genau ein $\langle x \rangle \in \mathcal{O}$ gibt mit $x \in W$.
- (ii) Falls $\mathcal{O}$ mit jedem maximalen total singulären Teilraum höchstens einen Punkt gemeinsam hat, so heißt $\mathcal{O}$ *Teilovoid*.

Ist zum Beispiel $V = V(3, q)$ oder $V = V^-(4, q)$, dann hat V den Wittindex 1, sodass ein Ovoid von V genau aus allen singulären Punkten von V besteht.

Ist $\mathcal{O}$ ein Teilovoid eines quadratischen Raums, so lässt sich $\mathcal{O}$ nicht notwendig zu einem Ovoid erweitern.

Definition 1.2.2. Sei V ein endlicher nicht ausgearteter quadratischer Raum. Zwei Teilovoide $\mathcal{O}$ und $\mathcal{O}'$ von V heißen äquivalent, wenn es eine Semiähnlichkeit γ auf V gibt, so dass $\mathcal{O}' = \gamma(\mathcal{O})$. Wir schreiben dann $\mathcal{O} \sim \mathcal{O}'$.

Je zwei verschiedene Punkte eines Ovoids $\mathcal{O}$ sind nicht orthogonal, denn sind $\langle x \rangle, \langle y \rangle \in \mathcal{O}$ mit $(x, y) = 0$, so gibt es einen maximalen total singulären Teilraum, der $\langle x, y \rangle$ enthält, also ist $\langle x \rangle = \langle y \rangle$.

Satz 1.2.3. *Sei $m \in \mathbb{N}$ und $V = V^+(2m, q)$, $V(2m - 1, q)$ oder $V^-(2m - 2, q)$ mit positivem Wittindex. Ist $\mathcal{O}$ eine Menge von singulären, paarweise nicht orthogonalen Punkten von V , so ist $\mathcal{O}$ genau dann ein Ovoid von V , wenn $|\mathcal{O}| = q^{m-1} + 1$.*

Beweis. Es bezeichne $H_{n,d}$ die Anzahl der maximalen total singulären Teilräume eines d -dimensionalen quadratischen Raumes vom Wittindex n . Dann gilt nach [Cam00, 6.14]:

$$H_{n,d} = \prod_{i=1}^n (1 + q^{i+\epsilon})$$

wobei

$$\epsilon = \begin{cases} 0, & \text{falls } d = 2n + 1 \\ -1, & \text{falls } d = 2n \\ 1, & \text{falls } d = 2n + 2. \end{cases}$$

Sei d nun die Dimension von V . Ist $n = 1$, so besteht ein Ovoid von V genau aus allen singulären Punkten von V und die Behauptung folgt daraus, dass $H_{1,d} = q^{m-1} + 1$ die Anzahl der singulären Punkte von V ist. Sei also im Folgenden $n \geq 2$.

Ist $0 \neq x \in V$ mit $Q(x) = 0$, dann ist die Anzahl der maximalen total singulären Teilräume von V , die x enthalten, gleich $H_{n-1,d-2}$. Falls $\mathcal{O}$ ein Ovoid von V ist, so ist also

$$|\mathcal{O}| = \frac{H_{n,d}}{H_{n-1,d-2}} = 1 + q^{n+\epsilon} = 1 + q^{m-1}.$$

Für die umgekehrte Richtung sei nun $|\mathcal{O}| = q^{m-1} + 1$. Da die Punkte von $\mathcal{O}$ paarweise nicht orthogonal sind, hat jeder maximale total singuläre Teilraum höchstens einen Punkt mit $\mathcal{O}$ gemeinsam. Gäbe es nun einen maximalen total singulären Teilraum, der keinen Punkt aus $\mathcal{O}$ enthält, so wäre $|\mathcal{O}| < \frac{H_{n,d}}{H_{n-1,d-2}} = 1 + q^{m-1}$. $\square$

Im Folgenden sehen wir, wie sich aus Ovoiden quadratischer Räume durch Projektion Ovoide von quadratischen Räumen kleinerer Dimension gewinnen lassen.

Sei (V, Q) ein nicht ausgearteter quadratischer Raum, $\mathcal{O}$ ein Ovoid von V und P ein singulärer Punkt von V mit $P \notin \mathcal{O}$. Definiere $\overline{V} := P^\perp/P$. Dann gilt:

$$\dim \overline{V} = \dim P^\perp - \dim P = \dim V - \dim P - 1 = \dim V - 2$$

Definiere außerdem $\overline{Q}: \overline{V} \rightarrow K, \overline{x} \mapsto Q(x)$. Da P singulär ist, ist $\overline{Q}$ wohldefiniert. $\overline{Q}$ ist dann eine quadratische Form auf $\overline{V}$. Dabei ist $\overline{V}$ vom Typ $V^+(2n, q)$ genau dann, wenn $\overline{V}$ vom Typ $V^+(2n - 2, q)$ ist.

Satz 1.2.4. *Sei $\mathcal{O}$ ein Ovoid eines nicht ausgearteten quadratischen Raums V und P ein singulärer Punkt von V mit $P \notin \mathcal{O}$. Es sei $\overline{V} = P^\perp/P$ und auf $\overline{V}$ sei eine quadratische Form definiert durch $\overline{Q}(\overline{x}) := Q(x)$. Dann gilt:*

- (i) Die Menge $\bar{\mathcal{O}} := \{ \langle \bar{x} \rangle \mid \langle x \rangle \in \mathcal{O}, x \in P^\perp \}$ ist ein Ovoid in $\bar{V}$.
(ii) Sei f eine Semiähnlichkeit von V mit $f(P) = P$ und $f(\mathcal{O}) = \mathcal{O}$. Definiere $\bar{f}: \bar{V} \rightarrow \bar{V}$, $\bar{v} \mapsto \overline{f(v)}$. Dann ist $\bar{f}(\bar{\mathcal{O}}) = \bar{\mathcal{O}}$.

Beweis. (i) Für alle $\langle \bar{x} \rangle \in \bar{\mathcal{O}}$ ist $\bar{Q}(\bar{x}) = Q(x) = 0$. Wegen $P \notin \mathcal{O}$, ist $\langle \bar{x} \rangle \neq 0$ für alle $\langle \bar{x} \rangle \in \bar{\mathcal{O}}$.

Sei W ein maximaler total singulärer Teilraum von $\bar{V}$. Es ist zu zeigen, dass es genau ein $\langle \bar{x} \rangle \in \bar{\mathcal{O}}$ gibt mit $\bar{x} \in W$.

Definiere $W' := \{ v \in P^\perp \mid \bar{v} \in W \}$. Dann ist W' total singulär und es gilt $\overline{W'} = W$.

W' ist maximaler total singulärer Teilraum von V . Denn ist $y \in V$ mit $Q(y) = 0$ und $y \perp v'$ für alle $v' \in W'$, so ist $y \in P^\perp$, da $P \subset W'$. Außerdem gilt $\bar{y} \perp v$ für alle $v \in W$, also $\bar{y} \in W$. Das heißt $y \in W'$.

Da W' maximaler total singulärer Teilraum von V ist, gibt es ein $x \in W'$ mit $\langle x \rangle \in \mathcal{O}$. Es folgt $\langle \bar{x} \rangle \in \bar{\mathcal{O}}$ und $\bar{x} \in W$.

$\mathcal{O}$ enthält offensichtlich höchstens einen singulären Punkt aus W , da $0 \neq (x, y) = (\bar{x}, \bar{y})$ für alle $\langle x \rangle, \langle y \rangle \in \mathcal{O}$.

- (ii) $\bar{f}$ ist wohldefiniert, da $f(P) = P$ ist. Weil f Semiähnlichkeit ist, folgt $f(P^\perp) = f(P)^\perp P^\perp$. Daraus ergibt sich $\bar{f}(\bar{\mathcal{O}}) = \bar{\mathcal{O}}$. □

1.3 Die Kleinkorrespondenz

Die Kleinkorrespondenz ist eine inklusionserhaltende Abbildung zwischen den Teilräumen eines vierdimensionalen K -Vektorraums V und total ausgearteten Teilräumen eines 6-dimensionalen K -Raums W vom Typ $V^+(6, q)$. Dabei werden Punkte und Ebenen von $\mathcal{P}(V)$ auf maximale total singuläre Teilräume von W und Geraden von $\mathcal{P}(V)$ auf singuläre Punkte abgebildet. Für uns ist die Kleinkorrespondenz deshalb interessant, weil sie eine Bijektion zwischen den Spreads von V und den Ovoiden von W liefert. Eine genauere Beschreibung der Kleinkorrespondenz ist in [Tay92, Kap. 12] zu finden.

Definition 1.3.1. Sei V ein $\text{GF}(q)$ -Raum und $\dim V = 2n$. Eine Menge $\mathcal{S}$ von n -dimensionalen Teilräumen von V heißt genau dann Spread, wenn

- (i) $V = \bigcup_{U \in \mathcal{S}} U$ und
(ii) $U \oplus W = V$ für alle $U, W \in \mathcal{S}$ mit $U \neq W$

Lemma 1.3.2. Ist V ein $2n$ -dimensionaler $\text{GF}(q)$ -Raum und $\mathcal{S}$ ein Spread von V , so ist $|\mathcal{S}| = q^n + 1$.

Beweis. Aus der Definition der Spreads folgt direkt, dass $V = \{0\} \cup \bigcup_{U \in \mathcal{S}} U \setminus \{0\}$ ist. Das heißt $q^{2n} = |V| = 1 + |\mathcal{S}| \cdot (q^n - 1)$ und somit ist $|\mathcal{S}| = \frac{q^{2n}-1}{q^n-1} = q^n + 1$. □

Sei nun V ein K -Vektorraum mit $\dim(V) = 4$ und $\Lambda_2 V$ das äußere Quadrat von V . Ist $(e_1, \dots, e_n)$ eine Basis von V , so ist $\{e_i \wedge e_j \mid i < j\}$ eine Basis von $\Lambda_2 V$ und durch

$$Q\left(\sum_{i < j} x_{i,j} e_i \wedge e_j\right) := x_{1,2}x_{3,4} - x_{1,3}x_{2,4} + x_{1,4}x_{2,3}$$

lässt sich eine quadratische Form auf $\Lambda_2 V$ definieren. $(\Lambda_2 V, Q)$ ist nicht ausgeartet und ist $K = \text{GF}(q)$, so ist $(\Lambda_2 V, Q) \simeq V^+(6, q)$.

Lemma 1.3.3. *Ist $\xi \in \Lambda_2 V$, so ist $Q(\xi) = 0$ genau dann, wenn es $v, w \in V$ gibt mit $\xi = v \wedge w$.*

Beweis. „ $\Leftarrow$ “: Ist $v = \sum_{i=1}^4 a_i e_i$ und $w = \sum_{i=1}^4 b_i e_i$ dann ist

$$\xi = v \wedge w = \sum_{i < j} (a_i b_j - a_j b_i) e_i \wedge e_j$$

Durch Einsetzen in die oben definierte quadratische Form Q rechnet man aus, dass $Q(\xi) = 0$ ist.

„ $\Rightarrow$ “: Sei $\xi = \sum_{i < j} x_{ij} e_i \wedge e_j \neq 0$. Dann gibt es $k < l$ mit $x_{kl} \neq 0$. Definiere

$$v := \sum_{i=1}^4 x_{ik} e_i \quad \text{und} \quad w := \sum_{i=1}^4 x_{il} e_i,$$

wobei $x_{ii} := 0$ für alle i und $x_{ij} := -x_{ji}$, falls $i > j$. Dann gilt

$$v \wedge w = \sum_{i < j} \underbrace{(x_{ik}x_{jl} - x_{jk}x_{il})}_{=: a_{ijkl}} e_i \wedge e_j$$

Falls i, j, k, l nicht paarweise verschieden sind, ergibt sich durch einfache Rechnung, dass $a_{ijkl} = x_{ij}x_{kl}$ ist. Falls i, j, k, l paarweise verschieden sind, folgt $a_{ijkl} = x_{ij}x_{kl}$ daraus, dass $Q(\xi) = 0$, also $x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}$ ist. Damit ist $x_{kl}^{-1}v \wedge w = \xi$. $\square$

Die Menge der singulären Punkte von $\Lambda_2 V$ heißt Kleinquadrik und wird hier mit $\mathcal{K}(V)$ bezeichnet. Außerdem sei in diesem Abschnitt $U_2(V)$ die Menge der zweidimensionalen Teilräume von V

Satz 1.3.4. *Sei V ein K -Raum mit $\dim(V) = 4$. Dann ist die Abbildung*

$$\begin{aligned} \kappa: U_2(V) &\rightarrow \mathcal{K}(V) \\ \langle x, y \rangle &\mapsto \langle x \wedge y \rangle \end{aligned}$$

bijektiv.

Beweis. κ ist wohldefiniert. Denn ist $\langle x, y \rangle = \langle x', y' \rangle$, so gibt es eine 2×2 Matrix $A = (a_{ij})$ über K , so dass $x = a_{11}x' + a_{21}y'$ und $y = a_{12}x' + a_{22}y'$ ist, woraus $x \wedge y = \det(A) x' \wedge y'$ folgt.

Aus Lemma 1.3.3 folgt, dass κ surjektiv ist und dass $\langle x \wedge y \rangle \in \mathcal{K}$ ist für alle zweidimensionalen Teilräume $\langle x, y \rangle$ von V . Beachte dabei, dass $x \wedge y = 0$ ist, genau dann, wenn x und y linear abhängig sind.

Es bleibt zu zeigen, dass κ injektiv ist. Seien $L_1, L_2 \in U_2$. Falls $L_1 \cap L_2 = \{0\}$, so ist $L_1 = \langle u, v \rangle$, $L_2 = \langle u', v' \rangle$ mit linear unabhängigen $u, v, u', v' \in V$. Dann sind auch $u \wedge v, u' \wedge v'$ linear unabhängig, also $\kappa(L_1) \neq \kappa(L_2)$.

Sei nun $0 \neq u \in L_1 \cap L_2$ und $v, v' \in V$ mit $L_1 = \langle u, v \rangle$ und $L_2 = \langle u, v' \rangle$. Ist $\kappa(L_1) = \kappa(L_2)$, also $u \wedge v = au \wedge v'$ für ein $a \in K^*$, dann ist $u \wedge (v - av') = 0$, sodass $u, v - av'$ linear abhängig sind. Es folgt, dass $v' \in \langle u, v \rangle = L_1$. Das heißt $L_1 = L_2$. □

Satz 1.3.5. *Sei V ein Vektorraum mit $\dim(V) = 4$. Dann ist $S \subseteq U_2(V)$ genau dann ein Spread von V , wenn $\kappa(S)$ ein Ovoid von $\Lambda_2 V$ ist.*

Beweis. Zeige: Für $W, W' \in U_2$ gilt: $W \cap W' \neq \{0\} \Leftrightarrow \kappa(W) \perp \kappa(W')$.

Dann folgt die Behauptung daraus, dass Spreads in V und Ovoids in $\Lambda_2 V$ die selbe Größe haben.

„ $\Rightarrow$ “: Ist $U \cap W \neq \{0\}$, dann gibt es ein $u, w, w' \in V$ mit $W = \langle u, w \rangle$ und $W' = \langle u, w' \rangle$. Mit Lemma 1.3.3 folgt:

$$\begin{aligned} (u \wedge w, u \wedge w') &= Q((u \wedge w) + (u \wedge w')) - Q(u \wedge w) - Q(u \wedge w') \\ &= Q(u \wedge (w + w')) = 0 \end{aligned}$$

„ $\Leftarrow$ “: Ist nun $W \cap W' = \{0\}$, so gibt es eine Basis $(v_1, \dots, v_4)$ von V mit $W = \langle v_1, v_2 \rangle$ und $W' = \langle v_3, v_4 \rangle$.

Angenommen $v_1 \wedge v_2 \perp v_3 \wedge v_4$. Dann ist $Q((v_1 \wedge v_2) + (v_3 \wedge v_4)) = 0$ und nach Lemma 1.3.3 gibt es $x = \sum a_i v_i$ und $y = \sum b_i v_i$ in V mit

$$\begin{aligned} (v_1 \wedge v_2) + (v_3 \wedge v_4) &= x \wedge y \\ &= \sum_{i < j} (a_i b_j - a_j b_i) v_i \wedge v_j \end{aligned}$$

Es folgt: (i) $a_1 b_2 - a_2 b_1 = 1$ und (ii) $a_3 b_4 - a_4 b_3 = 1$. Das heißt, $b_3 \neq 0$ oder $b_4 \neq 0$. Außerdem ist $a_1 b_4 = a_4 b_1$ und $a_2 b_4 = a_4 b_2$. Somit gilt $a_2 b_4 b_1 = a_4 b_1 b_2 = a_1 b_4 b_2$ und falls $b_4 \neq 0$ ist folgt damit $a_2 b_1 = a_1 b_2$. Das ist ein Widerspruch zu (i).

Falls $b_3 \neq 0$ ist, ergibt sich der Widerspruch analog aus $a_1 b_3 = a_3 b_1$ und $a_2 b_3 = a_3 b_2$. □

Definiert man für $f \in \text{GL}(V)$

$$\begin{aligned} \Lambda_2 f: \Lambda_2 V &\rightarrow \Lambda_2 V \\ \sum_{i < j} a_{ij} e_i \wedge e_j &\mapsto \sum_{i < j} a_{ij} f(e_i) \wedge f(e_j), \end{aligned}$$

dann ist $\Lambda_2 f \in \text{GL}(\Lambda_2 V)$. Nach Satz [Tay92, 12.17] gilt für alle $\xi \in \Lambda_2 V$:

$$Q((\Lambda_2 f)(\xi)) = \det(f)Q(\xi)$$

Das heißt, $\Lambda_2 f \in \text{GO}(\Lambda_2 V)$. Damit ist durch $f \mapsto \Lambda_2 f$ ein Homomorphismus von $\text{GL}(V)$ nach $\text{GO}(\Lambda_2 V)$ definiert.

Lemma 1.3.6. *Sei $\mathcal{S}$ ein Spread von V , $f \in \text{GL}(V)$ und $\mathcal{O} = \kappa(\mathcal{S})$. Dann ist $\mathcal{S}$ genau dann invariant unter f , wenn $\mathcal{O}$ invariant unter $\Lambda_2 f$ ist.*

Beweis. Sei $\langle x \wedge y \rangle \in \mathcal{O}$ mit $\langle x, y \rangle \in \mathcal{S}$. Dann ist

$$\Lambda_2 f(\langle x \wedge y \rangle) = \langle \Lambda_2 f(x \wedge y) \rangle = \langle f(x) \wedge f(y) \rangle = \kappa(\langle f(x), f(y) \rangle).$$

Also $\Lambda_2 f(\langle x \wedge y \rangle) \in \mathcal{O}$ genau dann, wenn $f(\langle x, y \rangle) \in \mathcal{S}$. □

Satz 1.3.7 ([Tay92, Thm. 12.20.]). *Die Abbildung*

$$\kappa: \text{SL}(V) \rightarrow \Omega(\Lambda_2(V)), \quad f \mapsto \Lambda_2 f$$

ist ein Epimorphismus mit Kern $\{\pm 1\}$. Dabei bezeichnet $\Omega(\Lambda_2(V))$ die Kommutatorgruppe von $\Lambda_2(V)$.

Anwendungsbeispiel

Die Sätze dieses Kapitels können verwendet werden um mittels der Kleinkorrespondenz aus Wissen über Spreads in vierdimensionalen Räumen Informationen über Ovoide in $V^+(6, q)$ und $V^+(8, q)$ zu gewinnen. Beispielsweise kann man in einigen Fällen ausschließen, dass bestimmte orthogonale Abbildungen Automorphismen von Ovoiden sind. Für einige orthogonale Abbildungen f kann gezeigt werden, dass alle f -invarianten Ovoide bestimmte Fixpunkte von f enthalten.

Bemerkung. *Sei $V = \text{GF}(q)^4$ und $a \in \mathbb{N}$ ungerade. Dann induziert der Epimorphismus κ aus Satz 1.3.7 eine Bijektion zwischen $\{g \in \text{SL}(V) \mid \text{ord}(g) = a\}$ und $\{f \in \Omega(\Lambda_2(V)) \mid \text{ord}(f) = a\}$.*

Beweis. Sei $f \in \Omega(\Lambda_2(V))$ mit $\text{ord}(f) = a$ ungerade, dann ist f ein Quadrat in $\Omega(\Lambda_2(V))$. Nach [Tay92, S. 164] gilt $\Omega(\Lambda_2(V)) = \langle g^2 \mid g \in \Omega(\Lambda_2(V)) \rangle$. Das heißt $f \in \Omega(\Lambda_2(V))$. Somit gibt es ein $g \in \text{SL}(V)$ mit $f = \Lambda_2 g$. Da $\text{Kern}(\kappa) = \{\pm 1\}$ ergibt sich $g^a = \pm 1$. Falls $g^a = -1$, ist $\text{ord}(-g) = a$ und $f = \Lambda_2(-g)$. Ist umgekehrt $h \in \text{SL}(V)$ mit $\text{ord}(h)$ ungerade, so ist $\text{ord}(\Lambda_2 h) = \text{ord}(h)$. □

Ist nun $f = \Lambda_2 g$ mit $g \in V = \text{GF}(q)^4$, dann gibt es nach Lemma 1.3.6 genau dann ein f -invariantes Ovoid von $\Lambda_2(V)$, wenn es einen g -invarianten Spread von V gibt. Kennt man also die Automorphismen der Spreads von $\text{GF}(q)^4$, so kennt man nach obiger Bemerkung die Automorphismen ungerader Ordnung von Ovoiden in $\Lambda_2(V)$.

Beispiel. Sei $\mathcal{S}$ ein Spread von $\text{GF}(7)^4$ und $g \in \text{GL}(4, 7)$ mit $\text{ord}(g) = 7$ und $g(\mathcal{S}) = \mathcal{S}$. Aus [MR95, CD98, Dema] folgt, dass es eine Zerlegung $V = V_1 \oplus V_2$ in g -invariante Teilräume V_1, V_2 gibt, sodass f auf beiden Teilräumen das Minimalpolynom $(X - 1)^2$ hat. Wir kennen also die Normalformen der Automorphismen der Ordnung 7 von $\mathcal{S}$. Diese Information verwenden wir nun, um die Normalformen orthogonaler Abbildungen der Ordnung 7 zu berechnen, die ein Ovoid von $\Lambda_2(V) \simeq V^+(6, 7)$ invariant lassen.

Sei $\mathcal{O}$ ein Ovoid von $W = \Lambda_2 V$ und $f \in \text{O}(W)$ der Ordnung 7, so dass $f(\mathcal{O}) = \mathcal{O}$ ist. Da $\text{ord}(f)$ ungerade ist, gibt es ein $g \in \text{SL}(V)$ mit $\text{ord}(g) = \text{ord}(f) = 7$ und $\Lambda_2 g = f$. Nach Satz 1.3.4 und 1.3.5 existiert ein Spread $S \subseteq V$ mit $\kappa(S) = \mathcal{O}$, dabei ist $g(S) = S$. Nun verwenden wir die obige Feststellung über Spreads in $\text{GF}(7)^4$: Es gibt also g -invariante Teilräume V_1, V_2 von V , so dass $V = V_1 \oplus V_2$ und g auf V_i das Minimalpolynom $(X - 1)^2$ hat.

Sei $\{e_1, e_2\}$ g -Jordanbasis von V_1 und $\{e_3, e_4\}$ g -Jordanbasis von V_2 , es gelte also $g(e_1) = e_1 + e_2$ und $g(e_2) = e_2$ sowie $g(e_3) = e_3 + e_4$ und $g(e_4) = e_4$. Dann ist $W_1 := \langle e_1 \wedge e_3, e_2 \wedge e_4, e_1 \wedge e_4 + e_2 \wedge e_3 \rangle$ ein von $e_1 \wedge e_3$ erzeugter zyklischer f -Modul, und auf $W_2 := \langle e_1 \wedge e_2, e_3 \wedge e_4, e_1 \wedge e_4 - e_2 \wedge e_3 \rangle$ ist f die Identität.

Das heißt, es gibt eine Basis von W , bezüglich der $\Lambda_2 g$ die folgende Jordannormalform hat:

$$(1.1) \quad \left(\begin{array}{cc|cc} 1 & & & & \\ 1 & 1 & & & \\ & 1 & 1 & & \\ \hline & & & 1 & \\ & & & & 1 & 1 \end{array} \right)$$

Ist also $f \in \text{O}(V^+(6, 7))$ der Ordnung 7 und $\mathcal{O}$ ein f -invariantes Ovoid, dann hat f die obige Normalform.

Betrachten wir nun Abbildungen $h \in \text{O}(V^+(8, q))$, so können wir mit Hilfe der Projektion aus Satz 1.2.4 feststellen, dass manche singulären Punkte in jedem h -invarianten Ovoid enthalten sind. Sei $W = V^+(8, q)$, $h \in \text{O}(W)$ und P ein singulärer Punkt von W mit $h(P) = P$. Wie auf Seite 9 definieren wir $\overline{W} := (W \cap P^\perp)/P$, und $\overline{h}: \overline{W} \rightarrow \overline{W}$ durch $\overline{v} \mapsto \overline{h(v)}$. Falls es keine Ovoide von $\overline{W}$ gibt, die invariant unter $\overline{h}$ sind, so folgt mit Satz 1.2.4, dass $P \in \mathcal{O}$ ist für alle Ovoide $\mathcal{O}$ von W .

Gibt es einen singulären Punkt P' in $W \cap P^\perp$ mit $h(P') = P'$, so dass es auch zur Abbildung $\tilde{h}: (W \cap P'^\perp)/P' \rightarrow (W \cap P'^\perp)/P'$, $v + P' \mapsto h(v) + P'$ keine $\tilde{h}$ -invarianten Ovoide gibt, dann enthält jedes h -invariante Ovoid die Punkte P und P' . Diese sind aber orthogonal zueinander. Es kann also kein h -invariantes Ovoid geben.

Beispiel. Sei $h \in \text{O}(V^+(8, 7))$ der Ordnung 7 und es gebe eine Zerlegung $U_1 \perp U_2$ von $V^+(8, 7)$ in h -invariante Teilräume. Dabei sei $h|_{U_1} \neq \mathbb{1}$ und das Minimalpo-

lynom m von $h|_{U_1}$ sei ungleich $(X - 1)^3$. (Die möglichen Normalformen für h , sind – in der Notation von Kapitel 3 – in Tabelle A.1 nachzulesen.)

Sei P ein singulärer Punkt von U_2 mit $h(P) = P$. Definiere wie in Satz 1.2.4 $\bar{h}$ auf $P^\perp/P$ durch $\bar{v} \mapsto \overline{h(v)}$. Dann ist

$$P^\perp/P = \overline{U_1} \perp \overline{U_2}$$

mit $\bar{h}$ -invarianten Räumen $\overline{U_1}, \overline{U_2}$. Dabei hat $\bar{h}|_{\overline{U_1}}$ das Minimalpolynom $m \neq (X - 1)^3$. Insbesondere hat die Jordan-Normalform nicht die Gestalt (1.1) aus obigem Beispiel, sodass es keine Ovoide gibt, welche invariant unter $\bar{h}$ sind. Nach Satz 1.2.4 gibt es folglich keine Ovoide, die invariant unter h sind und den singulären Punkt P nicht enthalten. Falls es ein h -invariantes Ovoid von $V^+(8, 7)$ gibt, so enthält dieses also alle singulären Fixpunkte von U_2 . Insbesondere gibt es keine h -invarianten Ovoide, falls U_2 zwei singuläre Fixpunkte P_1, P_2 mit $P_1 \perp P_2$ enthält.

Kapitel 2

Die bekannten Ovoide in $V^+(8, q)$

Es sind mehrere Konstruktionen für Ovoide in $V^+(8, q)$ bekannt. Diese führen zu mehreren Serien inäquivalenter Ovoide. Außerdem ist ein sporadisches Ovoid bekannt. In diesem Abschnitt werden kurz die Konstruktionen dieser Ovoide angegeben. Genauer findet sich in [CKW88, Kan82a, Moo93a].

2.1 Unitäre Ovoide

Für $q \equiv 0, 2 \pmod{3}$ definiert Kantor in [Kan82a, 4.] die unitären Ovoide von $V^+(8, q)$ wie folgt.

Sei p prim, $n \in \mathbb{N}$ und $q = p^n$ mit $q \equiv 0 \pmod{3}$ oder $q \equiv 2 \pmod{3}$. Sei weiterhin $K := \text{GF}(q)$ und $L := \text{GF}(q^2)$. Für $a \in L$ sei $\bar{a} := a^q$. Dann sind

$$T: L \rightarrow K, \quad x \mapsto a + \bar{a} \quad \text{und} \quad N: L \rightarrow K, \quad x \mapsto a\bar{a}$$

die Spur- und die Normabbildung. Es sei V der durch

$$V := \left\{ \begin{pmatrix} \alpha & \beta & c \\ \gamma & a & \bar{\beta} \\ b & \bar{\gamma} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta, \gamma \in L, a, b, c \in K, a + T(\alpha) = 0 \right\}$$

definierte K -Vektorraum. Sei weiterhin $Q: V \rightarrow K$ gegeben durch

$$Q(A) := \sum_{i < j} (a_{ij}a_{ji} - a_{ii}a_{jj}).$$

Dann ist Q eine quadratische Form auf V und ist $A = \begin{pmatrix} \alpha & \beta & c \\ \gamma & a & \bar{\beta} \\ b & \bar{\gamma} & \bar{\alpha} \end{pmatrix} \in V$, so gilt

$$Q(A) = \alpha^2 + \alpha\bar{\alpha} + \bar{\alpha}^2 + T(\beta\gamma) + bc.$$

Falls $q \equiv 2 \pmod{3}$, dann ist V isomorph zu $V^+(8, q)$. Ist $q \equiv 0 \pmod{3}$, so ist

$$\text{Rad}(V) = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle \text{ und } V/\text{Rad}(V) \text{ ist isomorph zu } V(7, q).$$

Sei nun

$$X_\infty := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{und} \quad X(\rho, \sigma) := \begin{pmatrix} \bar{\rho} & \bar{\rho}\sigma & N(\rho) \\ \bar{\sigma} & N(\sigma) & \rho\bar{\sigma} \\ 1 & \sigma & \rho \end{pmatrix}$$

für $\rho, \sigma \in L$. Definiert man

$$\mathcal{O} := \{ \langle X(\rho, \sigma) \rangle \mid T(\rho) + N(\sigma) = 0 \} \cup \{ \langle X_\infty \rangle \},$$

dann gilt:

- (i) Falls $p \neq 3$ ist, so ist $\mathcal{O}$ ein Ovoid von V .
- (ii) Ist $p = 3$ und $\bar{\mathcal{O}}$ das Bild von $\mathcal{O}$ unter der Projektion $V \rightarrow V/\text{Rad}(V)$ dann ist $\bar{\mathcal{O}}$ ein Ovoid von $V/\text{Rad}(V)$.

Das so konstruierte $\mathcal{O}$ heißt *unitäres* Ovoid.

Jeder quadratische Raum vom Typ $V(2n-1, q)$ lässt sich in einen Raum vom Typ $V^+(2n, q)$ einbetten. Ovoids von $V(2n-1, q)$ bestehen – ebenso wie Ovoids von $V^+(2n, q)$ – aus jeweils $q^{n-1} + 1$ paarweise nicht orthogonalen singulären Punkten (vgl. 1.2.3). Also lässt sich jedes Ovoid von $V(2n-1, q)$ in einen Raum vom Typ $V^+(2n, q)$ einbetten, so dass es auch dort ein Ovoid ist. Insbesondere gibt es eine Einbettung des unitären Ovoids $\bar{\mathcal{O}}$ für $p = 3$ in den Raum $V^+(8, q)$, ohne dass die Ovoid-Eigenschaft verloren geht.

2.2 Ree-Tits Ovoids

Weitere Ovoids von $V(7, q)$ sind die Ree-Tits Ovoids [Tit61]. Diese Ovoids sind auch bei Kantor in [Kan82a, 6.] beschrieben.

Sei $q = 3^{2e-1}$ mit $1 \leq e \in \mathbb{N}$ und $K := \text{GF}(q)$. Für $a \in K$ sei $a^\sigma := a^{3^e}$. Definiere $V := K^7$ und eine quadratische Form Q auf V durch

$$Q(x) := x_1x_7 + x_2x_6 + x_3x_5 + x_4^2.$$

Des Weiteren sei für $x, y, z \in K$:

$$\begin{aligned} u(x, y, z) &:= x^2y - xz + y^\sigma - x^{\sigma+3} \\ v(x, y, z) &:= x^\sigma y^\sigma - z^\sigma + xy^2 + yz - x^{2\sigma+3} \\ w(x, y, z) &:= xz^\sigma - x^{\sigma+1}y^\sigma - x^{\sigma+3}y + x^2y^2 - y^{\sigma+1} - z^2 + x^{2\sigma+4}. \end{aligned}$$

Dann ist

$$\begin{aligned} \mathcal{O} &:= \{ \langle (1, x, y, z, u(x, y, z), v(x, y, z), w(x, y, z)) \rangle \mid x, y, z \in K \} \\ &\quad \cup \{ \langle (0, 0, 0, 0, 0, 0, 1) \rangle \} \end{aligned}$$

ein Ovoid von V .

2.3 Desarguessche Ovoids

Bei Kantor ([Kan82a, 7.] und [Kan82b, 8., 12.]) ist folgende Beschreibung des desarguesschen Ovoids in $V^+(8, q)$ zu finden:

Es sei q eine Zweipotenz, $K = \text{GF}(q)$ und $L = \text{GF}(q^3)$. Weiter seien

$$T: L \rightarrow K, \quad x \mapsto x + x^q + x^{q^2} \quad \text{und} \quad N: L \rightarrow K, \quad x \mapsto x^{q^2+q+1}$$

die Spur- und die Normabbildung. Betrachte den K -Vektorraum

$$V := K \oplus L \oplus L \oplus K.$$

Definiert man $Q: V \rightarrow K$ durch $Q(a, b, c, d) := ad + T(bc)$, so ist Q eine quadratische Form und V mit dieser Form ein Raum vom Typ $V^+(8, q)$. Durch

$$\mathcal{O} := \left\{ \left\langle (1, t, t^{q+q^2}, N(t)) \right\rangle \mid t \in L \right\} \cup \{ \langle (0, 0, 0, 1) \rangle \}$$

ist ein Ovoid von V definiert.

2.4 Das Ovoid von Dye

Das Ovoid von Dye [Dye77, 4.] ist ein Ovoid von $V^+(8, 8)$. Die Konstruktion dieses Ovoids ist ebenfalls bei Kantor in [Kan82a, 8.] angegeben.

Sei $\mathcal{O} := \{ \langle e_1 \rangle, \dots, \langle e_9 \rangle \}$ ein Ovoid von $V^+(8, 2)$. (Bis auf Äquivalenz gibt es genau ein Ovoid in $V^+(8, 2)$, vgl. [Kan82a, 3.]). Sei $a \in \text{GF}(8)$ mit $a^3 + a^2 + 1 = 0$. Wähle eine Einbettung von $V^+(8, 2)$ in den Raum $V^+(8, 8)$. Dann definiert

$$\begin{aligned} \mathcal{O} := & \{ \langle e_i \rangle \mid 1 \leq i \leq 9 \} \\ & \cup \{ \langle ae_i + a^2e_j + a^4e_k \rangle \mid 1 \leq i, j, k \leq 9, i, j, k \text{ paarw. versch.} \} \end{aligned}$$

ein Ovoid von $V^+(8, 8)$.

2.5 Ovoids aus dem Wurzelsystem E_8

In diesem Abschnitt werden zuerst die Ovoids beschrieben, die Conway, Kleidman und Wilson in [CKW88] aus dem Wurzelsystem vom Typ E_8 konstruieren. Im Anschluss findet sich die Verallgemeinerung dieser Konstruktion von Moorhouse [Moo93a].

Sei $L \subseteq \mathbb{R}^8$ das Gitter zum Wurzelsystem vom Typ E_8 :

$$L = \left\{ \frac{1}{2}(a_1, \dots, a_8) \mid a_i \in \mathbb{Z}, a_i \equiv a_j \pmod{2} \text{ für alle } i, j, \sum_{i=1}^8 a_i \equiv 0 \pmod{4} \right\}.$$

Sei weiterhin p eine Primzahl. Dann ist $\bar{L} := L/pL$ ein 8-dimensionaler Vektorraum über $\text{GF}(p)$. Für $v \in L$ sei $\bar{v} := v + vL \in \bar{L}$. Es bezeichne hier $(\cdot, \cdot)$ das euklidische Skalarprodukt auf $\mathbb{R}^8$. Für alle $v \in L$ gilt $(v, v) \in 2\mathbb{Z}$, daher können wir folgende Abbildung definieren:

$$Q: \bar{L} \rightarrow \text{GF}(p), \quad \bar{v} \mapsto \overline{\frac{1}{2}(v, v)}.$$

Q ist eine quadratische Form auf $\bar{L}$ und $\bar{L} \simeq V^+(8, p)$. Dies führt nun zu zwei Konstruktionen für Ovoide.

Die binären Ovoide: Ist p ungerade und $x \in L$ mit $(x, x) = 2p$, dann ist

$$(2.1) \quad \mathcal{O}_{2,p}(x) := \{ \langle \bar{v} \rangle \mid v \in L, (v, v) = 2p, v \equiv x \pmod{2L} \}$$

ein Ovoid von $\bar{L}$.

Die ternären Ovoide: Ist $p \geq 5$ und $x \in L$ mit $(x, x) = 4p$, so ist

$$(2.2) \quad \mathcal{O}_{3,p}(x) := \{ \langle \bar{v} \rangle \mid v \in L, (v, v) = 4p, v \equiv x \pmod{3L} \}$$

ein Ovoid von $\bar{L}$.

In diesen Familien finden sich zwei zuvor bekannte „sporadische“ Ovoide wieder. Für $p = 7$ erhält man aus der ternären Konstruktion das Ovoid von Shult [Shu85]. Im Fall $p = 5$ gehört das Ovoid von Cooperstein [Coo90] zur Familie der ternären Ovoide.

Die ternären Ovoide zerfallen für $p \equiv 2 \pmod{3}$ in zwei Serien. Im Fall $p = 5$ ist dabei das Ovoid aus der ersten ternären Serie zum binären Ovoid äquivalent. Conway, Kleidman und Wilson haben jedoch gezeigt, dass für größere p die binäre Konstruktion Ovoide liefert, die nicht äquivalent zu Ovoiden der ersten ternären Serie sind ([CKW88, 5.]).

Moorhouse hat die obigen Konstruktionen von Conway, Kleidman und Wilson verallgemeinert. Für je zwei verschiedene Primzahlen r, p erhält er Ovoide $\mathcal{O}_{r,p}(x)$ aus dem Gitter L , siehe [Moo93a] und [Moo93b].

Seien p, r prim und $p \neq r$. Für $i \in \mathbb{N}$ mit $1 \leq i \leq \lfloor \frac{r}{2} \rfloor$ sei n_i die natürliche Zahl, für die $1 \leq n_i \leq \lfloor \frac{r}{2} \rfloor$ und $i^2 n_i^2 \equiv 1 \pmod{r}$ gilt. Definiere

$$S_{r,p} := \bigcup_{i=1}^{\lfloor r/2 \rfloor} \{ n_i v \mid v \in L, (v, v) = 2i(r-i)p \} \quad \text{und} \\ S'_{r,p} := \bigcup_{i=1}^{\lfloor r/2 \rfloor} \{ p n_i v \mid v \in L, (v, v) = 2i(r-i)/p \} \subseteq S_{r,p}.$$

Sei nun $x \in L$, so dass $-\frac{p}{2}(x, x) \not\equiv 0 \pmod{r}$ und ein Quadrat modulo r ist. Sei weiterhin $1 \leq n_x \leq \lfloor \frac{r}{2} \rfloor$ und $n_x^2(x, x) \equiv -2p \pmod{r}$. Setze

$$\mathcal{O}_{r,p}(x) := \{ \langle \bar{v} \rangle \mid v \in S_{r,p} \setminus pL, v \equiv n_x x \pmod{rL} \}.$$

Moorhouse hat gezeigt, dass $\mathcal{O}_{r,p}(x)$ genau dann ein Ovoid von $\bar{L}$ ist, wenn $(n_x x + rL) \cap S'_{r,p} = \emptyset$ ist. Dabei ist im Fall $r < p$ die Bedingung $(n_x x + rL) \cap S'_{r,p} = \emptyset$ immer erfüllt und falls $r > p$ ist, so existiert ein geeignetes x , so dass $(n_x x + rL) \cap S'_{r,p} = \emptyset$ gilt.

Es ist unklar, wie viele dieser Ovoide zueinander oder zu einem Ovoid der binären oder ternären Serie äquivalent sind. Für $p \leq 11$ und $r \leq 13$ tritt nur ein Ovoid auf, das nicht schon zur binären oder ternären Familie gehört. Es handelt sich dabei um ein Ovoid in $V^+(8, 11)$.

Kapitel 3

Normalformen orthogonaler Abbildungen

In diesem Kapitel befassen wir uns mit Normalformen orthogonaler Abbildungen. Ziel ist es, bis auf Konjugation die zyklischen Gruppen bestimmter Ordnungen in $O(V^+(8, q))$ berechnen zu können. Im ersten Abschnitt stellen wir fest, welches die Normalformen orthogonaler Abbildungen sind. Dann untersuchen wir die Möglichkeiten, zu einer linearen Abbildung $f \in GL(V)$ mit gegebener Normalform eine quadratischen Form auf V zu definieren, so dass f eine orthogonale Abbildung ist. Wir verwenden dabei die elementare Darstellung von Huppert [Hup80a, Hup80b]. Andere Zugänge zur Berechnung von Konjugiertenklassen in orthogonalen Gruppen finden sich beispielsweise in [Zas58] und [Wal63b].

3.1 Orthogonale Zerlegungen

In diesem Abschnitt beschäftigen wir uns damit, welche Normalformen linearer Abbildungen als Normalformen orthogonaler Abbildungen auftreten können.

Huppert teilt die bezüglich einer orthogonalen Abbildung orthogonal unzerlegbaren Räume in drei Klassen ein. Da sich diese Klasseneinteilung auf Ähnlichkeiten verallgemeinern lässt, betrachten wir in diesem Abschnitt zunächst auch Ähnlichkeiten. Bei der folgenden Untersuchung der einzelnen Typen orthogonal unzerlegbarer Räume beschränken wir uns dann jedoch auf die Betrachtung orthogonaler Abbildungen.

Definition 3.1.1. Sei $V \neq \{0\}$ ein K -Vektorraum und $g: V \rightarrow V$ eine lineare Abbildung.

- (i) V heißt *irreduzibler g -Modul*, wenn V außer $\{0\}$ und V keinen g -invarianten Teilraum enthält.
- (ii) V ist ein *unzerlegbarer g -Modul*, wenn es keine Teilräume V_1, V_2 von V gibt, so dass $V = V_1 \oplus V_2$ und $g(V_i) \subseteq V_i \neq \{0\}$.

- (iii) Ist eine symmetrische Bilinearform auf V definiert, so heißt V *orthogonal unzerlegbarer g -Modul*, wenn es keine Teilräume V_1, V_2 von V gibt, so dass $V = V_1 \perp V_2$ und $g(V_i) \subseteq V_i \neq \{0\}$ ist.

Bemerkung. (i) Ist $V = V_1 \oplus V_2$ ein orthogonal unzerlegbarer f -Modul mit f -invarianten Teilräumen V_1 und V_2 , so sind V_1, V_2 ausgeartet. Denn andernfalls wäre $V = V_i \perp V_i^\perp$ für ein $i \in \{1, 2\}$ eine Zerlegung von V in f -invariante Teilräume.

- (ii) Insbesondere ist $\text{Rad}(V_i)$ für $i \in \{1, 2\}$ ein nichttrivialer f -invarianter Teilraum von V_i . Ist p^n das Minimalpolynom von $f|_{V_i}$ mit irreduziblem p , dann enthält $\text{Rad}(V_i)$ den irreduziblen Teilmodul $p^{n-1}(f)(V_i)$ von V_i .

Definition 3.1.2. Sei K ein Körper und $p = \sum_{i=0}^m a_i X^i \in K[X]$ ein Polynom vom Grad m mit $p(0) \neq 0$.

- (i) Für $s \in K \setminus \{0\}$ definiere

$$p^{*s} := \frac{1}{p(0)} X^m \cdot p\left(\frac{s}{X}\right) = \frac{1}{a_0} \cdot \sum_{i=0}^m a_i s^i X^{m-i}.$$

Falls $s = 1$ ist, so schreiben wir p^* für p^{*s} .

- (ii) p heißt *symmetrisch*, wenn $p^* = a_m^{-1} \cdot p$ ist.

Es gilt $(p^{*s})^{*s} = a_m^{-1} p$, denn

$$\begin{aligned} (p^{*s})^{*s} &= \frac{1}{p^{*s}(0)} X^m \cdot p^{*s}\left(\frac{s}{X}\right) = \frac{1}{p^{*s}(0)} X^m \cdot \frac{1}{p(0)} \left(\frac{s}{X}\right)^m p(X) \\ &= a_m^{-1} \frac{p(0)}{s^m} \cdot \frac{1}{p(0)} \cdot s^m p(X) = a_m^{-1} p. \end{aligned}$$

Ist $q \in K[X]$ ein weiteres Polynom mit $q(0) \neq 0$, so ist $(pq)^{*s} = p^{*s} q^{*s}$.

Lemma 3.1.3 (analog [Hup80a, 1.6 a]). Sei V ein quadratischer K -Raum und $f \in \text{GO}(V)$ eine Ähnlichkeit mit Multiplikator s . Sei außerdem $p \in K[X]$ mit $p(0) \neq 0$ und sei $n := \deg(p)$, dann gilt für alle $v, w \in V$

$$(p(f)(v), w) = p(0) (v, f^{-n} p^{*s}(f)(w)).$$

Beweis. Es sei $p = \sum_{i=0}^n a_i X^i$. Dann gilt

$$\begin{aligned} (p(f)(v), w) &= \sum_{i=0}^n a_i (f^i(v), w) = \sum_{i=0}^n a_i s^i (v, f^{-i}(w)) \\ &= (v, \sum_{i=0}^n a_i s^i f^{-i}(w)) = p(0) (v, f^{-n} p^{*s}(f)(w)). \end{aligned}$$

□

Satz 3.1.4 (analog zu [Hup80a, 1.6 b])). Sei V ein K -Vektorraum mit Bilinearform $(\cdot, \cdot)$ und f eine Ähnlichkeit von V mit Multiplikator s . Seien $p_1, p_2 \in K[X]$ mit $p_1(0) \neq 0$. Sind p_1^{*s} und p_2 teilerfremd und ist $v_i \in \text{Kern } p_i(f)$ für $i \in \{1, 2\}$, dann ist $(v_1, v_2) = 0$.

Beweis. Sind p_1^{*s}, p_2 teilerfremd, so gibt es $q, r \in K[X]$, so dass $1 = rp_1^{*s} + qp_2$. Sei $m := \deg(p_1)$. Es gilt

$$\begin{aligned} 0 &= (p_1(f)(v_1), f^m r(f)(v_2)) = p_1(0) (v_1, f^{-m} p_1^{*s}(f)(f^m r(f)(v_2))) \\ &= p_1(0) (v_1, r(f) p_1^{*s}(f)(v_2) + \underbrace{qp_2(f)(v_2)}_{=0}) = p_1(0) (v_1, (rp_1^{*s} + qp_2)(f)(v_2)) \\ &= p_1(0) (v_1, v_2). \end{aligned}$$

□

Satz 3.1.5 (analog zu [Hup80a, 1.7 b])). Sei V ein nicht ausgearteter quadratischer Raum und $f \in \text{GO}(V)$ eine Ähnlichkeit mit Multiplikator s , so dass V ein zerlegbarer, orthogonal unzerlegbarer f -Modul ist. Ist $V = V_1 \oplus \cdots \oplus V_\ell$ eine Zerlegung in unzerlegbare f -Moduln, dann ist $\ell = 2$ und ist p das Minimalpolynom von $f|_{V_1}$, so ist p^{*s} das Minimalpolynom von $f|_{V_2}$.

Beweis. Für $1 \leq i \leq \ell$ sei $p_i^{k_i}$ das Minimalpolynom von $f|_{V_i}$ mit p_i irreduzibel. Weiterhin sei $k_1 \geq k_i$ für $i \geq 2$. Da V orthogonal unzerlegbar ist, ist jedes V_i ausgeartet, das heißt $\text{Rad}(V_i) \neq \emptyset$. Es folgt

$$p_i(f)^{k_i-1} V_i \subseteq \text{Rad}(V_i) \quad \text{für } 1 \leq i \leq \ell,$$

denn $p_i(f)^{k_i-1} V_i$ ist der einzige minimale nicht triviale f -Teilmodul von V und $\text{Rad}(V_i)$ ist f -invariant. Da V nicht ausgeartet ist, gilt $p_1(f)^{k_1-1}(V_1) \not\subseteq V_j^\perp$ für ein $j \geq 2$. Sei o.B.d.A. $j = 2$.

Sei $v_1 \in V_1$ und $v_2 \in V_2$, so dass $(p_1(f)^{k_1-1}(v_1), v_2) \neq 0$ und sei $m := \deg(p_1)$. Mit Lemma 3.1.3 ergibt sich

$$0 \neq (p_1(f)^{k_1-1}(v_1), v_2) = p_1(0)^{k_1-1} (v_1, f^{-m(k_1-1)} p_1^{*s}(f)^{k_1-1}(v_2)).$$

Also ist $p_1^{*s}(f)^{k_1-1}(V_2) \not\subseteq V_1^\perp$. Insbesondere ist $p_1^{*s}(f)^{k_1-1}(V_2) \neq \{0\}$ und $V_1^\perp \cap V_2 \subsetneq V_2$.

Für alle $w_1 \in V_1$ und $w_2 \in V_2$ gilt

$$0 = (p_1(f)^{k_1}(w_1), w_2) = p_1(0)^{k_1} (w_1, f^{-mk_1} p_1^{*s}(f)^{k_1}(w_2)),$$

so dass $p_1^{*s}(f)^{k_1}(V_2) \subseteq V_1^\perp \cap V_2$ ist. Da $V_1^\perp \cap V_2$ ein echter f -Teilmodul von V_2 ist und p_1^{*s}, p_2 irreduzibel sind, muss $p_1^{*s} = p_2$ gelten. Aus $p_1^{*s}(f)^{k_1-1}(V_2) \neq \{0\}$ und $k_1 \geq k_2$ ergibt sich $k_1 = k_2$.

Im Folgenden wird gezeigt, dass $V_1 \oplus V_2$ nicht ausgeartet ist, woraus $V = V_1 \oplus V_2$ folgt, da V orthogonal unzerlegbar ist. Angenommen es sei $\text{Rad}(V_1 \oplus V_2) \neq \{0\}$. Ist $U \subseteq \text{Rad}(V_1 \oplus V_2)$ ein minimaler nichttrivialer f -Teilmodul von $V_1 \oplus V_2$, dann ist $U \subseteq p_1(f)^{k_1-1}(V_1) \oplus p_2(f)^{k_2-1}(V_2)$. Es gibt also $w_1 \in p_1(f)^{k_1-1}(V_1)$ und $w_2 \in p_2(f)^{k_2-1}(V_2)$, so dass $0 \neq w_1 + w_2 \in \text{Rad}(V_1 \oplus V_2)$. Es sei $w_1 \neq 0$. Für alle $u_2 \in V_2$ gilt

$$0 = (w_1 + w_2, u_2) = (w_1, u_2),$$

da $w_2 \in p_2(f)^{k_2-1}(V_2) \subseteq \text{Rad}(V_2)$ ist. Somit ist $w_1 \in p_1(f)^{k_1-1}(V_1) \cap V_2^\perp$. Das heißt, $p_1(f)^{k_1-1}(V_1) \cap V_2^\perp$ ist ein nichttrivialer Teilmodul von V_1 , enthält also den irreduziblen f -Modul $p_1(f)^{k_1-1}(V_1)$. Es ergibt sich ein Widerspruch zu $p_1(f)^{k_1-1}(V_1) \not\subseteq V_2^\perp$. $\square$

Aus den obigen Sätzen erhält man die folgende Einteilung von orthogonal unzerlegbaren Moduln in drei Klassen:

Satz 3.1.6. *Sei V ein nicht ausgearteter quadratischer Raum und $f \in \text{GO}(V)$ eine Ähnlichkeit mit Multiplikator s , so dass V ein orthogonal unzerlegbarer f -Modul ist. Dann ist V von einem der folgenden Typen:*

Typ I: *Es gibt unzerlegbare f -Moduln V_1, V_2 , so dass $V = V_1 \oplus V_2$ ist. Dabei haben $f|_{V_1}$ und $f|_{V_2}$ das selbe Minimalpolynom p^n und es gilt $p^{*s} = p$.*

Typ II: *V ist ein unzerlegbarer f -Modul und das Minimalpolynom von f ist p^n für ein $n \in \mathbb{N}$ und ein irreduzibles Polynom p mit $p^{*s} = p$.*

Typ III: *Es ist $V = V_1 \oplus V_2$ mit unzerlegbaren f -Moduln V_1, V_2 . Ist p^n das Minimalpolynom von $f|_{V_1}$, dann ist $(p^{*s})^n$ das Minimalpolynom von $f|_{V_2}$. Dabei sind p und p^{*s} teilerfremd. V_1 und V_2 sind ausgeartet.*

Sei V ein orthogonal unzerlegbarer f -Modul. Der Typ (wie in Satz 3.1.6) von V sei $t \in \{\text{I}, \text{II}, \text{III}\}$ und f habe auf V das Minimalpolynom p . Dann sagen wir auch „ V ist vom Typ (t, p) “ oder „vom Typ t_p “.

Im Folgenden betrachten wir nur noch unzerlegbare f -Moduln zu orthogonalen Abbildungen f . Wir werden feststellen, zu welchen Polynomen p es quadratische Räume V und orthogonale Abbildungen $f \in \text{O}(V)$ mit Minimalpolynom p gibt, so dass V ein f -Modul von einem der obigen Typen ist.

Im Fall orthogonaler Abbildungen f gibt es nach [Hup80a, 2.1] f -Moduln vom Typ I nur für solche f , deren Minimalpolynom von der Form $(X \pm 1)^n$ ist:

Lemma 3.1.7 ([Hup80a, 2.1]). *Sei V ein nicht ausgearteter quadratischer Raum und $f \in \text{O}(V)$ eine orthogonale Abbildung, so dass V ein orthogonal unzerlegbarer f -Modul vom Typ I_{p^n} ist mit irreduziblem p und $n \in \mathbb{N}$. Dann ist $p = X \pm 1$.*

Zunächst beschäftigen wir uns nun speziell mit orthogonal unzerlegbaren f -Moduln auf denen $f \in \text{O}(V)$ das Minimalpolynom $(X \pm 1)^t$ mit $t \in \mathbb{N}$ hat.

Sei V ein K -Vektorraum, $f \in \text{GL}(V)$ und $b = (v_1, \dots, v_n)$ eine Basis von V . Wir bezeichnen b als f -Jordanbasis, wenn $f(v_n) = \lambda v_n$ und $f(v_i) = \lambda v_i + v_{i+1}$ ist für $i < n$ und ein $\lambda \in K$.

Lemma 3.1.8. *Sei V ein unzerlegbarer f -Modul, $f \in O(V)$ mit Minimalpolynom $(X - \lambda)^t$, $\lambda^2 = 1$ und $(v_1, \dots, v_n)$ eine f -Jordanbasis von V . Dann gilt:*

- (i) *Für alle $1 < i, j \leq n$ ist $(v_i, v_j) + \lambda(v_{i-1}, v_j) + \lambda(v_i, v_{j-1}) = 0$.*
- (ii) *Ist die Bilinearform von einer quadratischen Form Q induziert, so ist $Q(v_i) = -\lambda(v_i, v_{i-1})$ für alle $1 < i \leq n$.*

Beweis. Für alle $1 < i, j \leq n$ gilt

$$\begin{aligned} (v_{i-1}, v_{j-1}) &= (f(v_{i-1}), f(v_{j-1})) = (\lambda v_{i-1} + v_i, \lambda v_{j-1} + v_j) \\ &= (v_{i-1}, v_{j-1}) + \lambda(v_{i-1}, v_j) + \lambda(v_i, v_{j-1}) + (v_i, v_j). \end{aligned}$$

$$Q(v_{i-1}) = Q(f(v_{i-1})) = Q(v_i + \lambda v_{i-1}) = \lambda(v_i, v_{i-1}) + Q(v_i) + Q(v_{i-1}).$$

□

Satz 3.1.9. *Sei V ein K -Vektorraum mit symmetrischer Bilinearform $(\cdot, \cdot)$ und $f: V \rightarrow V$ eine orthogonale Abbildung mit Minimalpolynom $(X \pm 1)^t$. Seien außerdem V_1 und V_2 zwei f -invariante Teilräume von V und $(x_1, \dots, x_n)$ eine $f|_{V_1}$ -Jordanbasis von V_1 . Weiter sei $(y_1, \dots, y_n)$ eine $f|_{V_2}$ -Jordanbasis von V_2 . Dann gilt:*

- (i) *$(x_i, y_j) = 0$ für $i + j > n + 1$.*
- (ii) *Ist $k \in \{1, \dots, n\}$, so dass $(x_i, y_j) = 0$ für $i + j > k + 1$, so gilt*

$$(x_i, y_{k-i+1}) = (-1)^{i+1}(x_1, y_k)$$

für alle $1 \leq i \leq k$.

Beweis. Sei $(X + \lambda)^t$ das Minimalpolynom von f .

- (i) Sei zunächst $i = n$ und $1 \leq j < n$. Dann gilt wegen $\lambda = \pm 1$

$$(x_n, y_j) = (f(x_n), f(y_j)) = (\lambda x_n, \lambda y_j + y_{j+1}) = (x_n, y_j) + \lambda(x_n, y_{j+1}).$$

Es folgt $(x_n, y_{j+1}) = 0$.

Sei nun $1 \leq i < n$ und es gelte $(x_{i+1}, y_k) = 0$ für alle $k > n + 1 - (i + 1) = n - i$. Weiterhin sei $n > j \geq n + 1 - i$. Dann gilt

$$\begin{aligned} (x_i, y_j) &= (f(x_i), f(y_j)) = (\lambda x_i + x_{i+1}, \lambda y_j + y_{j+1}) \\ &= (x_i, y_j) + \lambda(x_i, y_{j+1}) + \lambda(x_{i+1}, y_j) + (x_{i+1}, y_{j+1}) \\ &= (x_i, y_j) + \lambda(x_i, y_{j+1}), \end{aligned}$$

da $j > n - i$. Also ist $(x_i, y_{j+1}) = 0$.

- (ii) Für $i = 1$ ist offensichtlich $(x_i, y_{k-i+1}) = (-1)^{i+1}(x_1, y_k)$. Sei also $1 < i \leq k$ und

$$(x_{i-1}, y_{k-(i-1)+1}) = (-1)^i(x_1, y_k).$$

Wie in Lemma 3.1.8 (i) gilt

$$0 = \lambda(x_{i-1}, y_{k-(i-1)+1}) + \lambda(x_i, y_{k-i+1}) + (x_i, y_{k-i+2}).$$

Wegen $i + (k - i + 2) > k + 1$ ist $(x_i, y_{(k+1)-i+1}) = 0$. Es folgt

$$(x_i, y_{k-i+1}) = -(x_{i-1}, y_{k-(i-1)+1}) = (-1)^{i+1}(x_1, y_k).$$

□

Mit diesen Hilfsmitteln können wir nun die möglichen Bilinearformen berechnen, bezüglich derer f orthogonal ist. Dies liefert Restriktionen an die Existenz orthogonal unzerlegbarer f -Moduln.

Beispiel. Sei V ein nicht ausgearteter quadratischer K -Raum und $f \in O(V)$ mit Minimalpolynom $(X - 1)^4$. Ist V orthogonal unzerlegbar, so ist V nach Satz 3.1.6 entweder vom Typ $I_{(X-1)^4}$ und es gibt eine Zerlegung $V = V_1 \oplus V_2$ mit unzerlegbaren Moduln V_i oder V ist vom Typ $II_{(X-1)^4}$.

(i) Sei V vom Typ $I_{(X-1)^4}$ und seien $(b_1, \dots, b_4)$ und $(b_5, \dots, b_8)$ Jordanbasen von V_1 bzw. V_2 . Es bezeichne $G = ((b_i, b_j))_{i,j \in \{1, \dots, 8\}}$ die Matrix der Bilinearform von V bzgl. der Basis $(b_1, \dots, b_8)$. Dann hat G nach Satz 3.1.9 und der Bemerkung von Seite 22 die folgende Form:

$$G = \left(\begin{array}{ccc|ccc} * & * & a & & * & * & * & d \\ * & -a & & & * & * & -d & \\ a & & & & * & d & & \\ \hline * & * & * & -d & * & * & c & \\ * & * & d & & * & -c & & \\ * & -d & & & c & & & \\ d & & & & & & & \end{array} \right).$$

(ii) Hat V den Typ $II_{(X-1)^4}$ und ist $(b_1, \dots, b_4)$ eine Jordanbasis von V , so sieht die Matrix $G = ((b_i, b_j))_{i,j \in \{1, \dots, 4\}}$ der Bilinearform von V wie folgt aus:

$$G = \begin{pmatrix} * & * & * & -a \\ * & * & a & \\ * & -a & & \\ a & & & \end{pmatrix}$$

Weil V nicht ausgeartet ist, ist dabei $a \neq 0$ und, da die Bilinearform symmetrisch ist, tritt dieser Fall nur auf, wenn $\text{Char}(K) = 2$ ist.

Folgerung 3.1.10. (i) Ist $\text{Char}(K) = 2$ und ist die Bilinearform von einer quadratischen Form induziert, dann gibt es Moduln vom Typ $II_{(X \pm 1)^n}$ höchstens für gerade n .

(ii) Bei ungerader Charakteristik gibt es Moduln vom Typ $II_{(X \pm 1)^n}$ höchstens für ungerade n .

(iii) Ist $\text{Char}(K) \neq 2$ und V ein orthogonal unzerlegbarer Modul vom Typ $\text{I}_{(X \pm 1)^n}$, so ist n gerade.

Beweis. (i) Sei V ein orthogonal unzerlegbar f -Modul vom Typ $\text{II}_{(X \pm 1)^n}$ und $(v_1, \dots, v_n)$ eine f -Jordanbasis von V . Wegen 3.1.9(i) gilt $(v_n, v_j) = 0$ für alle $j > 1$. Für ungerades n folgt aus 3.1.9(ii), dass

$$(v_1, v_n) = \pm(v_{\frac{n+1}{2}}, v_{\frac{n+1}{2}}) = 2Q(v_{\frac{n+1}{2}}) = 0$$

ist. Das heißt, $v_n \in \text{Rad}(V)$, was ein Widerspruch zu V nicht ausgeartet ist.

(ii) Sei V ein orthogonal unzerlegbar f -Modul vom Typ $\text{II}_{(X \pm 1)^n}$ und sei $(v_1, \dots, v_n)$ eine f -Jordanbasis von V . Für gerades n folgt aus 3.1.9 (ii), dass

$$(v_n, v_1) = (-1)^{n+1}(v_1, v_n) = -(v_n, v_1),$$

also $v_n \in \text{Rad}(V)$ ist.

(iii) Seien V_1, V_2 unzerlegbare Moduln mit $V = V_1 \oplus V_2$. Sei $(v_1, \dots, v_n)$ eine Jordanbasis von V_1 und $(w_1, \dots, w_n)$ eine Jordanbasis von V_2 . Sei weiterhin U der von $v_1 + w_1$ erzeugte Teilmodul von V . Dann sind V_1, V_2 und U ausgeartet. Damit ist $(v_1, v_n) = (w_1, w_n) = (v_1 + w_1, v_n + w_n) = 0$. Das heißt

$$0 = (v_1 + w_1, v_n + w_n) = (v_1, w_n) + (v_n, w_1).$$

Also ist $(v_n, w_1) = -(v_1, w_n)$. Aus Satz 3.1.9(ii) folgt außerdem $(v_n, w_1) = (-1)^{n+1}(v_1, w_n)$. Somit ist n gerade. □

Definition 3.1.11. Sei $(k, p) \in \{\text{I}, \text{II}, \text{III}\} \times K[X]$. Genau dann heißt (k, p) zulässiger Typ, wenn eine der folgenden Aussagen gilt:

- (i) Es ist $k = \text{I}$ und $p = (X \pm 1)^n$ für ein $n \in \mathbb{N}$, wobei n gerade ist, falls $\text{Char}(K) \neq 2$ ist.
- (ii) Es gibt ein irreduzibles, symmetrisches $q \in K[X]$ mit $\deg(q) > 1$, so dass $p = q^n$ für ein $n \in \mathbb{N}$, und $k = \text{II}$.
- (iii) Es gilt $k = \text{II}$ und $p = (X \pm 1)^n$, wobei n ungerade ist, falls $\text{Char}(K) \neq 2$ ist, und n gerade ist, wenn $\text{Char}(K) = 2$ ist.
- (iv) Es gibt ein unsymmetrisches und irreduzibles $q \in K[X]$, so dass $p = (qq^*)^n$ ist für ein $n \in \mathbb{N}$. Außerdem ist $k = \text{III}$.

Es bezeichne $\mathcal{T}$ die Menge der zulässigen Typen aus $\{\text{I}, \text{II}, \text{III}\} \times K[X]$.

Satz 3.1.12. Ist $t \in \mathcal{T}$ ein zulässiger Typ, dann gibt es einen quadratischen Raum V und eine orthogonale Abbildung $f \in \text{O}(V)$, so dass V ein orthogonal unzerlegbarer f -Modul vom Typ t ist.

Beweis. Für Typ II wird der Satz in [Hup80b, 3.2, 3.4 und 3.5] bewiesen.

Ist $t = (\text{III}, p)$, dann gibt es nach [Hup80b, 3.6] einen K -Vektorraum V mit symmetrischer Bilinearform $(\cdot, \cdot)$ und ein $f \in \text{O}(V)$, so dass V nicht ausgearteter

f -Modul vom Typ t ist. Sei $V = V_1 \oplus V_2$ mit unzerlegbaren f -Moduln V_i . Definiert man $Q(v_1 + v_2) := (v_1, v_2)$ für alle $v_1 \in V_1$ und $v_2 \in V_2$, dann ist Q eine quadratische Form auf V , bezüglich welcher f orthogonal ist. Da V_1 und V_2 total ausgeartet sind, ist $(x, y) = Q(x + y) - Q(x) - Q(y)$.

Im Fall des Typs I gilt die Behauptung bei ungerader Charakteristik nach [Hup80a, 2.3 b)]. Ist die Charakteristik gerade, so lässt sich Aussage genau wie im Beweis von [Hup80a, 2.3 b)] zeigen. $\square$

3.2 Die quadratischen Formen orthogonal unzerlegbarer Moduln

Im letzten Abschnitt haben wir gesehen, zu welchen linearen Abbildungen f sich eine quadratische Form definieren lässt, so dass f orthogonal ist. Hier untersuchen wir nun genauer, welches die möglichen f -invarianten quadratischen Formen sind. Zudem haben wir als Ziel, zu verschiedenen Ordnungen bis auf Konjugation die zyklischen orthogonalen Gruppen dieser Ordnungen zu finden.

Sei V ein quadratischer Raum und $f, g \in O(V)$. Es sei $V = V_1 \perp V_2 = W_1 \perp W_2$ mit f -invarianten Teilräumen V_1, V_2 und g -invarianten Räumen W_1, W_2 . Für $i \in \{1, 2\}$ sei der f -Modul V_i äquivalent zum g -Modul W_i in dem Sinne, dass es eine Isometrie $h_i: V_i \rightarrow W_i$ gibt mit $g|_{W_i} \circ h_i = h_i \circ f|_{V_i}$. Definiert man dann auf V eine Abbildung h durch $h(x_1 + x_2) := h_1(x_1) + h_2(x_2)$ für $x_i \in V_i$, so ist $h \in O(V)$ und es ist $h^{-1}gh = f$. Das heißt, f und g sind konjugiert in $O(V)$. Wir interessieren uns in diesem Abschnitt deshalb insbesondere dafür, welche Moduln der einzelnen Typen es bis auf Äquivalenz gibt.

Lemma 3.2.1. *Sei V ein K -Vektorraum und unzerlegbarer f -Modul. Außerdem sei $(v_1, \dots, v_n)$ eine f -Jordanbasis von V . Dann ist $(w_1, \dots, w_n)$ genau dann eine f -Jordanbasis von V , wenn es $a_1, \dots, a_n \in K$ gibt mit $a_1 \neq 0$, so dass $w_k = \sum_{i=k}^n a_{i-k+1} v_i$ ist.*

Beweis. „ $\Rightarrow$ “: Sei $(w_1, \dots, w_n)$ eine f -Jordanbasis von V . Dann gibt es Elemente $a_1, \dots, a_n \in K$ so dass $w_1 = \sum_{i=1}^n a_i v_i$ ist.

Sei $1 \leq k < n$ und es gelte $w_k = \sum_{i=k}^n a_{i-k+1} v_i$, dann ist

$$\begin{aligned} f(w_k) &= \sum_{i=k}^n a_{i-k+1} f(v_i) = \sum_{i=k}^n a_{i-k+1} \lambda v_i + \sum_{i=k}^{n-1} a_{i-k+1} v_{i+1} \\ &= \lambda w_k + \sum_{i=k+1}^n a_{i-1-k+1} v_i. \end{aligned}$$

Es folgt $\sum_{i=k+1}^n a_{i-(k+1)+1} v_i = f(w_k) - \lambda w_k = w_{k+1}$.

„ $\Leftarrow$ “: Seien nun $a_1, \dots, a_n \in K$, so dass $a_1 \neq 0$ und $w_k = \sum_{i=k}^n a_{i-k+1}v_i$ ist für alle k . Aus $a_1 \neq 0$ folgt, dass $(w_1, \dots, w_n)$ linear unabhängig, also eine Basis von V , ist.

Für $k = n$ ist $f(w_n) = f(a_1v_n) = a_1\lambda v_n = \lambda w_n$. Ist nun $1 \leq k < n$, so gilt

$$\begin{aligned} f(w_k) &= \sum_{i=k}^n a_{i-k+1}f(v_i) = \sum_{i=k}^n a_{i-k+1}\lambda v_i + \sum_{i=k}^{n-1} a_{i-k+1}v_{i+1} \\ &= \lambda \sum_{i=k}^n a_{i-k+1}v_i + \sum_{i=k+1}^n a_{i-k-1+1}v_i = \lambda w_k + w_{k+1}. \end{aligned}$$

□

Bemerkung. Die Basiswechselmatrix zum Basiswechsel aus obigem Satz hat also die folgende Form:

$$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ a_2 & a_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_n & \dots & a_2 & a_1 \end{pmatrix}$$

3.2.1 Moduln vom Typ $\Pi_{(x \pm 1)^n}$

Lemma 3.2.2. Sei K ein Körper, $p = X \pm 1 \in K[X]$ und V ein nicht ausgearteter quadratischer K -Raum. Weiterhin sei f eine orthogonale Abbildung von V , so dass V ein unzerlegbarer f -Modul vom Typ Π_{p^n} ist. Sei $i < \frac{n}{2}$ und $v \in V \setminus p(f)(V)$, dann gibt es ein $w \in V \setminus p(f)(V)$, so dass

$$\begin{aligned} Q(p^j(f)(w)) &= Q(p^j(f)(v)) \quad \text{für alle } j \geq i \text{ und} \\ Q(p^{i-1}(f)(w)) &= 0. \end{aligned}$$

Beweis. Da V nicht ausgeartet ist, gilt $(p^{n-1}(f)(v), v) \neq 0$. Wegen Satz 3.1.9 ist also $(p^{i-1}(f)(v), p^{n-i}(f)(v)) \neq 0$. Definiere

$$\alpha := -\frac{Q(p^{i-1}(f)(v))}{(p^{i-1}(f)(v), p^{n-i}(f)(v))} \quad \text{und} \quad w := v + \alpha p^{n-2i+1}(f)v.$$

Sei $j \geq i - 1$. Mit $i < \frac{n}{2}$ folgt $n - 2i + 1 + j \geq n - i > \frac{n}{2}$. Aus Satz 3.1.9 und Lemma 3.1.8 ergibt sich somit, dass $Q(p^{n-2i+1+j}(f)(v)) = 0$ ist. Für $j = i - 1$ gilt also

$$\begin{aligned} Q(p^{i-1}(f)(w)) &= Q(p^{i-1}(f)(v) + \alpha p^{n-i}(f)(v)) \\ &= Q(p^{i-1}(f)(v)) + \alpha (p^{i-1}(f)(v), p^{n-i}(f)(v)) = 0. \end{aligned}$$

Sei nun $j > i - 1$. Dann ist $j + n - 2i + 1 + j = n - 2i + 1 + 2j > n - 1$, woraus $(p^j(f)(v), p^{n-2i+1+j}(f)(v)) = 0$ folgt. Damit ist

$$Q(p^j(f)(w)) = Q(p^j(f)(v) + \alpha p^{j+n-2i+1}(f)(v)) = Q(p^j(f)(v)).$$

□

Beispiel. Sei V ein quadratischer K -Raum, $\text{Char}(K) \neq 2$ und $f \in \text{O}(V)$, so dass V ein f -Modul vom Typ $\text{II}_{(X-1)^n}$ ist. Dann folgt aus Lemma 3.2.2, dass es eine f -Jordanbasis von V gibt, so dass die Matrix G der Bilinearform bezüglich dieser Basis wie folgt aussieht.

$$G = \left(\begin{array}{ccc|ccc} 0 & \dots & 0 & * & \dots & * & a \\ \vdots & & \vdots & \vdots & & \ddots & \\ 0 & \dots & 0 & * & \dots & * & \\ \hline * & \dots & * & \pm a & & & \\ \vdots & \ddots & \ddots & & & & \\ * & \ddots & & & & & \\ a & & & & & & \end{array} \right)$$

Wegen Lemma 3.1.8 ist dabei G eindeutig durch a bestimmt.

Satz 3.2.3. Sei K ein endlicher Körper mit $\text{Char}(K) \neq 2$ und $p = X \pm 1 \in K[X]$. Für $i \in \{1, 2\}$ sei V_i ein K -Vektorraum mit quadratischer Form Q_i und $f_i \in \text{O}(V_i)$, so dass V_i ein nicht ausgearteter unzerlegbarer f_i -Modul vom Typ II_{p^n} ist. Bezeichne β_i die von Q_i induzierte Bilinearform auf V_i . Folgende Aussagen sind äquivalent:

- (i) V_1 ist isometrisch zu V_2 , das heißt, es gibt einen Isomorphismus $h: V_1 \rightarrow V_2$ mit $Q_2(h(x)) = Q_1(x)$ für alle $x \in V_1$.
- (ii) Ist $u \in V_1 \setminus p(f_1)(V_1)$ und $w \in V_2 \setminus p(f_2)(V_2)$, dann ist

$$\beta_1(p^{n-1}(f_1)u, u) \beta_2(p^{n-1}(f_2)w, w)^{-1}$$

ein Quadrat in K .

- (iii) Es gibt eine Isometrie $h: V_1 \rightarrow V_2$ mit $h \circ f_1 = f_2 \circ h$.

Beweis. Sei $K^\square := \{a^2 \mid a \in K^*\}$.

„(i) $\Rightarrow$ (ii)“: Sei $u \in V_1 \setminus p(f_1)(V_1)$ und $w \in V_2 \setminus p(f_2)(V_2)$ beliebig.

Dann ist $b_1 := (p^0(f_1)(u), \dots, p^{n-1}(f_1)(u))$ eine f_1 -Jordanbasis von V_1 , und $b_2 := (p^0(f_2)(w), \dots, p^{n-1}(f_2)(w))$ eine f_2 -Jordanbasis von V_2 . Für $i \in \{1, 2\}$ bezeichne G_i die Matrix der Bilinearform auf V_i bezüglich der Basis b_i .

Aus (i) folgt $\det(G_1) \det(G_2)^{-1} \in K^\square$. Da n ungerade ist ergibt sich aus Satz 3.1.9, dass $\det(G_1) = \beta_1(u, p^{n-1}(f_1)(u))^n$ und $\det(G_2) = \beta_2(w, p^{n-1}(f_2)(w))^n$ ist, woraus die Behauptung folgt.

„(ii) $\Rightarrow$ (iii)“: Nach 3.2.2 kann man eine f_1 -Jordanbasis $b_1 = (u_1, \dots, u_n)$ von V_1 und eine f_2 -Jordanbasis $b_2 = (w_1, \dots, w_n)$ von V_2 so wählen, dass $Q(u_i) = Q(w_i) = 0$ ist für alle $i < \frac{n}{2}$. Wegen (ii) ist

$$\beta_1(u_1, u_n) \beta_2(w_1, w_n)^{-1} = \beta_1(u_1, p^{n-1}(f_1)(u_1)) \beta_2(w_1, p^{n-1}(f_2)(w_1))^{-1} \in K^\square.$$

Sei $a \in K$ mit $a^2 = \beta_1(u_1, u_n) \beta_2(w_1, w_n)^{-1}$. Definiere $h: V_1 \rightarrow V_2$ durch lineare Fortsetzung von $u_i \mapsto aw_i$. $\square$

Satz 3.2.4. *Sei K ein endlicher Körper mit $\text{Char}(K) = 2$ und $p = X+1 \in K[X]$. Weiterhin sei V ein K -Vektorraum mit quadratischer Form Q und $f \in \mathcal{O}(V)$, so dass V ein nicht ausgearteter unzerlegbarer f -Modul vom Typ Π_{p^n} ist. Dann sind äquivalent:*

- (i) *Der Wittindex von V ist $\frac{n}{2}$.*
- (ii) *Es gibt ein $v \in p^{\frac{n}{2}-1}(f)(V) \setminus p^{\frac{n}{2}}(f)(V)$ mit $Q(v) = 0$.*

Beweis. Sei $U := p^{\frac{n}{2}+1}(f)(V)$. Mit 3.1.9 folgt, dass U total singulär und $U^\perp = p^{\frac{n}{2}-1}(f)(V)$ ist.

„(ii) $\Rightarrow$ (i)“: Ist $v \in p^{\frac{n}{2}-1}(f)(V) \setminus p^{\frac{n}{2}}(f)(V)$ mit $Q(v) = 0$, so ist $W := U \oplus \langle v \rangle$ ein total singulärer Teilraum von V mit

$$\dim W = \dim U + 1 = n - \left(\frac{n}{2} + 1\right) + 1 = \frac{n}{2}.$$

„(i) $\Rightarrow$ (ii)“: Ist der Wittindex von V gleich $\frac{n}{2}$, so gibt es einen total singulären Teilraum von V , der U enthält. Da

$$U^\perp = p^{\frac{n}{2}-1}(f)(V) = \langle p^{\frac{n}{2}-1}(f)(v), p^{\frac{n}{2}}(f)(v) \rangle \oplus U$$

ist gibt es ein $w \in \langle p^{\frac{n}{2}-1}(f)(v), p^{\frac{n}{2}}(f)(v) \rangle$ mit $Q(w) = 0$. Aus $Q(p^{\frac{n}{2}}(f)(v)) \neq 0$ folgt $w \in p^{\frac{n}{2}-1}(f)(V) \setminus p^{\frac{n}{2}}(f)(V)$. $\square$

Satz 3.2.5. *Sei K ein endlicher Körper mit $\text{Char}(K) = 2$ und $p = X+1 \in K[X]$. Für $i \in \{1, 2\}$ sei (V_i, Q_i) ein quadratischer K -Vektorraum und $f_i \in \mathcal{O}(V_i)$, so dass V_i ein nicht ausgearteter unzerlegbarer f_i -Modul vom Typ Π_{p^n} ist. Folgende Aussagen sind äquivalent*

- (i) *V_1 ist isometrisch zu V_2 .*
- (ii) *Es gibt eine Isometrie $h: V_1 \rightarrow V_2$ mit $h \circ f_1 = f_2 \circ h$.*

Beweis. Hat V_1 den Wittindex $\frac{n}{2}$, so gibt es ein $v \in p^{\frac{n}{2}-1}(f_1)(V_1) \setminus p^{\frac{n}{2}}(f_1)(V_1)$ mit $Q(v_1) = 0$. Mit Lemma 3.2.2 folgt, dass es ein $w \in V_1 \setminus p(f_1)(V_1)$ gibt mit $Q(p^i(f_1)(w)) = 0$ für alle $i \leq \frac{n}{2}$. O.B.d.A sei $Q(p^{\frac{n}{2}}(f_1)(w)) = 1$. Falls (i) gilt, so gibt es analog ein $u \in V_2 \setminus p(f_2)(V_2)$ mit $Q(p^i(f_2)(u)) = 0$ für alle $i \leq \frac{n}{2}$ und $Q(p^{\frac{n}{2}}(f_2)(u)) = 1$. Ist die Abbildung $h: V_1 \rightarrow V_2$ durch lineare Fortsetzung von $p^i(f_1)(w) \mapsto p^i(f_2)(u)$ definiert, so gilt $h \circ f_1 = f_2 \circ h$ und $Q_2(h(x)) = Q_1(x)$ für alle $x \in V_1$.

Der Wittindex von V_1 und V_2 sei nun kleiner als $\frac{n}{2}$. Für $i \in \{1, 2\}$ sei $v_i \in p^{\frac{n}{2}-1}(f_i)(V_i) \setminus p^{\frac{n}{2}}(f_i)(V_i)$ mit $Q(p(f_i)(v_i)) = 1$. Dann ist $Q(v_i) + X + X^2 \in K[X]$ irreduzibel. Es folgt, dass $Q(v_1) + Q(v_2) + X + X^2$ reduzibel ist.

Sei $\alpha \in K$ mit $Q(v_1) + \alpha + \alpha^2 = Q(v_2)$ und definiere $u := v_1 + \alpha p(f_1)(v_1)$. Dann ist $u \in V_1 \setminus p(f_1)(V_1)$. Außerdem gilt

$$Q(u) = Q(v_2) \quad \text{und} \quad Q(p(f_1)(u)) = Q(p(f_2)(v_2)).$$

Mit Lemma 3.2.2 folgt, dass es $w_1 \in V_1 \setminus p(f_1)(V_1)$ und $w_2 \in V_2 \setminus p(f_2)(V_2)$ gibt, so dass

$$\begin{aligned} Q(p^i(f_1)(w_1)) &= Q(p^i(f_2)(w_2)) = 0 \quad \text{für } i < \frac{n}{2} - 1, \\ Q(p^{\frac{n}{2}-1}(f_1)(w_1)) &= Q(p^{\frac{n}{2}-1}(f_2)(w_2)) \\ \text{und } Q(p^{\frac{n}{2}}(f_1)(w_1)) &= Q(p^{\frac{n}{2}}(f_2)(w_2)) = 1. \end{aligned}$$

Definiert man $h: V_1 \rightarrow V_2$ als lineare Fortsetzung von $p^i(f_1)(w_1) \mapsto p^i(f_2)(w_2)$, dann gilt $h \circ f_1 = f_2 \circ h$ und $Q_2(h(x)) = Q_1(x)$ für alle $x \in V_1$. $\square$

3.2.2 Moduln vom Typ $I_{(x \pm 1)^n}$

Ist V ein quadratischer K -Raum, $\text{Char}(K) \neq 2$ und V ein f -Modul vom Typ $I_{(X \pm 1)^n}$, dann gibt es nach [Hup80a, 2.4] total singuläre f -Moduln W_1, W_2 , so dass $V = W_1 \oplus W_2$. Falls $\text{Char } K = 2$, so gilt diese Aussage nicht mehr, wie folgendes Beispiel zeigt.

Beispiel. Sei $K = \text{GF}(8)$, $V := K^2$ und f die Identität auf V . Die quadratische Form auf V sei definiert durch $Q(x) := x_1^2 + x_1x_2 + x_2^2$. Dann ist V vom Typ I_{X-1} und es gibt keine total singulären Räume V_1, V_2 , so dass $V = V_1 \oplus V_2$ ist.

Es gibt im allgemeinen auch keine Zerlegung $V = W_1 \oplus W_2$ mit total ausgearteten Teilmoduln W_1, W_2 , vgl. Beispiel 2.5 in [Hup80a].

Wir werden im Folgenden zeigen, dass es für Moduln vom Typ $I_{(X \pm 1)^n}$ mit geradem n eine Zerlegung mit total singuläre Teilmoduln gibt. Im Fall ungerader Charakteristik gilt dies wegen 3.1.10 dann insbesondere für alle Moduln vom Typ I.

Satz 3.2.6. *Sei V ein f -Modul vom Typ $I_{(X \pm 1)^n}$. Dann gibt es f -invariante Teilräume U, W mit Jordanbasen $(u_1, \dots, u_n)$ und $(w_1, \dots, w_n)$ von U und W , so dass $V = U \oplus W$ und $Q(u_i) = Q(w_i) = 0$ für $i \leq \frac{n}{2}$.*

Beweis. Sei $V = U \oplus W$ mit f -invarianten Teilräumen U und W .

Sei $1 \leq i_0 \leq \frac{n}{2}$, so dass $Q(u_j) = 0$ ist für $i_0 + 1 \leq j \leq \frac{n}{2}$. Wegen Lemma 3.1.9 ist $(u_{i_0}, w_{n-i_0+1}) = \pm(u_1, w_n) \neq 0$. Definiere $\alpha := -\frac{Q(u_{i_0})}{(u_{i_0}, w_{n-i_0+1})}$ und

$$u'_j := \begin{cases} u_j - \alpha w_{n-2i_0+j+1}, & \text{falls } j \leq 2i_0 - 1 \\ u_j, & \text{sonst} \end{cases}$$

Dann ist $(u'_1, \dots, u'_n)$ eine f -Jordanbasis und es gilt $V = \langle u'_1, \dots, u'_n \rangle \oplus W$. Für $j > 2i_0 - 1$ ist offensichtlich $Q(u'_j) = Q(u_j)$.

Sei nun $i_0 \leq j \leq 2i_0 - 1$. Aus $j \geq i_0$ und $i_0 \leq \frac{n}{2}$ folgt

$$n - 2i_0 + j + 1 \geq n - i_0 + 1 \geq n - \frac{n}{2} + 1 = \frac{n}{2} + 1.$$

Da U ausgeartet ist, gilt $u_n \in \text{Rad}(U)$. Wegen 3.1.9 ist damit $(u_i, u_j) = 0$ für $j \geq n - i + 1$. Also ist $Q(u_i) = \pm(u_i, u_{i-1}) = 0$ für $i \geq \frac{n}{2} + 1$. Das heißt $Q(u_{n-2i_0+j+1}) = 0$, so dass

$$Q(u'_j) = Q(u_j) - \frac{Q(u_{i_0})}{(u_{i_0}, w_{n-i_0+1})}(u_j, w_{n-2i_0+j+1}),$$

woraus $Q(u'_{i_0}) = 0$ folgt. Falls $j > i_0$ ist, so gilt $n - 2i_0 + j + 1 > n - j + 1$, also ist $(v_j, w_{n-2i_0+j+1}) = 0$ und somit $Q(w_j) = Q(v_j)$. $\square$

Folgerung 3.2.7. *Ist n gerade und V ein f -Modul vom Typ $I_{(X \pm 1)^n}$, so gibt es total singuläre f -Moduln U, W , so dass $V = U \oplus W$ gilt.*

Beweis. Wie in Satz 3.2.6 sei $V = U \oplus W$ mit f -invarianten Räumen U, W und seien $(u_1, \dots, u_n)$ und $(w_1, \dots, w_n)$ Jordanbasen von U resp. W , so dass $Q(v_i) = Q(w_i) = 0$ ist für $i \leq \frac{n}{2}$.

Da V orthogonal unzerlegbar ist, sind U und W ausgeartet, so dass $u_n \in \text{Rad}(U)$, vgl. Bemerkung S. 22. Wegen Satz 3.1.9 (ii) ist also $(u_i, u_j) = 0$ für $i + j \geq n + 1$ und mit Lemma 3.1.8 folgt $Q(u_i) = \pm(u_i, u_{i-1}) = 0$ für $i \geq \frac{n}{2} + 1$.

Damit ist, da n gerade ist, $Q(u_i) = 0$ für $1 \leq i \leq n$. Somit ist U total singulär. Analog ist W total singulär. $\square$

Lemma 3.2.8. *Sei $V = V_1 \oplus V_2$ ein nicht ausgearteter quadratischer Raum und $f \in O(V)$. Des Weiteren seien V_1 und V_2 total singulär und f -invariant. Sei $(v_1, \dots, v_n)$ eine Basis von V_1 . Dann gilt:*

- (i) *Es gibt eine Basis $(v_{n+1}, \dots, v_{2n})$ von V_2 so dass $B_V := (v_1, \dots, v_{2n})$ eine hyperbolische Basis von V ist.*
- (ii) *Ist A die Matrix von $f|_{V_1}$ bezüglich der Basis $(v_1, \dots, v_n)$, so ist $\begin{pmatrix} A & \\ & A^{-t} \end{pmatrix}$ die Matrix zu f bezüglich B_V .*

Beweis. (i) Allgemein gilt: Sind $x_1, \dots, x_i \in V$, dann ist $\dim(\langle x_1, \dots, x_i \rangle^\perp) \geq \dim(V) - i$.

Also ist $\dim \langle v_2, \dots, v_n \rangle^\perp \geq n + 1$ und es gibt ein $v_{n+1} \in V_2 \cap \langle v_2, \dots, v_n \rangle^\perp$. Da V nicht ausgeartet ist, ist $\langle v_1, v_{n+1} \rangle$ eine hyperbolische Ebene. Per Induktion ergibt sich die Behauptung.

(ii) Ist M die Matrix zu f_V bezüglich der Basis B_V , dann ist $MGM^t = G$, wobei G die zur Bilinearform gehörige Matrix ist. Es folgt direkt, dass $M = \begin{pmatrix} A & \\ & A^{-t} \end{pmatrix}$ ist. $\square$

Lemma 3.2.9. *Sei n gerade und $p = (X \pm 1)^n$. Seien V, W zwei nicht ausgeartete quadratische Räume und f_V, f_W orthogonale Abbildungen auf V resp. W , so dass V und W als f_V - resp. f_W -Moduln vom Typ I_p sind. Dann gibt es eine Isometrie $h: V \rightarrow W$, so dass $h \circ f_V = f_W \circ h$ ist.*

Beweis. Wir wählen Zerlegungen $V = V_1 \oplus V_2$ und $W = W_1 \oplus W_2$ mit total singulären Teilmoduln V_i, W_i . Seien B_{V_1} und B_{W_1} Jordanbasen von V_1 resp. W_1 . Wie in Lemma 3.2.8 ergänzen wir diese Basen zu hyperbolischen Basen B_V und B_W von V resp. W . Die Matrizen von f_V und f_W bezüglich diesen Basen sind dann gleich und es folgt die Behauptung. $\square$

3.2.3 Moduln vom Typ III_{pp^*}

Lemma 3.2.10. *Sei K ein Körper mit $\text{Char}(K) = 2$, V ein quadratischer K -Raum und $f \in \text{O}(V)$, so dass V ein unzerlegbarer f -Modul ist. Des Weiteren sei p^n das Minimalpolynom von f mit irreduziblem $p \in K[X]$. Ist V total ausgeartet aber nicht total singulär, so ist $p = X + 1$.*

Beweis. Sei V total ausgeartet und $x \in V \setminus p(f)(V)$. Dann gilt

$$Q(x + f(x)) = Q(x) + Q(f(x)) + (x, f(x)) = 0.$$

Falls $p \neq X + 1$, so ist $y := x + f(x) \in V \setminus p(f)(V)$. Da $V = \langle y, f(y), \dots, f^k(y) \rangle$ für $k = n \cdot \deg(p)$, ist V total singulär. $\square$

Folgerung 3.2.11. *Sei $V = V_1 \oplus V_2$ ein nicht ausgearteter quadratischer K -Raum, $f \in \text{O}(V)$, so dass V ein orthogonal unzerlegbarer f -Modul vom Typ III_{pp^*} ist mit f -invarianten V_1, V_2 . Dann sind V_1, V_2 total singulär.*

Satz 3.2.12. *Seien V, W zwei nicht ausgeartete quadratische K -Räume und f_V, f_W orthogonale Abbildungen auf V resp. W . Weiterhin seien V und W als f_V - bzw. f_W -Moduln vom Typ III_{pp^*} . Dann gibt es eine Isometrie $h: V \rightarrow W$, so dass $h \circ f_V = f_W \circ h$ ist.*

Beweis. Seien $V = V_1 \oplus V_2$ und $W = W_1 \oplus W_2$ Zerlegungen in Teilmoduln, so dass V_1 und W_1 dasselbe Minimalpolynom haben. Wähle Basen B_{V_1} von V_1 und B_{W_1} von W_1 , so dass die Matrizen von f_V auf V_1 und f_W auf W_1 bezüglich dieser Basen gleich sind. Mit Lemma 3.2.8 ist es möglich, hyperbolische Basen von V und W zu wählen, sodass f_V und f_W in der jeweiligen Basis die selbe darstellende Matrix haben. $\square$

3.2.4 Moduln vom Typ II_{p^n}

In diesem Abschnitt betrachten wir Moduln vom Typ II_{p^n} mit irreduziblem $p \neq (X \pm 1)$.

Lemma 3.2.13. *Sei V ein nicht ausgearteter quadratischer Raum und $f \in \text{O}(V)$, so dass V ein unzerlegbarer f -Modul vom Typ II_{p^n} ist mit irreduziblem p . Ist $p \neq (X \pm 1)$, so ist $\deg(p)$ und somit $\dim(V)$, gerade.*

Beweis. Sei d ungerade und $p = \sum_{i=0}^d a_i X^i$ mit $a_d = 1$. Da p symmetrisch ist, folgt $a_0 a_{d-i} = a_i$ für $1 \leq i \leq d$. Mit $a_d = 1$ ergibt sich insbesondere, dass $a_0 = \pm 1$ ist. Es gilt nun

$$\begin{aligned} p &= \sum_{i=0}^{\frac{d-1}{2}} a_i X^i + \sum_{i=\frac{d+1}{2}}^d a_0 a_{d-i} X^i = \sum_{i=0}^{\frac{d-1}{2}} a_i X^i + a_0 \sum_{j=0}^{\frac{d-1}{2}} a_j X^{d-j} \\ &= \sum_{i=0}^{\frac{d-1}{2}} a_i (X^i + a_0 X^{d-i}). \end{aligned}$$

Falls $a_0 = -1$ ist, so ist $p(1) = 0$ und für $a_0 = 1$ ist $p(-1) = 0$. Das heißt, $(X \pm 1)$ teilt p . $\square$

Sei g eine lineare Abbildung eines Vektorraums W , so dass W ein unzerlegbarer g -Modul ist. g habe das Minimalpolynom p^d mit irreduziblem symmetrischem $p \neq X \pm 1$. Nach [Hup80b, 3.2, 3.5] lässt sich auf W eine quadratische Form so definieren, dass W nicht ausgeartet und g eine orthogonale Abbildung ist. Um eine solche quadratische Form konkret zu bestimmen, ist die folgende Beobachtung hilfreich.

Sei V ein quadratischer Raum und $f \in O(V)$, so dass V ein unzerlegbarer f -Modul ist. Es sei $a_n = 1$ und $p = \sum_{i=0}^n a_i X^i$ das Minimalpolynom von f . Für $v \in V$ und $j \leq n$ gilt dann:

$$\begin{aligned} (f^j(v), v) &= (f^n(v), f^{n-j}(v)) = - \sum_{i=0}^{n-1} a_i (f^i(v), f^{n-j}(v)) \\ (3.1) \quad &= - \sum_{i=0}^{n-j} a_i (v, f^{n-j-i}(v)) - \sum_{i=n-j+1}^{n-1} a_i (f^{i-j+n}(v), v) \\ &= - \sum_{k=0}^{n-j} a_{n-j-k} (v, f^k(v)) - \sum_{k=1}^{j-1} a_{k+n-j} (f^k(v), v). \end{aligned}$$

Das heißt, falls $j > \frac{n}{2}$ ist oder $j = \frac{n}{2}$ und $a_0 + 1 \neq 0$ ist, so ist $(f^j(v), v)$ durch $(v, v), (f(v), v), \dots, (f^{j-1}(v), v)$ bestimmt. Für $Q(v)$ erhält man durch eine ähnliche Rechnung die folgende Formel:

$$(3.2) \quad \left(1 - \sum_{i=0}^{n-2} a_i^2\right) Q(v) = \sum_{i < j \leq n-1} a_i a_j (v, f^{j-i}(v)).$$

Wählen wir also eine Basis der Form $(w, g(w), \dots, g^{n-1}(w))$ von W , so können wir (3.1) und (3.2) verwenden um eine Matrix G zu bestimmen, die bezüglich der gegebenen Basis eine quadratische Form auf W definiert, so dass g orthogonal ist.

Beispiel. Sei $K = \text{GF}(7)$ und $p = X^2 + \alpha X + 1 \in K[X]$ irreduzibel. Außerdem sei V ein nicht ausgearteter quadratischer K -Raum und $f \in \text{O}(V)$, so dass V als f -Modul vom Typ II_p ist. Es gibt ein $v \in V$ mit $Q(v) = 1$ (s. [Gro02, 4.8]). Im Fall $\deg(p) = 2$ vereinfacht sich (3.1) zu

$$(1 + a_0)(f(v), v) = -a_1(v, v).$$

Also gilt $(f(v), v) = -\frac{a_1}{2}(v, v) = -\alpha$. Bezüglich der Basis $(v, f(v))$ ist damit $\begin{pmatrix} 2 & -\alpha \\ -\alpha & 2 \end{pmatrix}$ die Matrix der Bilinearform von V .

In den Tabellen in Anhang A ist zu sehen, welche Moduln vom Typ II_p zu den für die Ovoidsuche in dieser Arbeit betrachteten orthogonalen Abbildungen tatsächlich aufgetreten sind. In allen Fällen mit $\deg(p) > 1$ ist hier p irreduzibel und oft ist $\deg(p) = 2$. Es ist deshalb leicht möglich mit Hilfe von (3.1), (3.2) und gegebenenfalls des Computers die möglichen quadratischen Formen zu diesen Typen zu bestimmen.

Im allgemeinen Fall gilt, dass irreduzible Moduln vom Typ II_p nicht maximalen Wittindex haben, wenn $\deg(p) > 1$ ist [Hup70, Satz 3 a),b)].

Für Körper K ungerader Charakteristik klassifiziert Zassenhaus in [Zas58] Paare (X, G) von $(n \times n)$ -Matrizen über K , wobei G die Matrix einer symmetrischen Bilinearform auf K^n und X die Matrix einer bezüglich dieser Bilinearform orthogonalen Abbildung auf K^n ist. Eine Normalform für Matrixpaare, die einen orthogonal unzerlegbaren Modul vom Typ II definieren, findet sich in dabei in [Zas58, § 3, Thm. 1 b)].

3.3 Typen orthogonaler Zerlegungen

Sei V ein quadratischer Raum und $f \in \text{O}(V)$. Aus Abschnitt 3.1 sind die möglichen Typen der orthogonal unzerlegbaren f -Moduln von V bekannt. Wir verallgemeinern hier nun den Begriff des Typs von unzerlegbaren Moduln und definieren Typen von orthogonalen Zerlegungen. Dann geben wir einen Algorithmus an, der die möglichen Typen von Zerlegungen zu orthogonalen Abbildungen vorgegebener Ordnung berechnet.

Sei V ein quadratischer K -Raum, $f \in \text{O}(V)$ und $V = V_1 \perp \cdots \perp V_r$ eine Zerlegung von V in orthogonal unzerlegbare f -Moduln. Dann bezeichnen wir $\{V_1, \dots, V_r\}$ als f -Zerlegung von V .

Wir schreiben in diesem Abschnitt $\llbracket x_1, \dots, x_n \rrbracket$ für die Mehrfachmenge zum Tupel $(x_1, \dots, x_n)$.

Definition 3.3.1. Sei $\mathcal{T}$ die Menge der zulässigen Typen nach Definition 3.1.11 und $Z := \{V_1, \dots, V_r\}$ eine f -Zerlegung eines quadratischen Raums V . Ist $t_i \in \mathcal{T}$ der Typ des f -Moduls V_i für $1 \leq i \leq r$, dann heißt

$$\tau(f, Z) := \llbracket t_1, \dots, t_r \rrbracket$$

der f -Typ der Zerlegung Z .

Wir schreiben auch $t_1 \perp \cdots \perp t_r$ für den Typ von Z .

Im Fall gerader Charakteristik ist es möglich, dass es zu einem quadratischen Raum V und einer Abbildung $f \in \mathcal{O}(V)$ mehrere f -Zerlegungen von V mit verschiedenem Typ gibt, wie im folgenden Beispiel zu sehen ist.

Beispiel. Sei K ein Körper mit $\text{Char}(K) = 2$, $V := K^6$ und $e_1, \dots, e_6$ eine Basis von V . Sei $Q: V \rightarrow K$ definiert durch $Q(\sum a_i e_i) := a_1 a_2 + a_2^2 + a_3 a_4 + a_4^2 + a_5 a_6 + a_5^2$. Des Weiteren sei $f \in \text{GL}(V)$, mit

$$f(e_i) = \begin{cases} e_i + e_{i+1}, & \text{falls } i \in \{1, 3, 5\} \\ e_i, & \text{falls } i \in \{2, 4, 6\}. \end{cases}$$

Dann ist $f \in \mathcal{O}(V)$ und für $i \in \{1, 2, 3\}$ ist $V_i := \langle e_{2i-1}, e_{2i} \rangle$ ein f -Modul vom Typ $\text{II}_{(X-1)^2}$. Also ist $V = V_1 \perp V_2 \perp V_3$ eine f -Zerlegung vom Typ

$$\text{II}_{(X-1)^2} \perp \text{II}_{(X-1)^2} \perp \text{II}_{(X-1)^2}.$$

Sei nun $v := e_3 + e_5$ und $w := e_1 + e_5$. Außerdem sei

$$U_1 := \langle v, f(v) \rangle \quad \text{und} \quad U_2 := \langle w, f(w) \rangle.$$

In [Hup80a, 2.2.b)] ist gezeigt, dass im Fall gerader Charakteristik ein nicht ausgearteter Modul $V = V_1 \oplus V_2$ mit Minimalpolynom $(X+1)^n$ orthogonal unzerlegbar ist, falls V_1, V_2 ausgeartete unzerlegbare Moduln sind (und die Bilinearform auf V symmetrisch oder symplektisch ist).

Da $(v, f(v)) = (e_3, e_4) + (e_5, e_6) = 0$ und $(w, f(w)) = (e_1, e_2) + (e_5, e_6) = 0$ ist, sind U_1 und U_2 ausgeartet. $U_1 + U_2$ ist jedoch nicht ausgeartet, sodass $U_1 \oplus U_2$ ein orthogonal unzerlegbarer f -Modul vom Typ $\text{I}_{(X-1)^2}$ ist. Also ist $V = (U_1 \oplus U_2) \perp (U_1 \oplus U_2)^\perp$ eine Zerlegung von V vom Typ $\text{I}_{(X-1)^2} \perp \text{II}_{(X-1)^2}$.

Für $g \in \mathcal{O}(V)$ sei im Folgenden $\bar{g} \in \text{PO}(V)$ das Bild des kanonischen Epimorphismus. Sei $f \in \mathcal{O}(V)$ und Z eine f -Zerlegung von V . Dann ist Z eine g -Zerlegung von V für alle $g \in \mathcal{O}(V)$ mit $\langle \bar{g} \rangle = \langle \bar{f} \rangle$. Gegebenenfalls sind jedoch der g -Typ und der f -Typ von Z verschieden.

Definition 3.3.2. Ist $f \in \mathcal{O}(V)$ und Z eine f -Zerlegung von V , dann sei

(i) $\tau(\langle f \rangle, Z) := \{ \tau(g, Z) \mid g \in \mathcal{O}(V), \langle g \rangle = \langle f \rangle \}$ der $\langle f \rangle$ -Typ der Zerlegung Z und

(ii) $\tau(\langle \bar{f} \rangle, Z) := \{ \tau(g, Z) \mid g \in \mathcal{O}(V), \langle \bar{g} \rangle = \langle \bar{f} \rangle \}$ der $\langle \bar{f} \rangle$ -Typ von Z .

Unser Ziel ist es nun einen Algorithmus anzugeben, der zu gegebener Ordnung $d \in \mathbb{N}$ Repräsentanten zu allen $\langle \bar{f} \rangle$ -Typen von Zerlegungen berechnet, für die $\langle \bar{f} \rangle \leq \text{PO}(V)$ und $\text{ord}(\bar{f}) = d$ ist.

Beachte: Ist $(k, p) \in \mathcal{T}$ der Typ eines orthogonal unzerlegbaren f -Moduls U und ist $\langle f \rangle = \langle \pm g \rangle$, so hat U als g -Modul den Typ (k, q) , wobei q das Minimalpolynom von g ist. Da sich lediglich die Polynomkomponente des Typs ändert, beschränken wir uns nun auf die Betrachtung der Minimalpolynome.

Notation. Ist $g \in \text{O}(V)$ und W ein g -invarianter Teilraum von V , so bezeichne $\mu_W(g)$ das Minimalpolynom von $g|_W$.

Sei $g = \lambda f^k$ mit $k \in \mathbb{N}$ und $\lambda \in K$ und sei W ein f -invarianter Teilraum von V . Dann hängt das Minimalpolynom von $g|_W$ nur von λ , k und $\mu_W(f)$ ab. Wir können $\mu_W(g)$ wie folgt bestimmen:

Ist $C_{\mu_W(f)}$ die Begleitmatrix des Polynoms $\mu_W(f)$, dann ist $\mu_W(g)$ das Minimalpolynom von $\lambda C_{\mu_W(f)}^k$. Wir führen die folgende Bezeichnung ein:

Notation. Sei $k \in \mathbb{N}$, $\lambda \in K$ und $p \in K[X] \setminus \{0\}$. Dann bezeichne $p^{[\lambda, k]}$ das Minimalpolynom von λC_p^k , wobei C_p die Begleitmatrix des Polynoms p ist.

Sei nun $f \in \text{O}(V)$ und $Z = \{V_1, \dots, V_r\}$ eine f -Zerlegung von V . Definiere

$$\begin{aligned} \mu_Z(f) &:= [\mu_{V_1}(f), \dots, \mu_{V_r}(f)] \quad \text{und} \\ \mu_Z(f)^{[\lambda, k]} &:= [\mu_{V_1}(f)^{[\lambda, k]}, \dots, \mu_{V_r}(f)^{[\lambda, k]}] \end{aligned}$$

für $k \in \mathbb{N}$ und $\lambda \in K$. Außerdem sei

$$T(\langle \bar{f} \rangle, Z) := \{ \mu_Z(g) \mid g \in \text{O}(V), \langle \bar{g} \rangle = \langle \bar{f} \rangle \}.$$

Dann gilt:

$$\begin{aligned} T(\langle \bar{f} \rangle, Z) &= \{ \mu_Z(g) \mid \text{ggT}(\text{ord}(\bar{f}), k) = 1, g = \pm f^k \} \\ &= \{ \mu_Z(f)^{[\lambda, k]} \mid \text{ggT}(\text{ord}(\bar{f}), k) = 1, \lambda = \pm 1 \}. \end{aligned}$$

Sei nun V ein n -dimensionaler K -Raum und $d \in \mathbb{N}$. Des Weiteren sei $G_d := \{ G \leq \text{PO}(V) \mid G \text{ zyklisch, } \text{ord}(G) = d \}$. Mit dem folgenden Schema berechnet man dann alle Zerlegungstypen, die als G -Typ für Gruppen $G \in G_d$ vorkommen können.

- (i) Berechne alle Teiler q von $X^d - 1$ bzw. $X^d + 1$ die in einem zulässigen Typ $(k, q) \in \mathcal{T}$ auftreten.
- (ii) Bilde die Menge M aller Mehrfachmengen von Polynomen, die zu zulässigen Zerlegungstypen gehören, d.h. aller Mehrfachmengen, für die die Summe der Grade kleiner als $n + 1$ ist. Weiterhin muss die Ordnung der zugehörigen Begleitmatrix d sein.

- (iii) Bilde die Klassen $\{m^{[\lambda,k]} \mid \text{ggT}(d,k) = 1, \lambda = \pm 1\}$ der Elemente $m \in M$. Sei $\{m_1, \dots, m_l\}$ ein Repräsentantensystem der Menge dieser Klassen.
- (iv) Ergänze jeden Repräsentanten $m_i = \llbracket q_1, \dots, q_r \rrbracket$ zu einer Liste (nach Definition 3.1.11) zulässiger Typen $\llbracket (k_1, q_1), \dots, (k_j, q_r) \rrbracket$.

Ist d ungerade, so führt die folgende Beobachtung zu einer Vereinfachung: Ist $G \leq \text{PO}(V)$ zyklisch mit $\text{ord}(G) = d$, so gibt es ein $f \in \text{O}(V)$, mit $\text{ord}(f) = \text{ord}(G)$ und $G = \langle \bar{f} \rangle$. Denn ist $f \in \text{O}(V)$ mit $G = \langle \bar{f} \rangle$, dann ist $f^d = \pm 1$. Falls $f^d = -1$ ist, so gilt $\text{ord}(f^2) = a$ und $\langle \bar{f^2} \rangle = G$, da d ungerade ist.

Suchen wir also die Typen von Zerlegungen, die zu zyklischen Gruppen $G \leq \text{PO}(V)$ ungerader Ordnung d gehören können, so genügt es, die Repräsentanten der $\langle f \rangle$ -Typen von Zerlegungen zu Abbildungen $f \in \text{O}(V)$ mit $\text{ord}(f) = d$ zu bestimmen.

In Schritt (i) werden in diesem Fall nur Teiler von $X^d - 1$ berechnet und in Schritt (iii) bildet man dann die Klassen

$$\{m^{[1,k]} \mid \text{ggT}(d,k) = 1\}$$

Eine genauere Formulierung des Verfahrens zur Bestimmung der Zerlegungstypen findet sich in Algorithmus 3.3.3.

Beispiel. Sei $V = V^+(8, 7)$ und $d := 19$. In $\text{GF}(7)[X]$ gilt

$$\begin{aligned} X^{19} - 1 = & (X^3 + 2X - 1)(X^3 + 3X^2 + 3X - 1)(X^3 + 4X^2 + X - 1) \\ & (X^3 + 5X^2 - 1)(X^3 + 4X^2 + 4X - 1)(X^3 - X^2 + 3X - 1)(X - 1). \end{aligned}$$

Ist $f \in \text{O}(V)$ mit $\text{ord}(f) = 19$ und ist Z eine f -Zerlegung von V , so ist Z von einem der folgenden drei Typen:

$$\begin{aligned} & \llbracket \text{III}_{(X^3+2X-1)(X^3+5X^2-1)}, \text{II}_{X-1}, \text{II}_{X-1} \rrbracket \\ & \llbracket \text{III}_{(X^3+3X^2+3X-1)(X^3+4X^2+4X-1)}, \text{II}_{X-1}, \text{II}_{X-1} \rrbracket \\ & \llbracket \text{III}_{(X^3+4X^2+X-1)(X^3-X^2+3X-1)}, \text{II}_{X-1}, \text{II}_{X-1} \rrbracket. \end{aligned}$$

Sei $p_0 := X - 1$, $p_1 := X^3 + 2X - 1$, $p_2 := X^3 + 3X^2 + 3X - 1$ und $p_3 := X^3 + 4X^2 + X - 1$. Dann ist

$$(p_1 p_1^*)^{[1,2]} = p_2 p_2^* \quad \text{und} \quad (p_1 p_1^*)^{[1,4]} = p_3 p_3^*.$$

Das heißt, der $\langle f \rangle$ -Typ von Z ist

$$\{\llbracket \text{II}_{p_0}, \text{II}_{p_0}, \text{III}_{p_1 p_1^*} \rrbracket, \llbracket \text{II}_{p_0}, \text{II}_{p_0}, \text{III}_{p_2 p_2^*} \rrbracket, \llbracket \text{II}_{p_0}, \text{II}_{p_0}, \text{III}_{p_3 p_3^*} \rrbracket\}.$$

Es gibt also ein $g \in \text{O}(V)$, so dass $\langle g \rangle = \langle f \rangle$ und Z eine g -Zerlegung vom Typ $\llbracket \text{II}_{p_0}, \text{II}_{p_0}, \text{III}_{p_1 p_1^*} \rrbracket$ ist.

Algorithmus 3.3.3 Zerlegungs-Typen**Eingabe:** K Körper, $n, d \in \mathbb{N}$ **Ausgabe:** Eine Liste L von Typen von Zerlegungen für die folgendes gilt: Ist V ein n -dimensionaler quadratischer K -Raum und G eine zyklische Untergruppe von $\text{PO}(V)$ der Ordnung d , dann gibt es ein $f \in \text{O}(V)$ mit $\langle \bar{f} \rangle = G$ und eine Zerlegung $V = V_1 \perp \dots \perp V_r$ in orthogonal unzerlegbare f -Moduln, deren Typ in L ist.**procedure** ZERLEGUNGSTYPEN(K, n, d)Sei $\Lambda := \begin{cases} \{1\}, & \text{falls } d \text{ ungerade} \\ \{1, -1\}, & \text{falls } d \text{ gerade.} \end{cases}$ **for** $\lambda \in \Lambda$ **do**Definiere $P := X^d - \lambda \in K[X]$ Berechne eine Faktorisierung $\prod_{i=1}^k p_i^{e_i}$ von P mit irreduziblen, normierten, paarweise teilerfremden Polynomen $p_1, \dots, p_k$.Setze $A := \{p_i^e \mid p_i \text{ symm.}, e < e_i\} \cup \{(p_i p_i^*)^e \mid p_i \text{ unsymm.}, e < e_i\}$

Sei

$$M_\lambda := \left\{ \llbracket q_1, \dots, q_r \rrbracket \mid r \in \mathbb{N}, q_i \in A, \sum_{i=1}^r \deg(q_i) \leq n, \right. \\ \left. \text{kgV}\{q_1, \dots, q_r\} \nmid (X^j \pm 1) \text{ für alle } j < d \right\}$$

for $m \in M_\lambda$ und $k \in N$ mit $\text{ggT}(k, d) = 1$ **do****if** $m^{[1,k]} \neq m$ **then**Entferne $m^{[1,k]}$ aus M_λ .**end if****if** d gerade, $\text{Char}(K) \neq 2$ und $m^{[-1,k]} \neq m$ **then**Entferne $m^{[-1,k]}$ aus M_λ .**end if****end for****end for**Setze $M := \bigcup_{\lambda \in \Lambda} M_\lambda$ und

$$\delta: \mathcal{T} \rightarrow \mathbb{N}, \quad (k, p) \mapsto \begin{cases} 2 \deg(p), & \text{falls } k = \text{I} \\ \deg(p), & \text{falls } k \in \{\text{II}, \text{III}\} \end{cases}$$

Für $m = \llbracket q_1, \dots, q_r \rrbracket \in M$ sei

$$T_m := \left\{ \llbracket (k_1, q_1), \dots, (k_r, q_r) \rrbracket \mid (k_i, q_i) \in \mathcal{T}, \sum_{i=1}^r \delta(k_i, q_i) = n \right\}.$$

return $\bigcup_{m \in M} T_m$ **end procedure**

Wegen Satz 3.2.12 gibt es bis auf Konjugation nur eine Abbildung $f \in O(V)$ vom Typ $\text{III}_{p_1 p_1^*}$. Folglich gibt es bis auf Konjugation nur eine zyklische Untergruppe der Ordnung 19 von $O(V)$.

Nach Lemma 3.2.8 können wir eine Basis B von V so wählen, dass die Matrix M_B von g bezüglich B und die Matrix G_B der Bilinearform auf V bezüglich B wie folgt aussehen:

$$M_B = \left(\begin{array}{ccc|ccc|cc} 0 & 1 & 0 & & & & & \\ 0 & 0 & 1 & & & & & \\ 1 & -2 & 0 & & & & & \\ \hline & & & 2 & 1 & 0 & & \\ & & & 0 & 0 & 1 & & \\ & & & 1 & 0 & 0 & & \\ \hline & & & & & & 1 & \\ & & & & & & & 1 \end{array} \right), \quad G_B = \left(\begin{array}{ccc|ccc|cc} & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ \hline 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ \hline & & & & & & 1 & 1 \end{array} \right).$$

Kapitel 4

Invarianten und Äquivalenz

In diesem Kapitel entwickeln wir einen Äquivalenztest, der zum Klassifizieren von Ovoiden benötigt wird. Der Algorithmus basiert auf der Idee, schrittweise eine Semiähnlichkeit zwischen Ovoiden zu konstruieren. Zur effizienten Berechnung werden dabei Invarianten verwendet, die wir im ersten Abschnitt des Kapitels einführen. Wir schließen das Kapitel mit einer Anwendung des Äquivalenztests zur Berechnung von Ovoidstabilisatoren ab.

4.1 Der Fingerprint

Der „Fingerprint“ ist eine Invariante für Ovoide und Teilovoide, die bei ungerader Charakteristik verwendet werden kann. Sie ist beispielsweise in [Moo93a] und [CD00] beschrieben.

Für $x \in \text{GF}(q)$ sei im Folgenden

$$[x] := \begin{cases} 0, & \text{falls } x = 0 \\ -1, & \text{falls } x \text{ kein Quadrat ist} \\ 1, & \text{sonst} \end{cases}$$

Ist q prim, so ist $[x] = \left(\frac{x}{q}\right)$ das Legendresymbol.

Definition 4.1.1. Sei V ein quadratischer Raum und $\mathcal{O} = \{\langle v_1 \rangle, \dots, \langle v_k \rangle\}$ ein Teilovoid von V . Definiere $A := (a_{ij})$ durch $a_{ij} := [(v_i, v_j)]$ und setze $M := AA^t$. Es sei $M = (m_{ij})$. Für $r \in \mathbb{N}$ definiere $f_r := |\{(i, j) \mid |m_{ij}| = r\}|$. Dann nennen wir $\mathfrak{J}_{\text{fi}}(\mathcal{O}) := (f_0, \dots, f_k)$ den *Fingerprint* von $\mathcal{O}$.

Satz 4.1.2. Sei V ein endlicher quadratischer K -Raum, $\mathcal{O}$ ein Teilovoid von V und $F := \mathfrak{J}_{\text{fi}}(\mathcal{O})$. Dann gilt:

- (i) F ist unabhängig von den in Definition 4.1.1 gewählten Repräsentanten v_i der singulären Punkte von $\mathcal{O}$.

(ii) Ist $\mathcal{O}'$ ein zu $\mathcal{O}$ äquivalentes Teilovoid, so gilt $F = \mathfrak{F}_{\text{fi}}(\mathcal{O}')$.

Beweis. Wir verwenden die Notation aus Definition 4.1.1. Die Einträge der Matrix M sind $m_{ij} = \sum_{l=1}^k [(v_i, v_l)][(v_l, v_j)]$.

Für $1 \leq i \leq k$ seien $\lambda_i \in K^*$ beliebig, dann gilt:

$$\begin{aligned} \sum_l [(\lambda_i v_i, \lambda_l v_l)][(\lambda_l v_l, \lambda_j v_j)] &= \sum_l [\lambda_i \lambda_l (v_i, v_l)][\lambda_l][\lambda_j][(v_l, v_j)] \\ &= \sum_l [\lambda_i][\lambda_j][\lambda_l]^2 [(v_i, v_l)][(v_l, v_j)] \\ &= [\lambda_i][\lambda_j] \sum_l [(v_i, v_l)][(v_l, v_j)] = \pm m_{ij}. \end{aligned}$$

Daraus folgt, dass $\mathfrak{F}_{\text{fi}}$ unabhängig von der Wahl der Repräsentanten ist.

Sei nun $\mathcal{O}'$ ein Teilovoid und γ eine Semiähnlichkeit von V mit Multiplikator s und Körperautomorphismus σ , so dass $\gamma(\mathcal{O}) = \mathcal{O}'$ ist. Dann gilt:

$$\begin{aligned} \sum_l [(\gamma(v_i), \gamma(v_l))][(\gamma(v_l), \gamma(v_j))] &= \sum_l [s \cdot (v_i, v_l)^\sigma][s \cdot (v_l, v_j)^\sigma] \\ &= \sum_l [s]^2 [(v_i, v_l)^\sigma][(v_l, v_j)^\sigma] = m_{ij}. \end{aligned}$$

□

Im Laufe des weiter unten entwickelten Äquivalenztests müssen die Invarianten vieler Teilovoide bestimmt werden. Da die Bestimmung des Fingerprints die Multiplikation zweier Matrizen erfordert, ist das sehr Zeitaufwendig. Die folgenden Varianten des Fingerprints sparen Rechenzeit gegenüber der Berechnung des vollen Fingerprints, wenn eine Äquivalenzabbildung bereits teilweise bekannt ist. Sie benötigen nur $O(|\mathcal{O}|^2)$ bzw. $O(|\mathcal{O}|)$ Rechenoperationen. Dies führt zu einer wesentlich Beschleunigung des Algorithmus.

Definition 4.1.3. Sei $\mathcal{O} = \{\langle v_1 \rangle, \dots, \langle v_k \rangle\}$ ein Teilovoid von V . Für $1 \leq i \leq k$ definiere $f_r^{(i)} := |\{j \mid |\sum_l [(v_i, v_l)][(v_l, v_j)]| = r\}|$. Dann sei

- (i) $\mathfrak{F}_{\text{fi}}(\mathcal{O}, \langle v_i \rangle) := (f_0^{(i)}, \dots, f_k^{(i)})$ und
- (ii) $\mathfrak{F}_{\text{fi}}(\mathcal{O}, \langle v_i \rangle, \langle v_j \rangle) := |\sum_l [(v_i, v_l)][(v_l, v_j)]|$.

Der Beweis von 4.1.2 liefert auch hier die Invarianz:

Lemma 4.1.4. Ist γ eine Semiähnlichkeit von V , dann ist

- (i) $\mathfrak{F}_{\text{fi}}(\mathcal{O}, \langle v_i \rangle) = \mathfrak{F}_{\text{fi}}(\gamma(\mathcal{O}), \langle \gamma(v_i) \rangle)$ und
- (ii) $\mathfrak{F}_{\text{fi}}(\mathcal{O}, \langle v_i \rangle, \langle v_j \rangle) = \mathfrak{F}_{\text{fi}}(\gamma(\mathcal{O}), \langle \gamma(v_i) \rangle, \langle \gamma(v_j) \rangle)$.

4.2 Der Footprint

Wenn die Charakteristik des Körpers 2 ist, dann ist $[(v_i, v_j)] = 0$ für alle paarweise verschiedenen Punkte $\langle v_i \rangle, \langle v_j \rangle$ des Ovoids und der Fingerprint liefert keine Information. Daher geben wir hier eine weitere Invariante an, die auch über Körpern gerader Charakteristik verwendet werden kann.

Definition 4.2.1. Sei $\mathcal{O}$ ein Teilovoid des quadratischen K -Raums V . Sind $u, p \in V$ mit $(u, p) \neq 0$, dann sei $u_p := \frac{u}{(u, p)}$. Für $\langle p \rangle, \langle q \rangle \in \mathcal{O}$ definiere

$$f_{\mathcal{O}, p}: K^* \rightarrow \mathbb{N}$$

$$a \mapsto |\{ \{ \langle v \rangle, \langle w \rangle \} \subseteq \mathcal{O} \setminus \{ \langle p \rangle \} \mid (v_p, w_p) = a \}| \quad \text{und}$$

$$f_{\mathcal{O}, p, q}: K^* \rightarrow \mathbb{N}$$

$$a \mapsto |\{ \langle v \rangle \in \mathcal{O} \setminus \{ \langle p \rangle, \langle q \rangle \} \mid (v_p, q_p) = a \}|.$$

Für $g = f_{\mathcal{O}, p}$ bzw. $g = f_{\mathcal{O}, p, q}$ bezeichne hier $\widetilde{\text{Im}}(g)$ die Mehrfachmenge zum Tupel $(g(a) \mid a \in K^*)$.

- (i) Es sei $\mathfrak{F}_{\text{fo}}(\mathcal{O})$ die Mehrfachmenge zum Tupel $(\widetilde{\text{Im}} f_{\mathcal{O}, p} \mid \langle p \rangle \in \mathcal{O})$. Wir nennen $\mathfrak{F}_{\text{fo}}(\mathcal{O})$ den *Footprint von $\mathcal{O}$* .
- (ii) Für $\langle p \rangle \in \mathcal{O}$ sei $\mathfrak{F}_{\text{fo}}(\mathcal{O}, \langle p \rangle) := \widetilde{\text{Im}} f_{\mathcal{O}, p}$.
- (iii) Sind $\langle p \rangle, \langle q \rangle \in \mathcal{O}$, mit $\langle p \rangle \neq \langle q \rangle$, dann sei $\mathfrak{F}_{\text{fo}}(\mathcal{O}, \langle p \rangle, \langle q \rangle) := \widetilde{\text{Im}} f_{\mathcal{O}, p, q}$.

Wir zeigen, dass die obigen Definitionen nicht von der Wahl der Erzeuger p der Punkte $\langle p \rangle \in \mathcal{O}$ abhängen und dass $\mathfrak{F}_{\text{fo}}$ eine Invariante ist.

Satz 4.2.2. Sei $\mathcal{O}$ ein Teilovoid von V und seien $\langle p \rangle, \langle q \rangle \in \mathcal{O}$ mit $\langle p \rangle \neq \langle q \rangle$. Dann gilt:

- (i) Ist $\lambda \in K^*$, dann ist $\widetilde{\text{Im}} f_{\mathcal{O}, p} = \widetilde{\text{Im}} f_{\mathcal{O}, \lambda p}$ und $\widetilde{\text{Im}} f_{\mathcal{O}, p, q} = \widetilde{\text{Im}} f_{\mathcal{O}, \lambda p, q}$.
- (ii) Ist γ eine Semiähnlichkeit von V , so ist

$$\mathfrak{F}_{\text{fo}}(\mathcal{O}, \langle p \rangle, \langle q \rangle) = \mathfrak{F}_{\text{fo}}(\gamma(\mathcal{O}), \gamma(\langle p \rangle), \gamma(\langle q \rangle)),$$

$$\mathfrak{F}_{\text{fo}}(\mathcal{O}, \langle p \rangle) = \mathfrak{F}_{\text{fo}}(\gamma(\mathcal{O}), \gamma(\langle p \rangle)) \quad \text{und}$$

$$\mathfrak{F}_{\text{fo}}(\mathcal{O}) = \mathfrak{F}_{\text{fo}}(\gamma(\mathcal{O})).$$

Beweis. (i) Da $(v_{\lambda p}, w_{\lambda p}) = \frac{(v, w)}{(v, \lambda p)(w, \lambda p)} = \frac{1}{\lambda^2}(v_p, w_p)$ ist, ist

$$f_{\mathcal{O}, p}(a) = f_{\mathcal{O}, \lambda p}\left(\frac{a}{\lambda^2}\right) \quad \text{und} \quad f_{\mathcal{O}, p, q}(a) = f_{\mathcal{O}, \lambda p, q}\left(\frac{a}{\lambda^2}\right),$$

woraus die Behauptung folgt.

- (ii) Sei γ Semiähnlichkeit mit Multiplikator s und Körperautomorphismus σ . Dann ist

$$\begin{aligned} (\gamma(v)_{\gamma(p)}, \gamma(w)_{\gamma(p)}) &= \frac{(\gamma(v), \gamma(w))}{(\gamma(v), \gamma(p)) (\gamma(w), \gamma(p))} \\ &= \frac{(v, v)^\sigma}{s \cdot (v, p)^\sigma (v, p)^\sigma} = \frac{1}{s} (v_p, w_p)^\sigma. \end{aligned}$$

Es folgt $f_{\gamma(\mathcal{O}), \gamma(p)}(\frac{a^\sigma}{s}) = f_{\mathcal{O}, p}(a)$. Also ist $\widetilde{\text{Im}} f_{\gamma(\mathcal{O}), \gamma(p)} = \widetilde{\text{Im}} f_{\mathcal{O}, p}$ und somit $\mathfrak{I}_{\text{fo}}(\mathcal{O}) = \mathfrak{I}_{\text{fo}}(\gamma(\mathcal{O}))$. Analog ist $\mathfrak{I}_{\text{fo}}(\mathcal{O}, \langle p \rangle, \langle q \rangle) = \mathfrak{I}_{\text{fo}}(\gamma(\mathcal{O}), \gamma(\langle p \rangle), \gamma(\langle q \rangle))$. $\square$

Tabelle 4.1 enthält die Footprints der bekannten Ovoide in $V^+(8, q)$ für $q = 7, 8, 9$. Die Beschreibungen dieser Ovoide finden sich in Kapitel 2. In der rechten Spalte der Tabelle geben die Exponenten die Vielfachheiten der Elemente in der jeweiligen Mehrfachmenge an.

Typ	q	Footprint
Dye-Ovoid	8	$\{\{12544^{(3)}, 23296^{(4)}\}^{(9)}, \{17248, 18400^{(3)}, 19456^{(3)}\}^{(504)}\}$
desarguessches Ovoid	8	$\{\{18688^{(7)}, \}^{(513)}\}$
unitäres Ovoid	8	$\{\{18688^{(7)}\}^{(513)}\}$
unitäres Ovoid	9	$\{\{29889^{(4)}, 36450^{(4)}\}^{(730)}\}$
ternäres Ovoid	7	$\{\{8085, 8477, 8575, 10290, 11221, 12005\}^{(64)}, \{8147, 8475, 9015, 10321, 11203, 11492\}^{(280)}\}$
binäres Ovoid	7	$\{\{8575, 8967, 9653, 9800, 10339, 11319\}^{(288)}, \{8676, 8739, 8811, 9099, 10989, 12339\}^{(56)}\}$

Tabelle 4.1: Der Footprint für einige Ovoide von $V^+(8, q)$

Es fällt auf, dass das unitäre und das desarguessche Ovoid den selben Footprint haben. Dies ist für alle endlichen Körper der Charakteristik 2 der Fall, wie wir im Folgenden sehen werden.

Satz 4.2.3. *Sei $K = \text{GF}(q)$ mit geradem q , V ein quadratischer K -Raum und sei $\mathcal{O}$ das desarguessche oder das unitäre Ovoid von V . Sind $\langle p \rangle, \langle v \rangle \in \mathcal{O}$ mit $\langle p \rangle \neq \langle v \rangle$ und ist $k \in K^*$, so gilt*

$$|\{\langle w \rangle \in \mathcal{O} \setminus \{\langle p \rangle, \langle v \rangle\} \mid (v_p, w_p) = k\}| = \frac{|\mathcal{O}| - 2}{|K^*|} = q^2 + q + 1.$$

Beweis. Sei $\mathcal{O}$ das desarguessche Ovoid. Wir verwenden die Notation aus Abschnitt 2.3. Nach [Kan82a, 7.] operiert $\text{PSL}(2, q^3)$ dreifach transitiv auf $\mathcal{O}$. Deshalb können wir o.B.d.A. annehmen, dass $p = (0, 0, 0, 1)$ und $v = (1, 0, 0, 0)$ ist.

Ist $\langle w \rangle \in \mathcal{O}$ mit $\langle w \rangle \neq \langle p \rangle$, so gibt es ein $t \in L$, so dass $w = (1, t, t^{q^2+q}, N(t))$. Es ist $(w, p) = Q(p + w) = 1 + N(t) + T(t^{q^2+q+1}) = 1$, also $w_p = w$ und es gilt

$$\begin{aligned} (v_p, w_p) &= (v, w) = Q(v + w) = Q(0, t, t^{q^2+q}, t^{q^2+q+1}) \\ &= T(t^{q^2+q+1}) = t^{q^2+q+1} = N(t). \end{aligned}$$

Für beliebiges $k \in K^*$ ist

$$|\{t \in L^* \mid N(t) = k\}| = |\text{Kern}(N|_{L^*})| = \frac{|L^*|}{|K^*|} = q^2 + q + 1,$$

woraus die Behauptung folgt.

Betrachte nun das unitäre Ovoid. Wir verwenden die Notationen aus 2.1. Nach [Kan82a, 4.] operiert $\text{GU}(3, q)$ als zweifach transitive Gruppe von Automorphismen auf dem unitären Ovoid. Sei also hier o.B.d.A. $p = X_\infty$ und $v := X(0, 0)$.

Für alle $\rho, \sigma \in L$ ist $(X_\infty, X(\rho, \sigma)) = 1$ und für $w = \langle X(\rho, \sigma) \rangle \in \mathcal{O}$ gilt $(v_p, w_p) = (X(0, 0), X(\rho, \sigma)) = N(\rho)$. Ist nun $k \in K^*$, so ist

$$\begin{aligned} &|\{X(\rho, \sigma) \mid N(\sigma) = T(\rho), N(\rho) = k\}| \\ &= |\{X(\rho, \sigma) \mid \rho \in L \setminus K, N(\sigma) = T(\rho), N(\rho) = k\} \dot{\cup} \{X(\rho, 0) \mid \rho \in K, N(\rho) = k\}| \\ &= \left(\bigcup_{\substack{\rho \in L \setminus K, \\ N(\rho) = k}} \{X(\rho, \sigma) \mid \sigma \in L^*, N(\sigma) = T(\rho)\} \right) \dot{\cup} \{X(\rho, 0) \mid \rho \in K, N(\rho) = k\}. \end{aligned}$$

Es folgt:

$$\begin{aligned} &|\{\langle w \rangle \in \mathcal{O} \setminus \{\langle p \rangle, \langle v \rangle\} \mid (v_p, w_p) = k\}| = |\{X(\rho, \sigma) \mid N(\sigma) = T(\rho), N(\rho) = k\}| \\ &= |\{\rho \in L \setminus K \mid N(\rho) = k\}| \cdot \frac{|L^*|}{|K^*|} + |\{\rho \in K \mid N(\rho) = k\}| \\ &= \left(\frac{|L^*|}{|K^*|} - 1 \right) (q + 1) + 1 = q^2 + q + 1. \end{aligned}$$

□

4.3 Die Dimensionsinvariante

Wie in Abschnitt 4.2 gesehen, unterscheidet die Invariante $\mathfrak{J}_{\text{fo}}$ das unitäre Ovoid und das desarguessche Ovoid nicht. Um diesen Mangel auszugleichen, definieren wir eine weitere Invariante, die für diese beiden Ovoids verschiedene Werte liefert.

Definition 4.3.1. Sei $\mathcal{C}$ ein Teilovoid eines quadratischen K -Raums V . Dann sei $\langle \mathcal{C} \rangle$ der kleinste Teilraum von V , so dass $\mathcal{C}$ in der Menge der singulären Punkte von V enthalten ist. Insbesondere sei $\dim \langle \mathcal{C} \rangle$ die K -Vektorraum-Dimension von $\langle \mathcal{C} \rangle$. Wir sagen auch, dass $\mathcal{C}$ die Dimension $\dim \langle \mathcal{C} \rangle$ hat.

Für beliebige paarweise verschiedene $p_1, \dots, p_4 \in \mathcal{O}$ ist $\dim \langle p_1, \dots, p_4 \rangle \in \{3, 4\}$, denn $\langle p_1, p_2 \rangle$ ist eine hyperbolische Ebene, die außer p_1 und p_2 keine singulären Punkte enthält. Das heißt $\dim \langle p_1, p_2, p_3 \rangle = 3$.

Definition 4.3.2. Sei V ein nicht ausgearteter quadratischer Raum und $\mathcal{O}$ ein Teilovoid von V . Setze

$$\mathfrak{J}_{\dim}(\mathcal{O}) := |\{M \subseteq \mathcal{O} \mid |M| = 4, \dim \langle M \rangle = 3\}|.$$

Offensichtlich ist $\mathfrak{J}_{\dim}$ invariant unter Semiähnlichkeiten.

Satz 4.3.3. Sei $\mathcal{O}$ das desarguessche Ovoid in $V^+(8, q)$. Für alle $M \subseteq \mathcal{O}$ mit $|M| = 4$ gilt $\dim \langle M \rangle = 4$.

Beweis. Es werden die Bezeichnungen aus Abschnitt 2.3 verwendet. Sei $M = \{\langle p_1 \rangle, \dots, \langle p_4 \rangle\} \subseteq \mathcal{O}$ mit $|M| = 4$. Sei o.B.d.A. $p_1 = (0, 0, 0, 1)$ und $p_2 = (1, 0, 0, 0)$ und für $i \in \{3, 4\}$ sei $t_i \in L$ mit $p_i = (1, t_i, t_i^{q^2+q}, N(t_i))$. Sind nun $\lambda_1, \dots, \lambda_4 \in K$ mit $\sum \lambda_i p_i = 0$, dann folgt

$$\lambda_3 t_3 + \lambda_4 t_4 = 0 \quad \text{und} \quad \lambda_3 t_3^{q^2+q} + \lambda_4 t_4^{q^2+q} = 0.$$

Nimmt man die zweite Gleichung hoch q^2 , so ergibt sich

$$\lambda_3 t_3 = \lambda_4 t_4 \quad \text{und} \quad \lambda_3 t_3^{q+1} + \lambda_4 t_4^{q+1} = 0.$$

Also gilt $0 = \lambda_4 t_4 t_3^q + \lambda_4 t_4^{q+1} = \lambda_4 t_4 (t_3 + t_4)^q$. Da $\langle p_1 \rangle, \dots, \langle p_4 \rangle$ paarweise verschieden sind, folgt $\lambda_4 = 0$. Wegen $\dim \langle p_1, p_2, p_3 \rangle = 3$ folgt $\lambda_1 = \lambda_2 = \lambda_3 = 0$, und somit ist $\dim \langle p_1, \dots, p_4 \rangle = 4$. $\square$

Satz 4.3.4. Sei V ein quadratischer $\text{GF}(q)$ -Raum mit geradem q und sei $\mathcal{O}$ das unitäre Ovoid von V . Sind $\langle p_1 \rangle \neq \langle p_2 \rangle \in \mathcal{O}$ beliebig, dann gilt

$$|\{M \subseteq \mathcal{O} \mid |M| = 4, \langle p_1 \rangle, \langle p_2 \rangle \in M, \dim \langle M \rangle = 3\}| = \binom{q-1}{2}$$

Beweis. Wir verwenden die Notationen aus Abschnitt 2.1. Sei o.B.d.A. $p_1 = X_\infty$ und $p_2 = X(0, 0)$. Außerdem seien $\langle p_3 \rangle, \langle p_4 \rangle \in \mathcal{O}$ mit $p_i = X(\rho_i, \sigma_i)$ und $\rho_i, \sigma_i \in L$, so dass $\langle p_1 \rangle, \dots, \langle p_4 \rangle$ paarweise verschieden sind.

Zeige dass $\{p_1, \dots, p_4\}$ genau dann linear abhängig ist, wenn $\sigma_3 = \sigma_4 = 0$ ist. „ $\Leftarrow$ “: Ist $X(\rho, 0) \in \mathcal{O}$, so ist $T(\rho) = N(0) = 0$, das heißt $\bar{\rho} = \rho$.

Sei nun $\sigma_3 = \sigma_4 = 0$. Dann gilt für $\lambda_1, \dots, \lambda_4 \in \text{GF}(q)$:

$$\sum_{i=1}^4 \lambda_i p_i = \begin{pmatrix} \lambda_3 \rho_3 + \lambda_4 \rho_4 & 0 & \lambda_1 + \lambda_3 N(\rho_3) + \lambda_4 N(\rho_4) \\ 0 & 0 & 0 \\ \lambda_2 + \lambda_3 + \lambda_4 & 0 & \lambda_3 \rho_3 + \lambda_4 \rho_4 \end{pmatrix}$$

Setze $\lambda_4 := 1$, $\lambda_3 := \rho_4 \rho_3^{-1}$, $\lambda_2 := \rho_4 \rho_3^{-1} + 1$ und $\lambda_1 := N(\rho_4) + \rho_4 \rho_3^{-1} N(\rho_3)$. Da q gerade ist, ergibt sich $\sum \lambda_i p_i = 0$.

„ $\Rightarrow$ “: Sei jetzt $\sigma_4 \neq 0$ und es gelte $\sum \lambda_i p_i = 0$. Das heißt,

$$0 = \sum_{i=1}^4 \lambda_i p_i = \begin{pmatrix} * & \lambda_3 \bar{\rho}_3 \sigma_3 + \lambda_4 \bar{\rho}_4 \sigma_4 & * \\ * & * & * \\ * & \lambda_3 \sigma_3 + \lambda_4 \sigma_4 & \lambda_3 \rho_3 + \lambda_4 \rho_4 \end{pmatrix}$$

Aus $\lambda_3 \sigma_3 + \lambda_4 \sigma_4 = \lambda_3 \bar{\rho}_3 \sigma_3 + \lambda_4 \bar{\rho}_4 \sigma_4 = 0$ ergibt sich $\lambda_4 \sigma_4 (\bar{\rho}_3 + \bar{\rho}_4) = 0$. Damit ist $\lambda_4 = 0$ oder $\rho_3 = \rho_4$. Falls $\rho_3 = \rho_4$ ist, folgt $\lambda_3 = \lambda_4$ und weiter $\sigma_3 = \sigma_4$, was ein Widerspruch zu $\langle p_3 \rangle \neq \langle p_4 \rangle$ ist. Das heißt $\lambda_4 = 0$. Die Vektoren p_1, p_2, p_3 sind aber linear unabhängig, woraus folgt, dass auch $\lambda_1 = \lambda_2 = \lambda_3 = 0$ ist. Also ist $\{p_1, \dots, p_4\}$ linear unabhängig.

Damit ist $\{p_1, \dots, p_4\}$ genau dann linear abhängig, wenn $\sigma_1 = \sigma_2 = 0$ ist, das heißt genau dann, wenn $T(\rho_3) = T(\rho_4) = 0$ ist, also genau dann wenn $\rho_3, \rho_4 \in K = \text{GF}(q)$ sind. Da $p_3, p_4 \neq p_2$ ist genau dann, wenn $\rho_3, \rho_4 \neq 0$ gilt, ergibt dies genau $\binom{|K^*|}{2}$ verschiedene Möglichkeiten für (ρ_3, ρ_4) , so dass $\{p_1, \dots, p_4\}$ linear abhängig ist. $\square$

Die Invariante $\mathfrak{I}_{\text{dim}}$ unterscheidet also das unitäre Ovoid vom desarguesschen Ovoid. Allerdings ist die Berechnung der Dimensionsinvariante recht aufwändig, sie wird daher nur verwendet, falls $\mathfrak{I}_{\text{fo}}$ nicht genug Information liefert.

4.4 Äquivalenztest

Wir geben in diesem Abschnitt einen Algorithmus an, der testet, ob zwei gegebene Ovoide äquivalent sind. Zwei Ovoide $\mathcal{O}$ und $\mathcal{O}'$ heißen äquivalent, wenn es eine Semiähnlichkeit gibt, die $\mathcal{O}$ auf $\mathcal{O}'$ abbildet. Im Falle äquivalenter Ovoide konstruiert der Algorithmus eine solche Semiähnlichkeit explizit. Wir formulieren den Algorithmus hier für Teilovoide, um ihn auch in Kapitel 5 bei der Ovoidsuche verwenden zu können.

Der Äquivalenztest, formuliert in Algorithmus 4.4.2, funktioniert folgendermaßen: Seien $\mathcal{O}$ und $\mathcal{O}'$ zwei Teilovoide und $(b_1, \dots, b_n)$ eine Basis von V , so dass $\langle b_i \rangle \in \mathcal{O}$ ist für $1 \leq i \leq \ell := \dim \langle \mathcal{O} \rangle \leq n$. Der Algorithmus sucht zunächst systematisch Bilder $P_1, \dots, P_\ell \in \mathcal{O}'$ für die Punkte $\langle b_1 \rangle, \dots, \langle b_\ell \rangle$. Die Invarianten $\mathfrak{I}_{\text{fi}}$ und $\mathfrak{I}_{\text{fo}}$ aus den Abschnitten 4.1 und 4.2 werden dabei verwendet, um nicht in Frage kommende Bilder frühzeitig auszuschließen. Mit dem unten angegebenen Satz 4.4.1 wird festgestellt, welche Erzeuger der Punkte $P_1, \dots, P_\ell$ als Bilder von $b_1, \dots, b_\ell$ in Frage kommen. Dies liefert eine Abbildung $\psi: \langle b_i \mid 1 \leq i \leq \ell \rangle \rightarrow V$. Falls $\ell < n$ ist, wird die Abbildung am Ende gegebenenfalls auf ganz V fortgesetzt.

Ist $0 \leq i_0 \leq \ell$ und $\varphi: \langle b_i \mid 1 \leq i \leq i_0 \rangle \rightarrow V$, so dass $\langle \varphi(b_i) \rangle \in \mathcal{O}'$ ist für $1 \leq i \leq i_0$, so ruft man Algorithmus 4.4.2 mit den Parametern $(\mathcal{O}, \mathcal{O}', (b_1, \dots, b_n))$,

φ, i_0) auf, um zu testen, ob es eine Semiähnlichkeit ψ gibt mit $\langle \varphi(b_i) \rangle = \langle \psi(b_i) \rangle$ für $1 \leq i \leq i_0$, welche $\mathcal{O}$ auf $\mathcal{O}'$ abbildet. Das Verfahren verläuft rekursiv: Die Funktion berechnet die möglichen Fortsetzungen von φ zu einer auf $b_1, \dots, b_{i_0+1}$ definierten Abbildung φ' und ruft sich für jede der gefundenen Fortsetzungen selbst auf. Die Parameter für den erneuten Aufruf sind dabei $(\mathcal{O}, \mathcal{O}', (b_1, \dots, b_n), \varphi', i_0 + 1)$. Für den vollen Äquivalenztest ruft man Algorithmus 4.4.2 also mit der leeren Abbildung als φ und $i_0 := 0$ auf.

Algorithmus 4.4.2 setzt Teilovoide der Länge mindestens 3 voraus, da er Satz 4.4.1 verwendet. Dies ist aber in der Praxis keine große Einschränkung.

Satz 4.4.1. *Sei V ein quadratischer K -Raum und ψ eine σ -Ähnlichkeit von V mit Multiplikator s . Des Weiteren sei $n \geq 3$ und es seien $\langle b_1 \rangle, \dots, \langle b_n \rangle$ paarweise verschiedene Punkte von $\mathcal{O}$. Sind $v_1, \dots, v_n \in V$, so dass $\psi(b_1) = v_1$ und $\langle \psi(b_i) \rangle = \langle v_i \rangle$ ist für $1 < i \leq n$, dann gilt:*

$$s = \frac{(b_2, b_3)^\sigma (v_1, v_2)(v_1, v_3)}{(v_2, v_3)(b_1, b_2)^\sigma (b_1, b_3)^\sigma}$$

und für $1 < i \leq n$ ist $\psi(b_i) = \lambda_i v_i$, wobei $\lambda_i = s \frac{(b_1, b_i)^\sigma}{(v_1, v_i)}$.

Beweis. Es existieren $\lambda_1, \dots, \lambda_n \in K$, so dass $\psi(b_i) = \lambda_i v_i$, dabei ist $\lambda_1 = 1$. Da ψ eine Ähnlichkeit ist, gilt für alle $i, j \in \{1, \dots, n\}$

$$s \cdot (b_i, b_j)^\sigma = (\psi(b_i), \psi(b_j)) = \lambda_i \lambda_j (v_i, v_j).$$

Insbesondere folgt für $j = 1$

$$\lambda_i = s \cdot \frac{(b_1, b_i)^\sigma}{(v_1, v_i)} \quad \text{für } 1 < i \leq n.$$

Außerdem ist

$$\begin{aligned} (b_2, b_3)^\sigma &= \frac{1}{s} \cdot \lambda_2 \lambda_3 (v_2, v_3) \\ &= s \cdot \frac{(b_1, b_2)^\sigma}{(v_1, v_2)} \cdot \frac{(b_1, b_3)^\sigma}{(v_1, v_3)} \cdot (v_2, v_3). \end{aligned}$$

Also ist $s = \frac{(v_1, v_2)}{(b_1, b_2)^\sigma} \frac{(v_1, v_3)}{(b_1, b_3)^\sigma} \frac{(b_2, b_3)^\sigma}{(v_2, v_3)}$. □

Algorithmus 4.4.2 Äquivalenztest für Teilovoide

Eingabe: $\mathcal{O}$, $\mathcal{O}'$ Teilovoide des quadratischen K -Raums V mit $\ell := \dim(\langle \mathcal{O} \rangle) = \dim(\langle \mathcal{O}' \rangle) \geq 3$ und $(b_1, \dots, b_n)$ Basis von V , so dass $\langle b_i \rangle \in \mathcal{O}$ für $1 \leq i \leq \ell \leq n$.

Weiter $0 \leq i_0 \leq \ell$ und $\varphi: \{b_i \mid 1 \leq i \leq i_0\} \rightarrow V$, so dass $\langle \varphi(b_i) \rangle \in \mathcal{O}'$ für $1 \leq i \leq i_0$.

Ausgabe: Semiähnlichkeit ψ von V , mit $\psi(\mathcal{O}) = \mathcal{O}'$ und $\psi(\langle b_i \rangle) = \langle \varphi(b_i) \rangle$ für $i \leq i_0$, falls eine solche existiert, $\emptyset$ sonst.

procedure OVOID-ÄQUIVALENZ($\mathcal{O}$, $\mathcal{O}'$, $(b_1, \dots, b_n)$, φ , i_0)

if $i_0 \geq 3$ **then**

 Setze $\Sigma := \{\sigma \mid \sigma \in \text{Aut}(K)\}$.

for $\sigma \in \text{Aut}(K)$ **do** # Verwende Satz 4.4.1:

 Setze $s_\sigma := \frac{(b_2, b_3)^\sigma (\varphi(b_1), \varphi(b_2)) (\varphi(b_1), \varphi(b_3))}{(\varphi(b_2), \varphi(b_3)) (b_1, b_2)^\sigma (b_1, b_3)^\sigma}$,

$\lambda_1 := 1$ und $\lambda_k := s_\sigma \frac{(b_1, b_k)}{(\varphi(b_1), \varphi(b_k))}$ für $2 \leq k \leq i_0$.

 Definiere $\psi_\sigma: \langle b_1, \dots, b_{i_0} \rangle \rightarrow V$ durch $\sum a_i b_i \mapsto \sum a_i^\sigma \lambda_i \varphi(b_i)$.

 # Teste, ob sich ψ_σ auf Definitionsbereich wie Semiähnlichkeit verhält:

if $\exists i \in \{1, \dots, i_0\}: Q(\psi_\sigma(b_i)) \neq s_\sigma Q(b_i)^\sigma$ **oder**

$\exists i, j \in \{1, \dots, i_0\}: (\psi_\sigma(b_i), \psi_\sigma(b_j)) \neq s_\sigma (b_i, b_j)^\sigma$ **then**

 Entferne σ aus Σ .

end if

if $\Sigma = \emptyset$ **then return** $\emptyset$

end if

end for

end if

if $i_0 = \ell$ **then**

for $\sigma \in \Sigma$ **do**

if $\psi_\sigma(\mathcal{O}) = \mathcal{O}'$ und $\exists$ Fortsetzung $\widehat{\psi}_\sigma$, von ψ_σ auf V **then**

return $\widehat{\psi}_\sigma$

end if

end for

else

for $\langle x \rangle \in \mathcal{O}' \setminus \{\langle \varphi(b_1) \rangle, \dots, \langle \varphi(b_{i_0}) \rangle\}$ **do**

 Setze $\varphi(b_{i_0+1}) := x$.

 Sei $\mathcal{C} := \mathcal{O} \setminus \{\langle b_1 \rangle, \dots, \langle b_{i_0+1} \rangle\}$ und $\mathcal{C}' := \mathcal{O}' \setminus \{\langle \varphi(b_1) \rangle, \dots, \langle \varphi(b_{i_0+1}) \rangle\}$.

 Sei $\text{fPrint} := \mathfrak{J}_{\text{fo}}$, falls $\text{Char}(K) = 2$ und $\text{fPrint} := \mathfrak{J}_{\text{fi}}$ sonst.

if $\text{fPrint}(\mathcal{C}, \langle b_k \rangle, \langle b_{i_0+1} \rangle) = \text{fPrint}(\mathcal{C}', \varphi(\langle b_k \rangle), \langle x \rangle)$ für $1 \leq k \leq i_0$ **then**

if $i_0 > 0$ **or** $\text{fPrint}(\mathcal{C}', \langle x \rangle) = \text{fPrint}(\mathcal{C}, \langle b_{i_0+1} \rangle)$ **then**

 Setze $\psi_x := \text{OVOID-ÄQUIVALENZ}(\mathcal{O}, \mathcal{O}', (b_1, \dots, b_n), \varphi, i_0 + 1)$

if $\psi_x \neq \emptyset$ **then return** ψ_x

end if

end if

end for

end if

return $\emptyset$

end procedure

Sei nun $O := \{\mathcal{O}_1, \dots, \mathcal{O}_r\}$ eine Menge von Teilovoiden gleicher Länge und gleicher Dimension. Um die Elemente von O auf Äquivalenz zu testen, partitioniert man O zunächst mit Hilfe einer der Invarianten $\mathfrak{I}$, die in den Abschnitten 4.1 bis 4.3 beschrieben wurden. Für jedes Element der Partition wird dann ein Äquivalenztest gegen ein „Prototyp“-Teilovoid durchgeführt (z.B. bei vollen Ovoiden ein bekanntes Ovoid mit gleicher Invariante).

Im Fall ungerader Charakteristik wird dabei als Invariante $\mathfrak{I}$ immer $\mathfrak{I}_{\text{fi}}$ verwendet. Bei gerader Charakteristik verwenden wir $\mathfrak{I}_{\text{fo}}$ als Invariante für Teilovoide.

Für volle achtdimensionale Ovoide über $\text{GF}(q)$ kommt, falls q gerade und $q \equiv 2 \pmod{3}$ ist, die Dimensionsinvariante als weiteres Kriterium zum Einsatz, da hier das desarguessche und das unitäre Ovoid auftreten können, die den selben Footprint haben. Hat ein Ovoid $\mathcal{O}$ den Footprint des desarguesschen/unitären Ovoids, so verwenden wir die Sätze 4.3.3 und 4.3.4: Man wählt zwei Punkte $P_1, P_2 \in \mathcal{O}$ und berechnet

$$|\{M \subseteq \mathcal{O} \mid |M| = 4, P_1, P_2 \in M, \dim \langle M \rangle = 3\}|.$$

Anhand dieses Wertes lässt sich nach Satz 4.3.3 und 4.3.4 das desarguessche Ovoid vom unitären Ovoid unterscheiden. Hierbei ist der Rechenaufwand deutlich geringer bei der Verwendung der „vollen“ Dimensionsinvariante, allerdings ist nicht mehr garantiert, dass Ovoide mit verschiedenen Werten auch wirklich inäquivalent sind (nur das desarguessche und das unitäre Ovoid werden zuverlässig unterschieden). Hier werden also gegebenenfalls weitere Äquivalenztest am Ende der Berechnungen nötig.

Zur Basiswahl

Algorithmus 4.4.2 verlangt als Eingabe eine Basis von V . Die Laufzeit des Algorithmus hängt von der Wahl der Basiselemente $b_1, \dots, b_\ell$ ab. Wir geben hier eine Wahl für $b_1, \dots, b_\ell$ an, die möglich ist, falls der Stabilisator von $\mathcal{O}$ in $\text{PGO}(V)$ bekannt ist, und die eine effektive Berechnung verspricht.

Seien $\mathcal{O}$ und $\mathcal{O}'$ Ovoide des quadratischen Raums V . Für $\mathcal{C} \subseteq \mathcal{O}$ sei außerdem

$$S_{\mathcal{O}, \mathcal{C}} := \{g \in \text{Stab}_{\text{GO}(V)}(\mathcal{O}) \mid g(P) = P \text{ für alle } P \in \mathcal{C}\}.$$

Ist $\gamma \in \text{GO}(V)$ mit $\gamma(\mathcal{O}) = \mathcal{O}'$, dann ist

$$\gamma S_{\mathcal{O}, \mathcal{C}} = \{\gamma' \in \text{GO}(V) \mid \gamma'(\mathcal{O}) = \mathcal{O}', \gamma'|_{\mathcal{C}} = \gamma|_{\mathcal{C}}\}$$

Für $x \in \mathcal{O}$ gibt es dann $|\gamma(x^{S_{\mathcal{O}, \mathcal{C}}})| = |x^{S_{\mathcal{O}, \mathcal{C}}}|$ mögliche Bildpunkte in $\mathcal{O}'$ unter Semiähnlichkeiten γ' für die $\gamma'(\mathcal{O}) = \mathcal{O}'$ und $\gamma'|_{\mathcal{C}} = \gamma|_{\mathcal{C}}$ gilt. Liegt $x \in \mathcal{O}$ also in einer langen Bahn von $S_{\mathcal{O}, \mathcal{C}}$, so gibt es viele mögliche Bilder von x unter Äquivalenzabbildungen zwischen $\mathcal{O}$ und $\mathcal{O}'$, die die Abbildung $\gamma|_{\mathcal{C}}$ fortsetzen. Es ist also – im Mittel wie im worst case – einfacher, ein „zulässiges“ Bild von x zu finden. Deshalb wird man bei der Basiswahl folgendermaßen vorgehen:

Sei $0 \leq k < \ell = \dim(\langle \mathcal{O} \rangle)$ und seien $b_1, \dots, b_k$ linear unabhängige Elemente von V mit $\langle b_i \rangle \in \mathcal{O}$ als Basiselemente gewählt. Man berechnet dann die Bahnenzerlegung von $\mathcal{O}$ unter $S_{\mathcal{O}, \{\langle b_1 \rangle, \dots, \langle b_k \rangle\}}$ und wählt den $(k+1)$ -ten Basisvektor $b_{k+1} \in V$, so dass $\langle b_{k+1} \rangle$ in einer möglichst langen Bahn liegt.

4.5 Stabilisatoren von Ovoiden

Mit Hilfe von Algorithmus 4.4.2 lässt sich auch der Stabilisator von Ovoiden in $\Gamma\mathcal{O}$ berechnen.

Sei V ein quadratischer Raum und $\mathcal{O}$ ein Ovoid von V . Sei weiterhin $\ell := \dim \langle \mathcal{O} \rangle$ und $b_1, \dots, b_n$ eine Basis von V mit $\langle b_i \rangle \in \mathcal{O}$ für $i \leq \ell$. Definiere $S_0 := \text{Stab}_{\Gamma\mathcal{O}(V)}(\mathcal{O})$ und

$$S_k := \{f \in S_0 \mid f(\langle b_i \rangle) = \langle b_i \rangle \text{ für } 1 \leq i \leq k\}$$

für $1 \leq k \leq \ell$. Wegen $S_\ell \leq S_{\ell-1} \leq \dots \leq S_0 = \text{Stab}_{\Gamma\mathcal{O}(V)}(\mathcal{O})$ genügt es also zunächst S_ℓ und dann S_{i-1} aus S_i für $1 \leq i \leq \ell$ zu berechnen. Dazu verwenden wir das folgende Lemma.

Lemma 4.5.1. *Sei $i_0 \geq 0$, $p \in \mathcal{O}$ und $M := \{g \in S_{i_0-1} \mid g(\langle b_{i_0} \rangle) \in \langle p \rangle^{S_{i_0}}\}$. Dann gilt:*

- (i) *Es gibt genau dann ein $f \in S_{i_0-1}$ mit $f(\langle b_{i_0} \rangle) = p$, wenn $M \neq \emptyset$ ist.*
- (ii) *Ist $f \in S_{i_0-1}$ mit $f(\langle b_{i_0} \rangle) = p$, dann ist $M \subseteq \langle S_{i_0} \cup f \rangle$.*

Beweis. (i) Sei $g \in M$. Dann gibt es ein $\varphi \in S_{i_0}$ mit $\varphi(p) = g(\langle b_{i_0} \rangle)$ und es ist $f := \varphi^{-1} \circ g \in S_{i_0-1}$ mit $f(\langle b_{i_0} \rangle) = p$.

(ii) Sei $g \in M$ und $\varphi \in S_{i_0}$ mit $\varphi(p) = g(\langle b_{i_0} \rangle)$. Dann ist $\psi := f^{-1} \circ \varphi^{-1} \circ g \in S_{i_0-1}$ mit $\psi(\langle b_{i_0} \rangle) = \langle b_{i_0} \rangle$. Also ist $\psi \in S_{i_0}$ und $g = \varphi \circ f \circ \psi \in \langle S_{i_0} \cup f \rangle$. $\square$

Nun lässt sich $\text{Stab}_{\Gamma\mathcal{O}(V)}(\mathcal{O})$ wie folgt bestimmen. Zunächst berechnen wir mit Hilfe von Satz 4.4.1 die Gruppe S_ℓ . Ist $1 \leq i_0 \leq \ell$ und S_{i_0} bekannt, dann berechnet sich S_{i_0-1} folgendermaßen:

1. Berechne eine Bahnenzerlegung

$$\mathcal{O} = \bigcup_{1 \leq j \leq r} \langle x_j \rangle^{S_{i_0}}$$

mit passendem $r \in \mathbb{N}$.

2. Wir verwenden Algorithmus 4.4.2 von Seite 50: Für $1 \leq j \leq r$ definiere $\varphi_j(b_i) := b_i$, falls $1 \leq i \leq i_0 - 1$ und $\varphi_j(b_{i_0}) := x_j$ und berechne nach Algorithmus 4.4.2

$$f_j := \text{OVOID-ÄQUIVALENZ}(\mathcal{O}, \mathcal{O}, (b_1, \dots, b_n), \varphi_j, i_0).$$

Dann ist $f_j \in S_{i_0-1}$ mit $f_j(\langle b_{i_0} \rangle) = \langle x_j \rangle$, falls eine solche Abbildung existiert, ansonsten ist $f_j = \emptyset$.

3. Setze

$$S' := \{f_j \mid 1 \leq j \leq r, f_j \neq \emptyset\}.$$

Aus Lemma 4.5.1 folgt, dass $\langle S_{i_0} \cup S' \rangle = S_{i_0-1}$ ist.

Kapitel 5

Ovoidsuche in $V^+(2n, q)$

Wir entwickeln hier einen Algorithmus zur Ovoidsuche in $V = V^+(2n, q)$. Da eine systematische Suche nach allen Ovoiden zu aufwändig ist, beschränken wir uns darauf, alle Ovoiden von V zu finden, die invariant unter einer Gruppe $1 \neq G \leq \Gamma\text{O}(V)$ sind. In diesem Fall vereinfacht sich die Suche, da dann jedes Ovoid Vereinigung von G -Bahnen ist.

Wir beginnen das Kapitel mit der Beschreibung einiger Hilfsmittel, die zur Beschleunigung der systematischen Suche nach Ovoiden beitragen und geben dann einen Suchalgorithmus an, der bis auf Äquivalenz alle G -invarianten Ovoiden findet.

5.1 Partition der singulären Punkte

Der unten beschriebene Algorithmus 5.3.1 sucht zu gegebener Gruppe $G \leq \Gamma\text{O}(V)$ alle Mengen von G -Bahnen, deren Vereinigung ein Ovoid ist. Das folgende Lemma liefert zu gegebenem singulären Punkt P eine Partition der Menge der singulären Punkte, so dass jedes Ovoid, welches P enthält, aus jeder Klasse genau ein Element enthält. Die Verwendung dieser Partition erleichtert die Suche nach den geeigneten Kombinationen von Bahnen.

Lemma 5.1.1 ([CD00]). *Sei $V = V^+(2n, q)$ und $(e_1, \dots, e_{2n})$ eine hyperbolische Basis (vgl. Def. 1.1.4) von V . Für $a = (a_2, \dots, a_n) \in \text{GF}(q)^{n-1}$ sei*

$$L_a := \left\{ \left\langle \sum_{i=1}^{2n} x_i e_i \right\rangle \in I(V) \mid x_1 = 1, x_i = a_i \text{ für } 2 \leq i \leq n \right\}.$$

Dann gilt

- (i) $I(V) \setminus I(\langle e_{n+1} \rangle^\perp) = \dot{\bigcup} L_a$.
- (ii) Ist $\mathcal{O}$ ein Ovoid von V mit $\langle e_{n+1} \rangle \in \mathcal{O}$, so gibt es zu jedem $a \in \text{GF}(q)^{n-1}$ genau ein $x \in L_a$ mit $\langle x \rangle \in \mathcal{O}$.

Beweis. (i) Sei $x = \sum_{i=1}^{2n} x_i e_i \in V$. Dann ist $x \notin \langle e_{n+1} \rangle^\perp$ genau dann, wenn $x_1 \neq 0$. Das heißt, $\langle x \rangle \in L_a$ für $a = \frac{1}{x_1}(x_2, \dots, x_n)$. Offensichtlich ist $L_a \cap L_b = \emptyset$ für $a \neq b$.

(ii) Sei $a \in \text{GF}(q)^{n-1}$ und $x \in L_a$. Falls $Q(x) = 0$ ist, so ist $0 = \sum_{i=1}^n x_i x_{n+i}$ und mit $x_1 = 1$ folgt

$$x_{n+1} = - \sum_{i=2}^n a_i x_{n+i}.$$

Ist y ein weiterer singulärer Punkt von L_a , dann gilt

$$(x, y) = \sum_{i=1}^n x_i y_{n+i} + y_i x_{n+i} = y_{n+1} + x_{n+1} + \sum_{i=2}^n a_i y_{n+i} + a_i x_{n+i} = 0.$$

Es gibt also höchstens ein $x \in L_a$ mit $\langle x \rangle \in \mathcal{O}$.

Sei nun $\langle e_{n+1} \rangle \neq \langle x \rangle \in \mathcal{O}$. Dann ist $x_1 = (x, e_{n+1}) \neq 0$. Sei o.B.d.A. $x_1 = 1$, dann ist $x \in L_{(x_2, \dots, x_n)}$.

Aus $|\mathcal{O} \setminus \{\langle e_{n+1} \rangle\}| = q^{n-1} = |\text{GF}(q)^{n-1}|$ und $L_a \cap L_b = \emptyset$ für $a \neq b$ folgt die Behauptung. □

5.2 Äquivalenz von Teilovoiden

Im Laufe des Suchalgorithmus werden die G -invarianten Ovoide schrittweise aus G -invarianten Teilovoiden konstruiert. Da wir die Ovoide nur bis auf Äquivalenz finden wollen, kann man Teilovoide vernachlässigen, von denen bekannt ist, dass alle Fortsetzungen äquivalent zu den Fortsetzungen schon berücksichtigter Anfangsstücke sind. Dies kann in manchen Fällen, beispielsweise falls der Algorithmus schon in den ersten Iterationsschritten sehr viele Teilovoide konstruiert hat, zu einer deutlichen Beschleunigung der Suche führen.

Die Methode basiert auf folgendem Äquivalenzbegriff für Teilovoide:

Definition 5.2.1. Sei V ein nicht ausgearteter quadratischer Raum und seien C_1, C_2 Teilovoide von V . Des Weiteren sei $H \leq \Gamma\text{O}(V)$. Die Teilovoide C_1 und C_2 heißen H -äquivalent genau dann, wenn es ein $\gamma \in H$ gibt mit $\gamma(C_1) = C_2$.

Damit sind äquivalente Ovoide im Sinne von Definition 1.2.2 auch $\Gamma\text{O}(V)$ -äquivalente Teilovoide nach Definition 5.2.1.

Sei V ein nicht ausgearteter quadratischer Raum, $H \leq \Gamma\text{O}(V)$ und $\gamma \in H$ mit $\gamma(C_1) = C_2$, das heißt, C_1, C_2 sind H -äquivalente Teilovoide von V . Ist dann $\mathcal{O}$ ein Ovoid mit $C_1 \subseteq \mathcal{O}$, so ist offensichtlich $\gamma(\mathcal{O})$ ein Ovoid, welches C_2 enthält. Mit anderen Worten: Zu jeder Fortsetzung von C_1 gibt es eine H -äquivalente Fortsetzung von C_2 .

Sei nun $G \leq \Gamma O(V)$ und $\mathcal{O}$ ein G -invariantes Ovoid von V . Ist dann $\gamma \in N_{\Gamma O(V)}(G)$, so gibt es für alle $g \in G$ ein $g' \in G$ mit $g\gamma = \gamma g'$ und es gilt

$$g(\gamma(\mathcal{O})) = \gamma(g'(\mathcal{O})) = \gamma(\mathcal{O}).$$

Also ist in diesem Fall auch $\gamma(\mathcal{O})$ ein G -invariantes Ovoid. Bei der Suche nach G -invarianten Ovoiden können wir also die $N_{\Gamma O(V)}(G)$ -Äquivalenz als Äquivalenzbegriff für Teilovoide verwenden.

Der Äquivalenztest für Teilovoide bzgl. H -Äquivalenz verläuft analog zum Äquivalenztest aus Algorithmus 4.4.2 von Seite 50. Es muss lediglich zusätzlich getestet werden, ob die konstruierten Semiähnlichkeiten in H enthalten sind.

5.3 Ein Algorithmus zur Ovoidsuche

In diesem Abschnitt formulieren wir nun den angekündigten Algorithmus zur Ovoidsuche. Zunächst geben wir die „Grobstruktur“ der Methode an. Danach konkretisieren wir das Kernstück des Algorithmus, die schrittweise Konstruktion von Ovoiden aus Teilovoiden, in Algorithmus 5.3.1. Den Abschluss des Kapitels bilden einige Bemerkungen zum Laufzeitverhalten des Algorithmus.

Es sei $V = V^+(2n, q)$ und $G \leq \Gamma O(V)$. Die Suche nach allen G -invarianten Ovoiden von V verläuft nach folgendem Schema:

- (i) Berechne die Bahnenzerlegung $I(V) = \bigcup x^G$
- (ii) Wähle einen maximalen total singulären Teilraum U von V und bestimme die Menge $S := \left\{ \langle x \rangle^G \mid x \in U, \langle x \rangle^G \text{ ist Teilovoid} \right\}$
- (iii) Bilde Äquivalenzklassen von S bezüglich $N_{\Gamma O(V)}(G)$ -Äquivalenz und wähle ein Repräsentantensystem $R := \{s_1, \dots, s_m\}$.
- (iv) Führe für jede „Startmenge“ $s \in R$ die folgenden Schritte durch:
 - iv(a) Wähle $\langle x \rangle \in s$ und eine hyperbolische Basis $(e_1, \dots, e_{2n})$ von V mit $e_{n+1} = x$. Bilde die Partition $I(V) \setminus I(x^\perp) = \bigcup_{a \in \text{GF}(q)^{n-1}} L_a$ wie in Satz 5.1.1.
 - iv(b) Ergänze s bahnenweise zu Ovoiden von V unter Berücksichtigung der Partition aus iv(a).

Dieser Schritt ist in Algorithmus 5.3.1 genauer dargestellt.
- (v) Führe Äquivalenztest mittels Algorithmus 4.4.2 durch.

Alternativen zur Wahl der Teilovoide in Schritt (ii)

In Schritt (ii) des Suchalgorithmus Seite 56 wird ein maximaler total singulärer Teilraum gewählt, um eine Menge S von „Startmengen“ so zu definieren, dass jedes G -invariante Ovoid von V eines der Teilovoide aus S enthält. Es sind auch andere Wahlen für S als die in Schritt (ii) angegebene denkbar. Hier werden einige

Möglichkeiten aufgelistet. Welche Methode nützlich oder auch nur anwendbar ist, hängt vom konkreten Fall ab. Es scheint hier keine Wahl zu geben, die in jedem Fall „gut“ oder „schlecht“ ist.

- (a) Sei $A := \{ |x^G| \mid x \in I(V), x^G \text{ Teilovoid} \}$. Gibt es eine Teilmenge $M \subseteq A$, so dass $\text{ggT}(A \setminus M) \nmid q^{n-1} + 1$, dann lässt sich aus den Bahnen, deren Länge in $A \setminus M$ ist, kein Ovoid zusammensetzen. Das heißt, für jedes Ovoid $\mathcal{O}$ von V gibt es ein $x \in \mathcal{O}$ mit $|x^G| \in M$. Wir können also

$$S := \{ x^G \mid x^G \text{ Teilovoid, } |x^G| \in M \}$$

wählen.

Beispiel. Es sei $K = \text{GF}(9) = \text{GF}(3)[z]/(z^2 - z - 1)$ und $V = V^+(8, 9)$. Außerdem sei $G = \langle f \rangle$ mit $f \in \text{O}(V)$ und $\text{ord}(f) = 7$. Da 7 kein Teiler von $9^3 + 1$ ist, enthält jedes Ovoid von V mindestens einen singulären Fixpunkt von V und wir könnten diese Fixpunkte als „Startmengen“ wählen. Wegen $\text{ord}(f) = 7$ ist nun

$$(X - 1)(X^3 + zX^2 + z^7X - 1)(X^3 + z^3X^2 + z^5X - 1)$$

das Minimalpolynom von f . Das heißt es gibt Teilräume V_1, V_2 von V , so dass $V = V_1 \perp V_2$ ist, wobei V_1 ein f -Modul vom Typ III und V_2 eine hyperbolische Ebene ist. V enthält also genau zwei singuläre Fixpunkte P_1, P_2 . Ist nun $\mathcal{O}$ ein Ovoid von V , dann ist $|\mathcal{O}| = 9^3 + 1 = 104 \cdot 7 + 2$. Falls $\mathcal{O}$ invariant unter f ist, so muss $\mathcal{O}$ die beiden Fixpunkte enthalten. Wir wählen also in diesem Fall $S = \{\{P_1, P_2\}\}$.

- (b) Sei V ein quadratischer Raum und $G = \langle f \rangle$ mit $f \in \Gamma\text{O}(V)$. Sei P wie in Satz 1.2.4 ein singulärer Punkt von V mit $f(P) = P$, $V_P := P^\perp/P$ und $f_P: V_P \rightarrow V_P$ definiert durch $\bar{v} \mapsto \overline{f(v)}$. Falls es keine Ovoide von V_P gibt, die invariant unter f_P sind, so ist P nach Satz 1.2.4 in jedem Ovoid von V , welches invariant unter f ist, enthalten. Definiere

$$S_1 := \{ P \in \mathcal{O} \mid f(P) = P, \text{ es gibt keine } f_P\text{-invarianten Ovoide von } V_P \}.$$

Falls $S_1 \neq \emptyset$ ist, so können wir $S := \{S_1\}$ wählen.

Beispiel. Sei $V = V^+(8, 7)$ und $f \in \text{O}(V)$, so dass V eine f -Zerlegung vom Typ $\text{II}_{(X-1)^3} \perp \text{II}_{(X-1)^3} \perp (\text{II}_{X-1})^2$ hat. Es ist also $V = V_1 \perp V_2 \perp V_3$ mit f -invarianten Teilräumen V_1, V_2, V_3 , so dass V_1, V_2 vom Typ $\text{II}_{(X-1)^3}$, $\dim V_3 = 2$ und $f|_{V_3} = \mathbb{1}$ ist. Außerdem habe V_3 den Wittindex 1 (das ist der Fall, wenn V_1 und V_2 verschiedenen Isometrie-Typ haben). Ist nun $P \in V_3$ mit $Q(P) = 0$ und sind V_P, f_P wie oben definiert, so gibt es keine f_P -invarianten Ovoide von V_P , vgl. Beispiel Seite 14. Bezeichnen nun P_1, P_2 die singulären Punkte von V_3 , so definieren wir $S := \{\{P_1, P_2\}\}$.

- (c) Sei $V = V^+(8, q)$ und $\mathcal{O}$ ein Ovoid von V , dann ist $\dim(\mathcal{O}) \geq 7$. Denn sonst wäre $\mathcal{O}$ Ovoid eines 6-dimensionalen Teilraums. Da Ovoids von $V^+(6, q)$ aber echt kleiner sind als solche von $V^+(8, q)$, vgl. Satz 1.2.3, kann dieser Teilraum nicht isomorph zu $V^+(6, q)$ sein. Nach [Tha81, Abschnitt 1] gibt es jedoch keine Ovoids von $V^-(6, q)$.

Es ist also möglich als „Startmengen“ alle solchen Bahnen zu betrachten, die nicht in einen gegebenen sechsdimensionalen Teilraum „passen“. Wähle also einen Teilraum W von V mit $\dim(W) = 6$ und setze

$$S := \left\{ \langle x \rangle^G \mid x \notin W, \langle x \rangle^G \text{ ist Teilovoid} \right\}.$$

Dies ist insbesondere dann interessant, wenn es einen großen f -invarianten Teilraum gibt, auf dem $\langle f \rangle$ nur kurze Bahnen hat. Im allgemeinen Fall ist jedoch nicht garantiert, dass dieses Vorgehen wirklich eine Erleichterung ist, da die so gewählte Menge S der „Startmengen“ sehr groß werden kann.

Algorithmus 5.3.1 Ovoidsuche

Eingabe: Sei $\emptyset \neq \mathcal{C}$ eine Menge nichtleerer G -invarianter Teilovoide von $V^+(2n, q)$. Dabei sei $\langle e_{n+1} \rangle \in C$ für alle $C \in \mathcal{C}$ und $I(V) \setminus I(\langle e_{n+1} \rangle^\perp) = \bigcup_{a \in \text{GF}(q)^{n-1}} L_a$ eine Partition von $I(V)$ wie in Satz 5.1.1. Außerdem sei $r \in \mathbb{Q}$.

Ausgabe: Bis auf Äquivalenz werden alle G -invarianten Ovoids bestimmt, die eines der Teilovoid aus $\mathcal{C}$ enthalten.

```

1: procedure OVOIDE( $\mathcal{C}, G, r$ )
2:   Setze  $O := \{C \in \mathcal{C} \mid |C| = q^{n-1} + 1\}$ .
3:   for  $C \in \mathcal{C} \setminus O$  do
4:     Wähle ein  $\alpha \in \text{GF}(q)^{n-1}$  mit  $L_\alpha \cap \mathcal{C} = \emptyset$ .
         # Ist  $\mathcal{O}$  Ovoid mit  $C \subseteq \mathcal{O}$ , dann existiert wegen 5.1.1 ein  $x \in L_\alpha$ ,
         # so dass  $C \cup x^G \subseteq \mathcal{O}$ .
5:     Sei  $E_C := \{C \cup x^G \mid x \in L_\alpha, C \cup x^G \text{ ist Teilovoid}\}$ .
6:     for  $\hat{C} \in E_C$  do
7:       Für  $a \in \text{GF}(q)^{n-1}$  sei  $L_a^{\hat{C}} := \{x \in L_a \mid \hat{C} \cup x^G \text{ ist Teilovoid}\}$ 
8:       if  $L_a^{\hat{C}} = \emptyset$  für ein  $a \in \text{GF}(q)^{n-1}$  then
9:         # Wegen 5.1.1 gibt es kein Ovoid das  $\hat{C}$  enthält.
10:        Entferne  $\hat{C}$  aus  $E_C$ .
11:      end if
12:    end for
13:  end for
14:  Setze  $E := \bigcup_{C \in \mathcal{C} \setminus O} E_C$ .
15:  if  $r \leq 0,9$  then
16:    Bilde Äquivalenzklassen von  $E$  bezüglich  $N_{\text{RO}(V)}(G)$ -Äquivalenz und
17:    bestimme ein Repräsentantensystem  $E'$  dieser Klassen.
18:    Setze  $r' := \frac{|E'|}{|E|}$ .
19:  else
20:    Setze  $E' := E$  und  $r' := r$ .
21:  end if
22:  Wähle eine Partition  $P$  von  $E'$ .
23:  for  $p \in P$  do
24:    Berechne rekursiv  $O_p := \text{OVOIDE}(p, G, r')$ .
25:    Füge die Ovoids aus  $O_p$  zur Menge  $O$  hinzu.
26:  end for
27:  return  $O$ 
28: end procedure

```

In Zeile 22 von Algorithmus 5.3.1 wird eine Partition P von E' gewählt. Dies hat rein technische Gründe. Je kleiner die Elemente von P gewählt werden desto weniger Speicher braucht der Algorithmus. In den nächsten Rekursionsschritten können dabei aber Teilovoiden, die aus verschiedenen Elementen der Partition hervorgegangen sind, natürlich nicht mehr auf Äquivalenz getestet werden, was von Nachteil ist, wenn es viele Äquivalenzen zwischen den Teilovoiden gibt. Hier wird dann möglicherweise doppelt gerechnet. Ist E' also klein, so wird man $P = \{E'\}$ wählen. Falls $r' > 0,9$ ist, also in den nächsten Iterationsschritten keine Äquivalenzttests zwischen Teilovoiden durchgeführt werden, so wählt man $P = \{\{C\} \mid C \in E'\}$. Ansonsten sind bei großem E' mögliche Kriterien für eine Partition außer dem Wert von r' die Größe der Teilovoiden in E' , die Größe von $N_{\text{RO}(V)}(G)$ und die Rekursionstiefe.

Variationen von Algorithmus 5.3.1

- In Schritt iv(a) des Suchalgorithmus (Seite 56) wird zu einem Punkt x der „Startmenge“ s eine Partition der singulären Punkte von V gewählt. Diese wird in Algorithmus 5.3.1, Zeilen 6 bis 12 verwendet um unter den bisher konstruierten Teilovoiden solche aus zu sortieren, die sich nicht zu vollen G -invarianten Ovoiden erweitern lassen. Die Partition hängt dabei von der Wahl von x und der Basiswahl ab. Wir können also in Schritt iv(a) Partitionen zu verschiedenen hyperbolischen Basen und gegebenenfalls zu verschiedenen Punkten von s wählen. Führt man dann die Schritte in Zeile 6 bis 12 von Algorithmus 5.3.1 für diese verschiedenen Partitionen durch, so lässt sich, falls ein gegebenes Teilovoid $\hat{C}$ nicht zu einem vollen G -invarianten Ovoid erweiterbar ist, dies gegebenenfalls früher feststellen.

In der praktischen Durchführung des Algorithmus wurden oft zwei bis drei solcher Partitionen verwendet.

- In Zeile 4 und 5 von Algorithmus 5.3.1 werden die Teilovoiden $C \in \mathcal{C}$ unter Berücksichtigung der Partition $I(V) \setminus I(\langle e_{n+1} \rangle^\perp) = \bigcup L_a$ erweitert. Hier kann es nützlich sein, statt der zuvor gewählten Partition eine andere zu berechnen.

Sei $C \in \mathcal{C}$ ein Teilovoid. Falls es einen Teilraum U von V gibt mit $C \subseteq U \simeq V^+(2n-2, q)$, können wir eine hyperbolische Basis $b' = (e'_1, \dots, e'_{2n})$ von V wählen, so dass $\langle C \rangle \subseteq \langle e'_1, \dots, e'_{n-1}, e'_{n+1}, \dots, e'_{2n-1} \rangle$ und $\langle e'_{n+1} \rangle \in C$ ist. Für $a = (a_2, \dots, a_n) \in \text{GF}(q)^{n-1}$ sei dann wie in Satz 5.1.1

$$L'_a := \left\{ \left\langle \sum_{i=1}^{2n} x_i e'_i \right\rangle \in I(V) \mid x_1 = 1, x_i = a_i \text{ für } 2 \leq i \leq n \right\}.$$

Wähle nun $\alpha = (a_2, \dots, a_n) \in \text{GF}(q)^{n-1}$ mit $a_n \neq 0$ und definiere

$$E_C := \{ C \cup x^G \mid x \in L'_\alpha, C \cup x^G \text{ ist Teilovoid} \}$$

Dann ist $\dim(\widehat{C}) > \dim(C)$ für alle $\widehat{C} \in E_C$.

Wir können also erreichen, dass bei der Erweiterung des Teilovoids die Dimension steigt. Dies ist nützlich, falls es in V viele G -invariante Teilovoide gibt, die in einem Teilraum vom Typ $V^+(2n-2, q)$ enthalten sind.

- In Zeile 16 werden die bisher gefundenen Teilovoide auf Äquivalenz getestet. Für die Entscheidung, ob solche Tests durchgeführt werden sollen, hat es sich als praktikabel erwiesen, sich danach zu richten wie viele Äquivalenzen im letzten Rekursionsschritt an dieser Stelle gefunden wurden. Für die zu dieser Arbeit durchgeführten Rechnungen erscheint die Schranke 0,9 zweckmäßig. Es ist jedoch möglich, dass andere Schranken bessere Ergebnisse liefern. Außerdem ist es gegebenenfalls nützlich, die Teilovoide nach ihrer Größe oder Dimension zunächst in Klassen einzuteilen, um dann klassenweise zu entscheiden, ob ein Äquivalenztest durchgeführt werden soll.

Das Laufzeitverhalten des Suchalgorithmus

Um einen Eindruck von der Leistungsfähigkeit des oben beschriebenen Suchalgorithmus zu bekommen, sind in Tabelle 5.1 die Laufzeiten einiger Beispiele zur Ovoidsuche mit Algorithmus 5.3.1 zusammengestellt.

Wir betrachten den quadratischen Raum $V = V^+(8, q)$ und eine zyklische Gruppe $G \leq \text{PO}(V)$. Weiter sei C_0 ein G -invariantes Teilovoid von V und $\mathcal{C} = \{C_0\}$. Außerdem sei $r := 0$. Dies ist hier die Ausgangssituation für Algorithmus 5.3.1.

In Zeile 22 von Algorithmus 5.3.1 muss eine Partition P der Menge der bis dahin gefundenen Teilovoide E' gewählt werden. Für die Beispiele dieses Abschnitts wurde P folgendermaßen gewählt:

$$\begin{aligned} P &:= \{P_0\} \cup \{\{C\} \mid C \notin P_0\} \quad \text{mit} \\ P_0 &:= \{C \in E' \mid C, \dim(\langle C \rangle) < 7 \text{ oder } |C| \leq 15\} \end{aligned}$$

Für Teilovoide, die im Verlauf des Algorithmus aus den Teilovoiden aus P_0 entstanden sind, wurden keine Äquivalenztests mehr durchgeführt.

In Tabelle 5.1 sind nun die folgende Werte aufgelistet.

- die Größe q des Körpers über welchem die Suche durchgeführt wurde.
- die Ordnung der zyklischen Gruppe G ,
- der Typ einer f -Zerlegung von V , wobei $G = \langle \bar{f} \rangle$, mit $f \in \text{O}(V)$. Falls $q = 8$ ist, bezeichnet z ein Element von $\text{GF}(8)$ mit $z^3 + z + 1 = 0$, d.h. einen Erzeuger von $\text{GF}(8)^*$. Die Exponenten $+$ bzw $-$ geben an ob der zugehörige f -Modul maximalen bzw. nicht maximalen Wittindex hat.
- die Größe des Teilovoids C_0 ,
- die Dimension d_{C_0} von $\langle C_0 \rangle$,

- die Längen der G -Bahnen C' , für die $C_0 \cup C'$ ein Teilovoid ist (Die Exponenten geben die Häufigkeiten an mit der die einzelnen Bahnlängen auftreten.)
- die Anzahl $\#\hat{C}$ der Teilovoide $\hat{C}$, die in Zeile 10 von Algorithmus 5.3.1 aus der Menge der bisher gefunden Teilovoide entfernt wurden,
- die durchschnittliche Größe $\varnothing_{|\hat{C}|}$ der Teilovoide $\hat{C}$, die in Zeile 10 von Algorithmus 5.3.1 aus der Menge der bisher gefunden Teilovoide entfernt wurden,
- die Anzahl $\#\mathcal{O}$ der insgesamt gefundenen Ovoide,
- die Laufzeit des in GAP implementierten Algorithmus auf einem AMD Opteron 242 Prozessor.

q	$ G $	Typ	$ C_0 $	d_{C_0}	Bahnlängen	$\#\hat{C}$	$\emptyset_{ \hat{C} }$	$\#\mathfrak{o}$	Zeit
7	7	$\Pi_{(X-1)^5} \perp (\Pi_{X-1})^3$	7	5	$\{1^{(49)}, 7^{(4011)}\}$	1221	28	0	0:06:55
7	7	$\Pi_{(X-1)^5} \perp (\Pi_{X-1})^3$	8	3	$\{7^{(4410)}\}$	281	29	0	0:04:03
7	7	$\Pi_{(X-1)^7} \perp \Pi_{X-1}$	1	1	$\{7^{(10633)}\}$	12551	29	41	1:20:47
7	7	$\Pi_{(X-1)^7} \perp \Pi_{X-1}$	7	7	$\{1^{(1)}, 7^{(4055)}\}$	674	27	9	0:01:04
7	7	$(\Pi_{(X-1)^3} \perp \Pi_{(X-1)^3})^+ \perp (\Pi_{x-1})^2$	7	3	$\{1^{(91)}, 7^{(5292)}\}$	895	32	0	80:32:32
7	7	$(\Pi_{(X-1)^3} \perp \Pi_{(X-1)^3})^+ \perp (\Pi_{x-1})^2$	2	2	$\{7^{(10584)}\}$	216	9	0	0:01:55
7	6	$(\text{III}_{(X-3)(X-5)})^2 \perp \left((\Pi_{X-1})^2\right)^- \perp \left((\Pi_{X+1})^2\right)^-$	6	4	$\{1^{(14)}, 2^{(24)}, 3^{(564)}, 6^{(5757)}\}$	142539	29	18	2:51:18
7	6	$(\text{III}_{(X-3)(X-5)})^2 \perp \left((\Pi_{X-1})^2\right)^+ \perp \left((\Pi_{X+1})^2\right)^+$	6	4	$\{1^{(18)}, 2^{(15)}, 3^{(426)}, 6^{(5048)}\}$	47185	28	0	1:32:55
7	6	$\text{III}_{(X-3)(X-5)} \perp \left((\Pi_{X-1})^2\right)^+ \perp \left((\Pi_{X+1})^4\right)^+$	6	4	$\{1^{(60)}, 2^{(749)}, 3^{(8)}, 6^{(5110)}\}$	809914	31	737	16:44:00
7	6	$\text{III}_{(X-3)(X-5)} \perp \left((\Pi_{X-1})^2\right)^+ \perp \left((\Pi_{X+1})^4\right)^+$	6	3	$\{1^{(58)}, 2^{(861)}, 3^{(6)}, 6^{(6069)}\}$	313327	32	187	9:47:16
8	7	$\text{III}_{(X-z)(X-z^6)} \perp \text{III}_{(X-z^2)(X-z^5)} \perp (\text{I}_{(X-1)})^2$	7	5	$\{1^{(68)}, 7^{(10912)}\}$	27609	30	0	3:50:58
8	9	$(\Pi_{X^2+z^4X+1})^3 \perp \Pi_{X^2+X+1}$	9	4	$\{9^{(9408)}\}$	955	36	42	0:19:11
8	9	$\Pi_{(x^2+z^4x+1)} \perp \Pi_{(x^2+z^4x+1)} \perp (\text{I}_{(x-1)})^2$	9	3	$\{1^{(72)}, 9^{(10592)}\}$	17128	45	28	2:17:26

Tabelle 5.1: Rechenbeispiele zu Algorithmus 5.3.1

Kapitel 6

Ergebnisse der Ovoidsuche

Für $q \in \{7, 8, 9\}$ wurde per Computer eine systematische Suche nach Ovoiden in $V = V^+(8, q)$ durchgeführt. Dazu wurde Algorithmus 5.3.1 verwendet, der zu vorgegebener Gruppe G die G -invarianten Ovoids berechnet. Als G wurden vorwiegend zyklische Untergruppen von $\text{PO}(V)$ verwendet. Die Ergebnisse der Ovoidsuche zu zyklischen Gruppen finden sich in tabellarischer Form in Anhang A.

Bei der Ovoidsuche wurden keine neuen Ovoids gefunden. Aus der Suche ergeben sich jedoch Restriktionen an die Stabilisatoren neuer Ovoids. Diese sind in den folgenden Abschnitten zusammengefasst.

Seien $G, G' \leq \text{PFO}(V)$ zueinander konjugiert, es gebe also ein $\gamma \in \text{PFO}(V)$, so dass $\gamma^{-1}G\gamma = G'$ ist. Weiter sei $\mathcal{O}$ ein G -invariantes Ovoid. Dann gibt es für alle $g' \in G'$ ein $g \in G$ mit $g' = \gamma^{-1}g\gamma$ und es gilt

$$g'(\gamma^{-1}(\mathcal{O})) = \gamma^{-1}(g(\mathcal{O})) = \gamma^{-1}(\mathcal{O}).$$

Also ist $\gamma^{-1}(\mathcal{O})$ ein zu $\mathcal{O}$ äquivalentes, G' -invariantes Ovoid. Daher ist bei der Ovoidsuche aus jeder Konjugiertenklasse von $\text{PFO}(V)$ nur ein Repräsentant zu betrachten.

Um bis auf Konjugation die zyklischen Gruppen $G \leq \text{PO}(V)$ einer vorgegebenen Ordnung $d \in \mathbb{N}$ zu finden, wurden die Ergebnisse aus Kapitel 3 verwendet: Zunächst wurden dabei mit Algorithmus 3.3.3 die möglichen G -Typen orthogonaler Zerlegungen von V bestimmt. Dann wurden mit Hilfe der Ergebnisse aus Abschnitt 3.2 bis auf Konjugation die zyklischen Gruppen bestimmt, die eine Zerlegung von einem der berechneten Typen zulassen (beachte dazu auch das Beispiel von Seite 39).

6.1 Ovoids von $V^+(8, 7)$

Es sei hier $V := V^+(8, 7)$. In V sind bis auf Äquivalenz zwei Ovoids bekannt. Sie gehören zur binären und ternären Familie von Conway, Kleidman und Wilson (siehe Abschnitt 2.5).

In diesem Abschnitt sind zunächst in Lemma 6.1.1 die Ergebnisse der Suche nach Ovoiden von V , die invariant unter zyklischen Gruppen $G \leq \text{PO}(V)$ sind, angegeben. Anschließend wird untersucht, zu welchen Abbildungen $\bar{f} \in \text{PGO}(V) \setminus \text{PO}(V)$ es $\langle \bar{f} \rangle$ -invariante Ovoides gibt. Schließlich wurde in $V^+(8, 7)$ auch eine Ovoidsuche zu elementarabelschen Gruppen der Ordnung 9 durchgeführt. Die Resultate, die sich insgesamt aus diesen Betrachtungen ergeben, sind am Ende des Abschnitts in Satz 6.1.4 zusammengefasst.

Die Suche nach Ovoiden von $V^+(8, 7)$, die invariant unter zyklischen Gruppen $G \leq \text{PO}(V)$ fester Ordnung sind, liefert das folgende Lemma:

Lemma 6.1.1. *Sei $V = V^+(8, 7)$ und $g \in \text{PO}(V)$. Ist $\mathcal{O}$ ein g -invariantes Ovoid von V , welches keines der beiden bekannten Ovoides ist, also nicht aus der binären oder ternären Konstruktion stammt, dann gilt:*

- (i) $a \nmid \text{ord}(g)$ für $a \in \{43, 19, 9, 8, 7, 5\}$.
- (ii) Falls $\text{ord}(g) = 6$ ist, dann gibt es g -invariante Teilräume V_1, V_2 von V , so dass $V = V_1 \perp V_2$, $\dim(V_2) = 6$ und $\text{ord}(g|_{V_2}) \leq 2$ ist.

Beachte, dass 2, 3, 5, 7, 19 und 43 genau die Primteiler von $|\text{PO}(V^+(8, 7))|$ sind.

Ist V ein nicht ausgearteter quadratischer Raum und $f \in \text{GO}(V)$, so bezeichne hier $\bar{f} \in \text{PGO}(V)$ das Bild von f unter dem kanonischen Epimorphismus. Im Folgenden werden zyklische Gruppen $\langle \bar{f} \rangle$ mit $\bar{f} \in \text{PGO}(V) \setminus \text{PO}(V)$ betrachtet und untersucht, welche dieser Gruppen $\langle \bar{f} \rangle$ -invariante Ovoides zulassen.

Lemma 6.1.2. *Sei V ein nicht ausgearteter quadratischer Raum über einem endlichen Körper K . Ist $g \in \text{GO}(V)$ mit Multiplikator s_g , so dass $\bar{g} \in \text{PGO}(V) \setminus \text{PO}(V)$ ist. Dann gilt:*

- (i) s_g ist kein Quadrat in K und $\text{ord}(\bar{g})$ ist gerade.
- (ii) Ist $s \in K$ ein beliebiges Nichtquadrat, dann gibt es eine Ähnlichkeit $f \in \text{GO}(V)$ mit Multiplikator s , so dass $\bar{g} = \bar{f}$.

Beweis. (i) Sei $\alpha = \text{ord}(\bar{g})$ und $\lambda \in K$ mit $g^\alpha = \lambda \mathbb{1}$. Dann gilt für alle $x, y \in V$:

$$\lambda^2(x, y) = (\lambda x, \lambda y) = (g^\alpha(x), g^\alpha(y)) = s_g^\alpha(x, y).$$

Da V nicht ausgeartet ist, folgt $\lambda^2 = s_g^\alpha$. Ist $s_g = a^2$ für ein $a \in K$, so ist $g' := \frac{1}{a}g \in \text{O}(V)$ mit $\bar{g} = \overline{g'}$, das heißt $\bar{g} \in \text{PO}(V)$. Also ist s_g kein Quadrat in K und α gerade.

(ii) Da s_g kein Quadrat ist, gibt es ein $b \in K$ mit $b^2 s_g = s$. Dann ist $f := bg \in \text{GO}(V)$ mit Multiplikator s und $\bar{g} = \bar{f}$. $\square$

Sei nun $V = V^+(8, 7)$ und $f \in \text{GO}(V)$, so dass $\bar{f} \in \text{PGO}(V) \setminus \text{PO}(V)$ ist. Falls es ein $\langle f \rangle$ -invariantes Ovoid von V gibt, welches nicht eines der beiden bekannten

ist, so folgt, wegen $\bar{f}^2 \in \text{PO}(V)$, aus Lemma 6.1.1, dass $\text{ord}(\bar{f}) = 2^\ell \cdot 3^m$ ist mit $\ell \leq 3$ und $m \leq 1$. Das heißt, $\text{ord}(\bar{f}) \in \{2, 4, 8, 6, 12, 24\}$.

In den Fällen $\text{ord}(\bar{f}) \in \{2, 4\}$ konnte keine vollständige Suche nach $\langle \bar{f} \rangle$ -invarianten Ovoiden durchgeführt werden. In den anderen Fällen, das heißt für $\text{ord}(\bar{f}) \in \{8, 6, 12, 24\}$, gibt es keine $\langle \bar{f} \rangle$ -invarianten Ovoiden.

Die hierzu untersuchten Fälle sind in Tabelle 6.1 angegeben. Dabei steht jeweils in der ersten Spalte die Ordnung von $\bar{f}$ und in der zweiten Spalte der Multiplikator des für die Rechnungen gewählten Repräsentanten $f \in \text{GO}(V)$ von $\bar{f}$. Wegen Lemma 6.1.2 müssen nur Abbildungen $f \in \text{GO}(V)$ mit Multiplikator $s_f = -1$ betrachtet werden. Die dritte Spalte enthält den Typ einer Zerlegung von V in orthogonal unzerlegbare f -Moduln. In der letzten Spalte ist gegebenenfalls verzeichnet, ob bei der Suche Ovoiden aufgetreten sind, falls hier „?“ eingetragen ist, konnte die Suchen nicht vollständig durchgeführt werden.

Zu jeder auftretenden Ordnung $|\bar{f}|$ sind lediglich jene Fälle aufgelistet, die zu zyklischen Gruppen $\langle \bar{f} \rangle \leq \text{PGO}(V)$ gehören, bei denen die Suche nach Ovoiden, die invariant unter der Gruppe $\langle \bar{f}^2 \rangle \leq \text{PO}(V)$ sind, nicht (vollständig) durchgeführt wurde.

Im Fall $\text{ord}(\bar{f}) = 6$ wurden nur solche Abbildungen f betrachtet, für die $f^6 = -1$ ist, denn andernfalls hat V eine f^3 -Zerlegung vom Typ $(\text{III}_{(X-1)(X+1)})^4$ und in diesem Fall gibt es keine f^3 -invarianten Ovoiden. Falls $\text{ord}(\bar{f}) = 24$ ist, so ist $\bar{f}^3 \in \text{PGO}(V) \setminus \text{PO}(V)$ mit $\text{ord}(\bar{f}^3) = 8$, sodass auch hier keine $\langle \bar{f} \rangle$ -invarianten Ovoiden auftreten.

$ \bar{f} $	s_f	Typ eine Zerlegung in orthogonal unzerlegbare f -Moduln	Ovoiden
2	-1	$(\text{III}_{(X-1)(X+1)})^4$	—
2	-1	$(\text{II}_{X^2+1})^4$	?
6	-1	$\text{II}_{(X^2+2)(X^2+4)} \perp (\text{II}_{X^2+1})^2$	—
6	-1	$(\text{II}_{(X^2+2)(X^2+4)})^2$	—
8	-1	$(\text{III}_{(X^2+3X+1)(X^2+4X+1)})^2$	—
8	-1	$\text{III}_{(X^2+3X+1)(X^2+4X+1)} \perp (\text{II}_{X^2+1}^+)^2$	—
8	-1	$\text{III}_{(X^2+3X+1)(X^2+4X+1)} \perp \text{II}_{X^2+1} \perp \text{III}_{(X-1)(X+1)}$	—
8	-1	$\text{III}_{(X^2+3X+1)(X^2+4X+1)} \perp (\text{III}_{(X-1)(X+1)})^2$	—
8	-1	$\text{II}_{x^2+a_1x-1} \perp \text{II}_{x^2+a_2x-1} \perp \text{II}_{x^2+a_3x-1} \perp \text{II}_{x^2+a_4x-1},$ $a_i \in \{\pm 1, \pm 4\}$	—
12	-1	$\text{III}_{(X-4)(X-5)} \perp \text{II}_{X^2+1} \perp \text{II}_{X^2+1} \perp \text{II}_{X^2+1}$	—
12	-1	$\text{III}_{(X-4)(X-5)} \perp \text{II}_{X^2+1} \perp \text{II}_{X^2+1} \perp \text{III}_{(X-1)(X+1)}$	—

$ \bar{f} $	s_f	Zerlegung in orthogonal unzerlegbare f -Moduln	Ovoide
12	-1	$\text{III}_{(X-4)(X-5)} \perp \text{II}_{X^2+1} \perp \text{III}_{(X-1)(X+1)} \perp \text{III}_{(X-1)(X+1)}$	—

Tabelle 6.1: Ovoidsuche zu Ähnlichkeiten von $V \simeq V^+(8, 7)$

Außer der Suche zu zyklischen Gruppen wurde in $V^+(8, 7)$ auch eine Suche nach den Ovoiden durchgeführt, die invariant unter elementarabelschen Gruppen der Ordnung 9 sind. Auch hier sind außer den bekannten keine weiteren Ovoiden aufgetreten:

Lemma 6.1.3. *Sei $V = V^+(8, 7)$ und $G \leq \text{PGO}(V)$ elementarabelsch der Ordnung 9. Ist $\mathcal{O}$ ein G -invariantes Ovoid von V , dann ist $\mathcal{O}$ eines der beiden bekannten Ovoiden von $V^+(8, 7)$.*

Ein neues Ovoid $\mathcal{O}$ besitzt nun nach Lemma 6.1.1 keinen Automorphismus der Ordnung 9 und ist nach Lemma 6.1.3 unter keiner elementarabelschen Gruppe der Ordnung 9 invariant. Da p -Gruppen ein nichttriviales Zentrum besitzen, ist also die 3-Sylow Untergruppe des Stabilisators von $\mathcal{O}$ eine Untergruppe von Z_3 . Mit $|\text{PO}(V^+(8, 7))| = 2^{18} \cdot 3^5 \cdot 5^4 \cdot 7^{12} \cdot 19 \cdot 43$, erhält man somit aus 6.1.1 und 6.1.3 den folgenden Satz.

Satz 6.1.4. *Sei $V = V^+(8, 7)$ und $\mathcal{O}$ ein Ovoid von V , welches nicht aus der binären bzw. ternären Konstruktion stammt. Dann gilt:*

- (i) $|\text{Stab}_{\text{PGO}(V)}(\mathcal{O})| = 2^\ell \cdot 3^m$ für ein $\ell \geq 0$ und $m \in \{0, 1\}$.
- (ii) Ist $\bar{f} \in |\text{Stab}_{\text{PGO}(V)}(\mathcal{O})|$ mit $\text{ord}(\bar{f}) = 2^k$, so ist $k \leq 2$.

6.2 Ovoide von $V^+(8, 8)$

Die bekannten Ovoiden von $V := V^+(8, 8)$ sind das unitäre Ovoid, das desarguesche Ovoid und das Ovoid von Dye, siehe Kapitel 2.

Aus der Suche nach G -invarianten Ovoiden in V zu zyklischen Gruppen $G \leq \text{PO}(V)$ ergibt sich das folgende Lemma:

Lemma 6.2.1. *Sei $V = V^+(8, 8)$ und $g \in \text{PO}(V)$. Ist $\mathcal{O} = g(\mathcal{O})$ ein Ovoid von V , das nicht das desarguessche oder unitäre Ovoid und nicht das Dye-Ovoid ist, dann gilt:*

- (i) $a \nmid \text{ord}(g)$ für $a \in \{73, 19, 13, 8\}$.
- (ii) Falls $\text{ord}(g) \in \{9, 7\}$, dann gibt es g -invariante Teilräume V_1, V_2 von V , so dass $V = V_1 \perp V_2$, $\dim(V_2) = 6$ und $g|_{V_2} = \mathbb{1}$ ist.

Weitere Betrachtungen ergeben, dass es keine zyklischen Gruppen der Ordnung 49 in $\text{PO}(V)$ gibt. Ist außerdem $G \leq \text{PO}(V)$ elementarabelsch der Ordnung 49, so enthält G ein Element g , welches nicht von der Form aus 6.2.1 (ii) ist.

Alle Ovoids, die G als Automorphismengruppe zulassen, sind also bekannt. In $\text{PO}(V)$ gibt es des Weiteren keine zyklischen Gruppen der Ordnung 27. Eine 5-Sylowgruppe von $\text{O}(V)$ hat die Ordnung 25 und es gibt keine Ovoids die invariant unter einer solchen Gruppe sind.

Da $|\text{PO}(V)| = |\text{O}(V)| = 2^{37} \cdot 3^9 \cdot 5^2 \cdot 7^4 \cdot 13^2 \cdot 19 \cdot 73$ ist, ergibt sich schließlich mit Lemma 6.2.1 der folgende Satz.

Satz 6.2.2. *Sei $V = V^+(8, 8)$ und $\mathcal{O}$ ein Ovoid von V , das nicht das unitäre, desarguessche oder das Ovoid von Dye ist. Dann gilt:*

- (i) $|\text{Stab}_{\text{PO}(V)}(\mathcal{O})| = 2^\ell \cdot 3^m \cdot 5^k \cdot 7^r$ mit geeigneten $\ell, m \geq 0$ und $k, r \in \{0, 1\}$.
 - (ii) Hat $\bar{f} \in \text{Stab}_{\text{PO}(V)}(\mathcal{O})$ die Ordnung 2^j , so ist $j \leq 2$.
 - (iii) Ist $\bar{f} \in \text{Stab}_{\text{PO}(V)}(\mathcal{O})$ der Ordnung 3^j , so ist $j \leq 2$.
- Genauer: $j = 1$ oder $V = V_1 \perp V_2$ mit $\bar{f}$ -invarianten Teilräumen V_i von V , so dass $\dim(V_2) = 6$ und $\bar{f}|_{V_2} = 1$.

6.3 Ovoids von $V^+(8, 9)$

Für $V = V^+(8, 9)$ ist bis auf Äquivalenz nur ein Ovoid von V bekannt, das unitäre Ovoid. Es ist $|\text{PO}(V)| = 2^{18} \cdot 3^{24} \cdot 5^4 \cdot 7 \cdot 13 \cdot 41^2 \cdot 73$. Da dieser Wert sehr groß ist, gestaltet sich die Ovoidsuche hier schwierig.

Die Ergebnisse einer Suche nach Ovoiden von V zu zyklischen Gruppen G sind in Anhang Seite 79 aufgelistet. Insgesamt ergibt sich:

Satz 6.3.1. *Sei $V = V^+(8, 9)$ und $\mathcal{O}$ ein Ovoid von V , das nicht das unitäre Ovoid ist. Weiter sei $g \in \text{PO}(V)$ mit $g(\mathcal{O}) = \mathcal{O}$, dann gilt $a \nmid \text{ord}(g)$ für alle $a \in \{2^4, 3^2, 5^2, 13, 41, 73\}$.*

Beachte dazu, dass eine 5-Sylow Untergruppe von $\text{PO}(V)$ elementarabelsch ist, es also keine zyklischen Untergruppen von $\text{PO}(V)$ der Ordnung 25 gibt.

Um Abschätzungen über die Größe der 5-Sylow Untergruppen der Automorphismengruppe neuer Ovoids $\mathcal{O}$ zu erhalten, wäre es interessant, alle Ovoids zu bestimmen, die invariant unter einer elementarabelschen Gruppe $G \leq \text{PO}(V)$ der Ordnung 25 sind. Leider konnte diese Suche, wegen des hohen rechnerischen Aufwandes, nicht durchgeführt werden.

Aus dem selben Grund wäre natürlich eine vollständige Suche nach Ovoiden in V wünschenswert, die invariant unter einer zyklischen Gruppe der Ordnung 7 sind. Die Suche mit zyklische Gruppen der Ordnungen 7 und 8 ist jedoch sehr aufwändig und konnte nicht vollständig durchgeführt werden. Auch eine randomisierte unvollständige Suche erbrachte hier keine neuen Ovoids.

Kapitel 7

Anwendung der Algorithmen in $V^+(6, 8)$

Die in den Kapiteln 4 und 5 zur Suche 8-dimensionaler Ovoide entwickelten Methoden lassen sich natürlich auch auf Räume anderer Dimension anwenden. In diesem Kapitel werden nun einige Beispiele solcher Anwendungen für Ovoide in $V^+(6, 8)$ gegeben.

7.1 Die Projektionen des Dye-Ovoids

Durch Projektion wie in Satz 1.2.4 ergeben sich aus dem Ovoid von Dye bis auf Äquivalenz 13 Ovoide von $V^+(6, 8)$, vgl. auch [Wil99, 4.2.1]. Wir erweitern hier das Ergebnis von B.Williams und berechnen die Stabilisatoren dieser Ovoide.

Sei $V = V^+(8, 8)$. Wie in Abschnitt 2.4 sei $\{e_1, \dots, e_9\}$ ein Ovoid von $V^+(8, 2)$ und $a \in \text{GF}(8)$ mit $a^3 + a^2 + 1 = 0$. Es sei $\mathcal{O}$ das Ovoid von Dye, bestehend aus den Punkten $\langle e_1 \rangle_V, \dots, \langle e_9 \rangle_V$ und den Punkten $\langle ae_i + a^2e_j + a^4e_k \rangle_V$ mit paarweise verschiedenen i, j, k .

Tabelle 7.1 enthält die 13 Projektionen von $\mathcal{O}$. Dabei steht in der ersten Spalte der singuläre Punkt $P \notin \mathcal{O}$, zu welchem die Projektion wie in Satz 1.2.4 durchgeführt wurde. Die zweite Spalte enthält den Stabilisator der Projektion in $\text{PFO}(\langle \bar{\mathcal{O}} \rangle)$. In der dritten Spalte ist gegebenenfalls eine Referenz, in der das entsprechende sechsdimensionale Ovoid zu finden ist, angegeben.

Der Stabilisator wurde mit Hilfe des auf Seite 52 beschriebenen Algorithmus berechnet. Die Notation der Gruppen orientiert sich an der Notation in GAP.

7.2 Semifields und Ovoide

Wie in Abschnitt 1.3 beschrieben, entsprechen Ovoide von $V^+(6, q)$ eindeutig Spreads von $\text{GF}(q)^4$ und somit Translationsebenen der Ordnung q^2 mit Kern

	Projektionspunkt	$\text{Stab}_{\text{PRO}(\langle \bar{0} \rangle)}(\bar{0})$	Bemerkungen
1	$e_2 + e_3 + e_4 + e_5 + a^2e_8$	$S_4 \times (((C_2)^4 : C_3) : C_2)$	[HJ90, Tb.1 VI]
2	$e_2 + e_3 + a^4e_4 + a^4e_5 + a^6e_7 + a^2e_8 + a^6e_9$	$C_2 \times C_2 \times A_4$	
3	$e_1 + a^5e_2 + a^5e_3 + a^1e_4 + a^1e_5 + e_6$	$C_2 \times S_3 \times A_4$	[Kan82a, 8.4]
4	$a^2e_1 + a^5e_4 + a^6e_6 + a^6e_7 + a^4e_8 + a^4e_9$	$C_2 \times C_2 \times S_3$	
5	$a^5e_1 + a^2e_2 + a^3e_3 + a^6e_4 + a^4e_5 + ae_6 + e_7$	$C_2 \times (C_7 : C_3)$	
6	$e_1 + a^6e_5 + a^3e_6 + a^5e_7 + e_8 + e_9$	$C_3 \times S_3 \times S_3$	
7	$a^5e_1 + a^6e_2 + a^4e_3 + a^2e_4 + a^6e_5 + e_8$	D_{12}	
8	$a^3e_1 + ae_2 + a^4e_3 + e_4 + e_5 + a^3e_6 + a^6e_7$	$C_2 \times A_4$	
9	$e_1 + ae_2 + a^6e_3 + a^4e_4 + ae_5$	$C_6 \times S_4$	[Kan82a, 8.3]
10	$e_1 + a^7e_4 + a^5e_8 + a^2e_9$	$C_2 \times S_5$	[Kan82a, 8.2]
11	$e_1 + ae_3 + e_6 + e_7 + a^6e_8 + a^6e_9$	$C_2 \times S_3 \times S_3$	
12	$e_1 + a^3e_2 + a^5e_3 + a^2e_4 + a^3e_5$	$C_2 \times S_4$	
13	$e_2 + e_3 + e_4 + e_5$	$(PSL(2, 64) : C_3) : C_2$	[Kan82a, 8.1]

Tabelle 7.1: Die Projektionen des Ovoids von Dye

$\text{GF}(q)$. Ein Spezialfall der Translationsebenen sind solche Ebenen, die durch Semifields beschrieben werden.

Ist p eine Primzahl, dann sind für $e \geq 4$ sind Semifieldebenen der Ordnung p^e für die Ordnungen 16, 32 und 81 in [Knu65, 6.2], [Wal63a] und [Demb] klassifiziert. Cardinali, Polverino und Trombetti geben in [CPT06] eine Klassifikation der Semifield Ebene der Ordnung q^4 mit Kern $\text{GF}(q^2)$ und Zentrum $\text{GF}(q)$. Wir betrachten in diesem Abschnitt die Semifieldebenen der Ordnung 2^6 mit Kern $\text{GF}(2^3)$ also solche Ebenen, die Ovoiden von $V^+(6, 8)$ entsprechen.

Die im Folgenden angegebenen Überlegungen führen zu einem Algorithmus, mit welchem die Semifieldebenen der Ordnung 64 mit Kern $\text{GF}(8)$ bestimmt werden können.

Es sei p eine Primzahl $q = p^e$ für ein $e \in \mathbb{N}$. Jede Semifieldebene der Ordnung q^2 mit Kern $\text{GF}(q)$ wird durch eine sogenannte Spreadmenge $S \subseteq \text{GF}(q)^{2 \times 2}$ beschrieben. Dabei ist S ein $2e$ -dimensionaler $\text{GF}(p)$ -Vektorraum und es ist $S \setminus \{0\} \subseteq \text{GL}(2, q)$. Um alle Semifieldebenen zu bestimmen, berechnen wir alle Basen solcher Spreadmengen in $\text{GL}(2, 8)$.

Sei $S \subseteq \text{GF}(q)^{2 \times 2}$ eine Spreadmenge. Dann ist die Abbildung

$$\alpha: S \rightarrow \text{GF}(q)^2, \quad \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \mapsto (a_{11}, a_{12})$$

bijektiv. Ein Element A einer Spreadmenge ist also durch $(1, 0)A$ bestimmt.

Für jedes $A \in S$ ist $S' := \{sA^{-1} \mid s \in S\}$ eine zu S äquivalente Spreadmenge, das heißt S und S' definieren äquivalente Ebenen. Wir können also o.B.d.A. annehmen, dass $1 \in S$ ist.

Für unseren Fall sei nun $p = 2$ und $q = 8$. Die Spreadmengen haben dann die Dimension 6 über $\text{GF}(2)$. Wir schreiben $\text{GF}(8) = \text{GF}(2)[\zeta]$. Um die gesuchten Spreadmengen zu bestimmen, sucht man nun sukzessive die 5-Tupel $(s_1, \dots, s_5) \in \text{GL}(2, 8)^5$, für die

$$\begin{aligned} (1, 0)s_1 &= (\zeta, 0), & (1, 0)s_2 &= (\zeta^2, 0), & (1, 0)s_3 &= (0, 1), \\ (1, 0)s_4 &= (0, \zeta) & \text{und} & & (1, 0)s_5 &= (0, \zeta^2) \end{aligned}$$

gilt, und die zusammen mit 1 eine Basis einer Spreadmenge bilden.

Bis auf Äquivalenz ergeben sich 10 Semifieldebenen der Ordnung 64 mit Kern $\text{GF}(8)$. All diese Ebenen sind bereits bekannt. Acht dieser Ebenen sind in [HJ90] beschrieben. Die anderen beiden finden sich in [CW99, S. 128 ii, iv].

Mit Hilfe der Kleinkorrespondenz ergeben sich aus diesen Ebenen bis auf Äquivalenz acht Ovoide von $V^+(6, 8)$. Dabei ist zu beachten, dass transponierte Spreadmengen äquivalente Ovoide induzieren.

Der Algorithmus aus Abschnitt 4.5 wurde angewendet um die Stabilisatoren dieser Ovoide zu bestimmen. Die Ergebnisse der Rechnungen sind in Tabelle 7.2 verzeichnet. Dabei enthält die zweite Spalte einen Verweis auf die Konstruktion der betreffenden Ebene und die dritte Spalte eine Beschreibung des Stabilisators des Ovoids in $\text{P}\Gamma\text{O}$. In der vierten Spalte ist die Größe dieses Stabilisators angegeben.

	Ebene	$\text{Stab}_{\text{P}\Gamma\text{O}(\langle\mathcal{O}\rangle)}(\mathcal{O})$	$ \text{Stab}_{\text{P}\Gamma\text{O}(\langle\mathcal{O}\rangle)}(\mathcal{O}) $
1	[HJ90, Tbl. 1, I]	$(\text{PSL}(2, 64) : C_3) : C_2$	$2^8 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$
2	[HJ90, Tbl. 1, II]	$((((C_2)^4 : C_3) : C_2) \times D_8$	$2^8 \cdot 3$
3	[HJ90, Tbl. 1, III]	$((((C_2)^4 : C_3) : C_2) \times D_8$	$2^8 \cdot 3$
4	[HJ90, Tbl. 1, IV], [HJ90, Tbl. 1, V]	$(C_2)^6 : C_2$	2^7
5	[HJ90, Tbl. 1, VI]	$((((C_2)^4 : C_3) : C_2) \times S_4$	$2^8 \cdot 3^2$
6	[HJ90, Tbl. 1, VII]	$((((C_2)^4 : C_3) : C_2) \times D_8$	$2^8 \cdot 3$
7	[HJ90, Tbl. 1, VIII]	$((((C_2)^4) : C_2) \times S_4$	$2^8 \cdot 3$
8	[CW99, S. 128 ii], [CW99, S. 128 iv]	$((C_2)^6 : C_7) : C_9$	$2^6 \cdot 3^2 \cdot 7$

Tabelle 7.2: Die Semifield-Ovoide in $V^+(6, 8)$

Man beachte, dass Huang und Johnson [HJ90] in drei Fällen zu kleine Automorphismengruppen angeben: Aus der Kleinkorrespondenz erhält man einen Isomorphismus zwischen der Gruppe $\text{PTL}^*(V)$ der Kollineationen und Korrelationen auf $\mathcal{P}(V)$ und der Gruppe $\text{P}\Gamma\text{O}(\Lambda_2(V))$, siehe [Tay92, Thm. 12.18]. Da die Gruppe der Kollineationen auf $\mathcal{P}(V)$ den Index 2 in $\text{PTL}^*(V)$ hat, kann sich die Größe der Stabilisatoren der Ovoide von $V^+(6, 8)$ höchstens um den Faktor 2 von der Größe der Automorphismengruppen der zugehörigen Semifieldebenen unterscheiden. Das heißt im Fall [HJ90, Tbl. 1, VI] ist die Automorphismengruppe um den

Faktor 3^2 und in den Fällen [HJ90, Tbl. 1, VII VIII] um den Faktor 3 größer als Huang und Johnson angeben.

7.3 Weitere Ovoide von $V^+(6, 8)$

Die Ovoide von $V^+(6, q)$ sind für $q \leq 7$ klassifiziert. Wir betrachten hier $V = V^+(6, 8)$ und bestimmen bis auf Äquivalenz alle Ovoide $\mathcal{O}$ von V , die invariant unter einer Abbildung $f \in \text{PO}(V)$ mit $\text{ord}(f) \in \{5, 7, 8, 9, 13, 73\}$ sind. Beachte, dass 2, 3, 5, 7, 13 und 73 genau die Teiler von $|\text{PO}(V)|$ sind.

Die Ergebnisse dieser Rechnung finden sich in Tabelle 7.3. Die erste Spalte enthält die Ordnung von f , die zweite eine Beschreibung des Stabilisators des Ovoids. In der dritten Spalte wird gegebenenfalls angegeben, welcher Translationsebene das Ovoid via Kleinkorrespondenz entspricht.

Es fällt auf, dass einige der Ovoide ausgesprochen kleine Automorphismengruppen besitzen. Außerdem treten viele Ovoide auf, die nicht in den Tabellen 7.2 und 7.1 vorkommen. Dies gibt einen weiteren Hinweis darauf, dass es sehr viele Ovoide in $V^+(6, 8)$ gibt. Eine vollständige Klassifikation ist wahrscheinlich nur mit speziell auf diesen Fall zugeschnittenen Methoden möglich.

Es ist $\text{PO}(V^+(6, 8)) \simeq \text{PSL}(4, 8)$. B. Mwene beschreibt in [Mwe76] die Untergruppenstruktur von $\text{PSL}(4, 2^m)$. Daraus ergibt sich, dass die Ordnungen nicht auflösbarer Untergruppen von $\text{PO}(V^+(6, 8))$ durch 5 oder 7 teilbar sind. Mit den in Tabelle 7.3 eingetragenen Ergebnissen der Ovoidsuche in $V^+(6, 8)$ erhalten wir:

Folgerung 7.3.1. *Es sei $\mathcal{O}$ ein Ovoid von $V^+(6, 8)$ mit nicht auflösbarem Stabilisator $S_{\mathcal{O}}$, dann enthält $S_{\mathcal{O}}$ einen einfachen Normalteiler N , so dass $S_{\mathcal{O}}/N$ auflösbar ist. Dabei gilt eine der folgenden Aussagen:*

- (i) $N \simeq A_5$ und $\mathcal{O}$ entspricht entweder mittels Kleinkorrespondenz der Translationsebene der Ordnung 64 aus [Kan82c] oder ist die in [Kan82a, 8.2] beschriebene Projektion des Ovoids von Dye.
- (ii) $N \simeq \text{Sz}(8)$ und $\mathcal{O}$ entspricht der Lüneburg-Ebene der Ordnung 64.
- (iii) $N \simeq \text{PSL}(2, 64)$ und $\mathcal{O}$ entspricht der Desargueschen Ebene.
- (iv) $N \simeq \text{PSL}(2, 8)$ und $\mathcal{O}$ entspricht entweder einer der beiden Ott-Schäffer-Ebenen der Ordnung 64 oder der Hall-Ebene der Ordnung 64.

$ f $	$\text{Stab}_{\text{PRO}(\langle \mathcal{O} \rangle)}(\mathcal{O})$	Bemerkung
5	$S_5 \times S_3$	[Kan82c]
5	$S_5 \times C_2$	Proj. des Dye-Ovoids, Tbl. 7.1 Nr. 10
5	D_{20}	
5	C_5	
5	$C_3 \times D_{10}$	
5, 7, 13	$Sz(8) : C_3$	Lüneburg-Ebene [Lün80]
5, 7, 9, 13	$(PSL(2, 64) : C_3) : C_2$	desarguessche Ebene
7	$C_2 \times (((C_2)^3 : C_7) : C_3)$	
7	$(C_7 : C_3) : C_2$	
7	$(C_7 : C_3) \times C_2$	Proj. des Dye-Ovoids, Tbl. 7.1, Nr. 5.
7	D_{14}	
7	D_{14}	
7	$(C_{63} : C_3) : C_2$	
7, 9	$(PSL(2, 8) : C_3) \times C_2$	Ott-Schäffer-Ebene [FJ84]
7	$((C_7 : C_3) : C_2) \times C_2$	
7	$((C_2)^6 : C_7) : C_9$	Semifieldebene. [CW99, S. 128, ii, iv]
7, 9	$(PSL(2, 8) : C_3) \times C_2$	Ott-Schäffer-Ebene [FJ84]
7	$((C_4)^3 : C_7) : C_3 : C_2$	
7, 9	$((C_9 \times PSL(2, 8)) : C_3) : C_2 \times C_2$	Hall-Ebene [HP73, IX 2.]
9	D_{18}	
9	$((C_9)^2 : C_3) : C_2 : C_2$	verallgemeinerte André-Ebene
9	$C_2 \times (D_{18})^2$	verallgemeinerte André-Ebene
9	$C_2 \times S_3 \times D_{18}$	
9	$(C_2)^2 \times D_{18}$	
9	$C_2 \times D_{18} \times S_3$	
9	$D_{18} \times D_8$	
9	$S_4 \times D_{18}$	
9	$C_2 \times (D_{18})^2$	verallgemeinerte André-Ebene
9	$(C_2)^2 \times D_{18}$	
9	D_{18}	
9	$((C_9 : C_3) : C_2) \times C_2$	
9	$(C_{63} : C_3) : C_2$	
9	$(C_9 : C_3) : C_2$	
9	$C_9 : C_3$	
9	D_{18}	

Tabelle 7.3: Einige Ovoids von $V^+(6, 8)$

Anhang A

Ergebnistabellen

In $V = V^+(8, q)$ wurde für $q \in \{7, 8, 9\}$ mit Hilfe der Algorithmen aus den Kapiteln 4 und 5 zu verschiedenen Ordnungen d nach allen Ovoiden gesucht, die invariant unter einer zyklischen Gruppe $\langle \bar{f} \rangle \leq \text{PO}(V)$ der Ordnung d sind. Die Ergebnisse werden in Kapitel 6 zusammengefasst und sind in den folgenden Tabellen aufgeführt. Die ersten Spalte enthält dabei jeweils die Ordnung der Abbildung $\bar{f} \in \text{PO}(V)$, die zweite Spalte den Typ einer f -Zerlegung von V für einen Repräsentanten $f \in \text{O}(V)$ von $\bar{f}$ und die letzte Spalte die Isomorphieklasse der $\langle \bar{f} \rangle$ -invarianten Ovoide. Bei den Typen der Zerlegungen bedeutet ein $+$ oder $-$ als Exponent, dass der entsprechende Modul von maximalem resp. nichtmaximalem Wittindex ist. Über jeder Tabelle ist die Ordnung der zugehörigen projektiven orthogonalen Gruppe des jeweiligen Raumes angegeben. Tritt in einer Tabelle eine mögliche Ordnung nicht auf, so waren die Berechnung zu dieser Ordnung zu aufwändig, sodass sie nicht (vollständig) durchgeführt wurden. Tritt eine Ordnung jedoch auf, so sind bis auf Konjugation alle Gruppen dieser Ordnung aufgelistet. Gegebenenfalls besitzen sie jedoch den Eintrag “?” in der dritten Spalte. Dieser Fall musste dann ebenfalls offen bleiben.

A.1 $V = V^+(8, 7)$

$$|\text{PO}(V^+(8, 7))| = 2^{18} \cdot 3^5 \cdot 5^4 \cdot 7^{12} \cdot 19 \cdot 43$$

$ \bar{f} $	Zerlegung in orthogonal unzerlegbare f -Moduln	Ovoide
43	$\text{II}_{X^6-3X^5+X^4-X^3+X^2-3X+1}^- \perp (\text{II}_{(X-1)})^2$	—
19	$\text{III}_{(X^3+2X-1)(X^3-2X^2-1)} \perp (\text{II}_{(X-1)})^2$	—
9	$\text{III}_{(X^3-4)(X^3-2)} \perp \text{III}_{(X-4)(X-2)}$	—
9	$\text{III}_{(X^3-4)(X^3-2)} \perp \text{II}_{(X-1)} \perp \text{II}_{(X-1)}$	binär
8	$(\text{II}_{X^2+4X+1})^3 \perp \text{II}_{X^2+1}$	—

$ \bar{f} $	Zerlegung in orthogonal unzerlegbare f -Moduln	Ovoide
8	$(\Pi_{X^2+4X+1})^3 \perp (\Pi_{X-1})^2$	—
8	$(\Pi_{X^2+4X+1})^3 \perp \Pi_{X-1} \perp \Pi_{X+1}$	—
8	$(\Pi_{X^2+4X+1})^2 \perp \Pi_{X^2+3X+1} \perp \Pi_{X^2+1}$	—
8	$(\Pi_{X^2+4X+1})^2 \perp \Pi_{X^2+3X+1} \perp (\Pi_{X-1})^2$	—
8	$(\Pi_{X^2+4X+1})^2 \perp \Pi_{X^2+3X+1} \perp \Pi_{X-1} \perp \Pi_{X+1}$	—
8	$(\Pi_{X^2+4X+1})^2 \perp (\Pi_{X^2+1})^2$	—
8	$(\Pi_{X^2+4X+1})^2 \perp \Pi_{X^2+1} \perp (\Pi_{X-1})^2$	—
8	$(\Pi_{X^2+4X+1})^2 \perp \Pi_{X^2+1} \perp \Pi_{X-1} \perp \Pi_{X+1}$	—
8	$(\Pi_{X^2+4X+1})^2 \perp (\Pi_{X-1})^4$	—
8	$(\Pi_{X^2+4X+1})^2 \perp \left((\Pi_{X-1})^2\right)^- \perp \left((\Pi_{X+1})^2\right)^-$	—
8	$(\Pi_{X^2+4X+1})^2 \perp \left((\Pi_{X-1})^2\right)^+ \perp \left((\Pi_{X+1})^2\right)^+$	—
8	$(\Pi_{X^2+4X+1})^2 \perp (\Pi_{X-1})^3 \perp \Pi_{X+1}$	—
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+3X+1} \perp (\Pi_{X^2+1})^2$	—
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+3X+1} \perp \Pi_{X^2+1} \perp (\Pi_{X-1})^2$	binär, ternär
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+3X+1} \perp \Pi_{X^2+1} \perp \Pi_{X-1} \perp \Pi_{X+1}$	binär, ternär
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+3X+1} \perp (\Pi_{X-1})^4$	ternär
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+3X+1} \perp \left((\Pi_{X-1})^2\right)^- \perp \left((\Pi_{X+1})^2\right)^-$	ternär, binär
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+3X+1} \perp \left((\Pi_{X-1})^2\right)^+ \perp \left((\Pi_{X+1})^2\right)^+$	—
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+3X+1} \perp (\Pi_{X-1})^3 \perp \Pi_{X+1}$	ternär, binär
8	$\Pi_{X^2+4X+1} \perp (\Pi_{X^2+1})^3$	—
8	$\Pi_{X^2+4X+1} \perp (\Pi_{X^2+1})^2 \perp (\Pi_{X-1})^2$	—
8	$\Pi_{X^2+4X+1} \perp (\Pi_{X^2+1})^2 \perp \Pi_{X-1} \perp \Pi_{X+1}$	—
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+1} \perp (\Pi_{X-1})^4$	—
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+1} \perp \left((\Pi_{X-1})^2\right)^- \perp \left((\Pi_{X+1})^2\right)^-$	—
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+1} \perp \left((\Pi_{X-1})^2\right)^+ \perp \left((\Pi_{X+1})^2\right)^+$	—
8	$\Pi_{X^2+4X+1} \perp \Pi_{X^2+1} \perp (\Pi_{X-1})^3 \perp \Pi_{X+1}$	—
8	$\Pi_{X^2+4X+1} \perp \left((\Pi_{X-1})^4\right)^+ \perp \left((\Pi_{X+1})^2\right)^-$	—
8	$\Pi_{X^2+4X+1} \perp \left((\Pi_{X-1})^4\right)^- \perp \left((\Pi_{X+1})^2\right)^+$	—
8	$\Pi_{X^2+4X+1} \perp (\Pi_{X-1})^5 \perp \Pi_{X+1}$	—
8	$\Pi_{X^2+4X+1} \perp (\Pi_{X-1})^3 \perp (\Pi_{X+1})^3$	—
8	$\Pi_{X^2+4X+1} \perp (\Pi_{X-1})^6$	—

$ \bar{f} $	Zerlegung in orthogonal unzerlegbare f -Moduln	Ovoide
8	$(\text{III}_{(X^2+X-1)(X^2-X-1)})^2$	—
8	$\text{III}_{(X^2+X-1)(X^2-X-1)} \perp \text{III}_{(X^2+3X-1)(X^2+4X-1)}$	—
7	$\text{I}_{(X-1)^2} \perp \text{I}_{(X-1)^2}$	—
7	$\text{I}_{(X-1)^2} \perp (\text{II}_{X-1})^4$	—
7	$(\text{II}_{(X-1)^3})^2 \perp ((\text{II}_{X-1})^2)^-$	—
7	$(\text{II}_{(X-1)^3})^2 \perp ((\text{II}_{X-1})^2)^+$	—
7	$\text{I}_{(X-1)^4}$	—
7	$\text{I}_{(X-1)^2} \perp \text{II}_{(X-1)^3} \perp \text{II}_{X-1}$	—
7	$\text{II}_{(X-1)^7} \perp \text{II}_{X-1}$	binär, ternär
7	$\text{II}_{(X-1)^5} \perp \text{II}_{(X-1)^3}$	—
7	$\text{II}_{(X-1)^5} \perp (\text{II}_{X-1})^3$	—
7	$\text{II}_{(X-1)^3} \perp (\text{II}_{X-1})^5$	—
6	$(\text{III}_{(X-3)(X-5)})^3 \perp \text{III}_{(X-2)(X-4)}$	—
6	$(\text{III}_{(X-3)(X-5)})^2 \perp (\text{III}_{(X-2)(X-4)})^2$	—
6	$(\text{III}_{(X-3)(X-5)})^3 \perp \text{II}_{X+1} \perp \text{II}_{X-1}$	binär
6	$(\text{III}_{(X-3)(X-5)})^3 (\text{II}_{X-1})^2$	—
6	$(\text{III}_{(X-3)(X-5)})^2 \perp \text{III}_{(X-2)(X-4)} \perp (\text{II}_{X+1})^2$	—
6	$(\text{III}_{(X-3)(X-5)})^2 \perp \text{III}_{(X-2)(X-4)} \perp \text{II}_{X+1} \perp \text{II}_{X-1}$	binär
6	$(\text{III}_{(X-3)(X-5)})^2 \perp \text{III}_{(X-2)(X-4)} \perp (\text{II}_{X-1})^2$	binär
6	$(\text{III}_{(X-3)(X-5)})^2 \perp (\text{II}_{X+1})^3 \perp \text{II}_{X-1}$	binär, ternär
6	$(\text{III}_{(X-3)(X-5)})^2 \perp ((\text{II}_{X+1})^2)^- \perp ((\text{II}_{X-1})^2)^-$	binär, ternär
6	$(\text{III}_{(X-3)(X-5)})^2 \perp ((\text{II}_{X+1})^2)^+ \perp ((\text{II}_{X-1})^2)^+$	—
6	$(\text{III}_{(X-3)(X-5)})^2 \perp \text{II}_{X+1} \perp (\text{II}_{X-1})^3$	—
6	$(\text{III}_{(X-3)(X-5)})^2 \perp (\text{II}_{X-1})^4$	—
6	$\text{III}_{(X-3)(X-5)} \perp \text{III}_{(X-2)(X-4)} \perp (\text{II}_{X-1})^4$	—
6	$\text{III}_{(X-2)(X-4)} \perp \text{III}_{(X-3)(X-5)} \perp \text{II}_{X+1} \perp (\text{II}_{X-1})^3$	binär, ternär
6	$\text{III}_{(X-2)(X-4)} \perp \text{III}_{(X-3)(X-5)} \perp ((\text{II}_{X+1})^2)^+ \perp ((\text{II}_{X-1})^2)^+$	binär, ternär
6	$\text{III}_{(X-2)(X-4)} \perp \text{III}_{(X-3)(X-5)} \perp ((\text{II}_{X+1})^2)^- \perp ((\text{II}_{X-1})^2)^-$	—
6	$\text{III}_{(X-3)(X-5)} \perp (\text{II}_{X-1})^6$	?
6	$\text{III}_{(X-3)(X-5)} \perp \text{II}_{X+1} \perp (\text{II}_{X-1})^5$	?
6	$\text{III}_{(X-3)(X-5)} \perp ((\text{II}_{X+1})^2)^+ \perp ((\text{II}_{X-1})^4)^+$	ternär, binär
6	$\text{III}_{(X-3)(X-5)} \perp ((\text{II}_{X+1})^2)^- \perp ((\text{II}_{X-1})^4)^-$	—

$ \bar{f} $	Zerlegung in orthogonal unzerlegbare f -Moduln	Ovoide
6	$\text{III}_{(X-3)(X-5)} \perp (\text{II}_{X+1})^3 \perp (\text{II}_{X-1})^3$	?
6	$\text{III}_{(X-3)(X-5)} \perp ((\text{II}_{X+1})^4)^+ \perp ((\text{II}_{X-1})^2)^+$	—
6	$\text{III}_{(X-3)(X-5)} \perp ((\text{II}_{X+1})^4)^- \perp ((\text{II}_{X-1})^2)^-$	?
6	$\text{III}_{(X-3)(X-5)} \perp (\text{II}_{X+1})^5 \perp \text{II}_{X-1}$	?
6	$(\text{III}_{(X^2-5)(X^2-3)})^2$	—
6	$\text{III}_{(X^2-5)(X^2-3)} \perp (\text{II}_{X^2+1})^2$	—
5	$\text{II}_{X^4+X^3+X^2+X+1} \perp \text{II}_{X^4+X^3+X^2+X+1}$	—
5	$(\text{II}_{X-1})^4 \perp \text{II}_{X^4+X^3+X^2+X+1}$	binär, ternär

A.2 $V = V^+(8, 8)$

$$|\text{PO}(V^+(8, 8))| = 2^{37} \cdot 3^9 \cdot 5^2 \cdot 7^4 \cdot 13^2 \cdot 19 \cdot 73$$

In der folgenden Tabelle bezeichnet z ein Element von $\text{GF}(8)$ mit $z^3 + z + 1 = 0$, z ist also ein Erzeuger von $\text{GF}(8)^*$.

$ \bar{f} $	Zerlegung in orthogonal unzerlegbare f -Moduln	Ovoide
73	$\text{I}_{X+1} \perp \text{III}_{(X^3+zX+1)(X^3+zX^2+1)}$	desarguessch
19	$\text{I}_{X+1}^- \perp \text{II}_{X^6+z^3X^5+z^6X^4+z^6X^3+z^6X^2+z^3X+1}$	desarguessch, unitär
13	$\text{II}_{X^4+z^3X^3+z^5X^2+z^3X+1}^+ \perp \text{II}_{X^4+z^3X^3+z^5X^2+z^3X+1}^+$	—
13	$\text{II}_{X^4+z^3X^3+z^5X^2+z^3X+1}^+ \perp \text{II}_{X^4+z^5X^3+z^6X^2+z^5X+1}^+$	—
13	$\text{I}_{X+1}^+ \perp \text{I}_{X+1}^+ \perp \text{II}_{X^4+z^3X^3+z^5X^2+z^3X+1}^+$	—
9	$(\text{II}_{X^2+z^4X+1})^4$	—
9	$(\text{II}_{X^2+z^4X+1})^3 \perp \text{II}_{X^2+z^2X+1}$	—
9	$(\text{II}_{X^2+z^4X+1})^2 \perp (\text{II}_{X^2+z^2X+1})^2$	—
9	$(\text{II}_{X^2+z^4X+1})^2 \perp \text{II}_{X^2+z^2X+1} \perp \text{II}_{X^2+zX+1}$	—
9	$(\text{II}_{X^2+z^4X+1})^3 \perp \text{II}_{X^2+X+1}$	desarguessch
9	$(\text{II}_{X^2+z^4X+1})^2 \perp \text{II}_{X^2+z^2X+1} \perp \text{II}_{X^2+X+1}$	—
9	$(\text{II}_{X^2+z^4X+1})^2 \perp \text{II}_{X^2+zX+1} \perp \text{II}_{X^2+X+1}$	—
9	$(\text{II}_{X^2+z^4X+1})^2 \perp (\text{II}_{X^2+X+1})^2$	—
9	$\text{II}_{X^2+z^4X+1} \perp \text{II}_{X^2+z^2X+1} \perp \text{II}_{X^2+zX+1} \perp \text{II}_{X^2+X+1}$	desarguessch, Dye
9	$\text{II}_{X^2+z^4X+1} \perp \text{II}_{X^2+z^2X+1} \perp (\text{II}_{X^2+X+1})^2$	—
9	$\text{II}_{X^2+z^4X+1} \perp (\text{II}_{X^2+X+1})^3$	—
9	$(\text{II}_{X^2+z^4X+1})^3 \perp (\text{II}_{X-1})^2$	—

$ \bar{f} $	Zerlegung in orthogonal unzerlegbare f -Moduln	Ovoide
9	$(\Pi_{X^2+z^4X+1})^2 \perp \Pi_{X^2+z^2X+1} \perp (\Pi_{X-1})^2$	—
9	$(\Pi_{X^2+z^4X+1})^2 \perp \Pi_{X^2+zX+1} \perp (\Pi_{X-1})^2$	unitär
9	$(\Pi_{X^2+z^4X+1})^2 \perp \Pi_{X^2+X+1} \perp (\Pi_{X-1})^2$	—
9	$\Pi_{X^2+z^4X+1} \perp \Pi_{X^2+z^2X+1} \perp \Pi_{X^2+zX+1} \perp (\Pi_{X-1})^2$	—
9	$\Pi_{X^2+z^4X+1} \perp \Pi_{X^2+z^2X+1} \perp \Pi_{X^2+X+1} \perp (\Pi_{X-1})^2$	unitär
9	$\Pi_{X^2+z^4X+1} \perp \Pi_{X^2+zX+1} \perp \Pi_{X^2+X+1} \perp (\Pi_{X-1})^2$	unitär
9	$\Pi_{X^2+z^4X+1} \perp (\Pi_{X^2+X+1})^2 \perp (\Pi_{X-1})^2$	—
9	$(\Pi_{X^2+z^4X+1})^2 \perp (\Pi_{X-1})^4$	unitär
9	$\Pi_{X^2+z^4X+1} \perp \Pi_{X^2+z^2X+1} \perp (\Pi_{X-1})^4$	—
9	$\Pi_{X^2+z^4X+1} \perp \Pi_{X^2+X+1} \perp (\Pi_{X-1})^4$	—
9	$\Pi_{X^2+z^4X+1} \perp (\Pi_{X-1})^6$	?
8	$(\Pi_{X-1})^+ \perp (\Pi_{(X-1)^6})^+$	—
8	$(\Pi_{X-1})^- \perp (\Pi_{(X-1)^6})^-$	—
8	$\Pi_{(X-1)^8}$	Dye, unitär
8	$(\Pi_{(X-1)^2})^+ \perp (\Pi_{(X-1)^6})^+$	—
8	$(\Pi_{(X-1)^2})^- \perp (\Pi_{(X-1)^6})^-$	—
7	$(\text{III}_{(X-z)(X-z^6)})^4$	—
7	$(\text{III}_{(X-z)(X-z^6)})^3 \perp \text{III}_{(X-z^2)(X-z^5)}$	—
7	$(\text{III}_{(X-z)(X-z^6)})^3 \perp \text{III}_{(X-z^3)(X-z^4)}$	desarguessch
7	$(\text{III}_{(X-z)(X-z^6)})^3 \perp (\Pi_{X-1})^2$	—
7	$(\text{III}_{(X-z)(X-z^6)})^2 \perp (\text{III}_{(X-z^2)(X-z^5)})^2$	—
7	$(\text{III}_{(X-z)(X-z^6)})^2 \perp \text{III}_{(X-z^2)(X-z^5)} \perp \text{III}_{(X-z^3)(X-z^4)}$	—
7	$(\text{III}_{(X-z)(X-z^6)})^2 \perp \text{III}_{(X-z^2)(X-z^5)} \perp (\Pi_{X-1})^2$	unitär
7	$(\text{III}_{(X-z)(X-z^6)})^2 \perp \text{III}_{(X-z^3)(X-z^4)} \perp (\Pi_{X-1})^2$	—
7	$(\text{III}_{(X-z)(X-z^6)})^2 \perp (\Pi_{X-1})^4$	—
7	$\text{III}_{(X-z)(X-z^6)} \perp \text{III}_{(X-z^2)(X-z^5)} \perp \text{III}_{(X-z^3)(X-z^4)} \perp (\Pi_{X-1})^2$	Dye
7	$\text{III}_{(X-z)(X-z^6)} \perp \text{III}_{(X-z^2)(X-z^5)} \perp (\Pi_{X-1})^4$	—
7	$\text{III}_{(X-z)(X-z^6)} \perp (\Pi_{X-1})^6$	?
5	$\Pi_{X^4+X^3+X^2+X+1} \perp \Pi_{X^4+X^3+X^2+X+1}$	—
5	$\text{I}_{X+1} \perp \text{I}_{X+1} \perp \Pi_{X^4+X^3+X^2+X+1}$	?

A.3 $V \simeq V^+(8, 9)$

$$|\text{PO}(V)| = 2^{18} \cdot 3^{24} \cdot 5^4 \cdot 7 \cdot 13 \cdot 41^2 \cdot 73$$

In dieser Tabelle bezeichnet z ein Element von $\text{GF}(9)$ für das $z^2 - z - 1 = 0$ gilt, d.h. einen Erzeuger von $\text{GF}(9)^*$.

$ \overline{f} $	Zerlegung in orthogonal unzerlegbare f -Moduln	Ovoide
73	$\Pi_{X-1} \perp \Pi_{X-1} \perp \Pi_{X^6+X^5+z^5X^4+z^7X^3+z^5X^2+X+1}$	unitär
41	$\Pi_{X^4-X^3+zX^2-X+1} \perp \Pi_{X^4-X^3+zX^2-X+1}$	—
41	$\Pi_{X^4-X^3+zX^2-X+1} \perp \Pi_{X^4-X^3+z^3X^2-X+1}$	—
41	$\Pi_{X^4-X^3+zX^2-X+1} \perp \Pi_{X^4+zX^3+z^5X^2+zX+1}$	—
41	$\Pi_{X^4-X^3+zX^2-X+1} \perp \Pi_{X^4+z^2X^3+z^3X^2+z^2X+1}$	—
41	$\Pi_{X^4-X^3+zX^2-X+1} \perp \Pi_{X^4+z^3X^3+z^7X^2+z^3X+1}$	—
41	$\Pi_{X^4-X^3+zX^2-X+1} \perp \Pi_{X^4+z^5X^3+z^5X+1}$	—
41	$\Pi_{X-1} \perp \Pi_{X-1} \perp \Pi_{X-1} \perp \Pi_{X-1} \perp \Pi_{X^4-X^3+zX^2-X+1}$	—
16	$(\text{III}_{(X+z)(X+z^7)})^2 \perp \text{III}_{(X^2+z)(X^2+z^7)}$	—
16	$\text{III}_{(X+z)(X+z^7)} \perp \text{III}_{(X+z^2)(X+z^6)} \perp \text{III}_{(X^2+z)(X^2+z^7)}$	—
16	$\text{III}_{(X+z)(X+z^7)} \perp \text{III}_{(X+z^3)(X+z^5)} \perp \text{III}_{(X^2+z)(X^2+z^7)}$	—
16	$(\text{III}_{(X+z^2)(X+z^6)})^2 \perp \text{III}_{(X^2+z)(X^2+z^7)}$	—
16	$\text{III}_{(X^2+z)(X^2+z^7)} \perp \text{III}_{(X+z)(X+z^7)} \perp (\Pi_{X+1})^2$	unitär
16	$\text{III}_{(X^2+z)(X^2+z^7)} \perp \text{III}_{(X+z)(X+z^7)} \perp \Pi_{X-1} \perp \Pi_{X+1}$	unitär
16	$\text{III}_{(X^2+z^3)(X^2+z^5)} \perp \text{III}_{(X+z)(X+z^7)} \perp (\Pi_{X+1})^2$	unitär
16	$\text{III}_{(X^2+z)(X^2+z^7)} \perp \text{III}_{(X+z^2)(X+z^6)} \perp (\Pi_{X+1})^2$	—
16	$\text{III}_{(X^2+z)(X^2+z^7)} \perp \text{III}_{(X+z^2)(X+z^6)} \perp \Pi_{X-1} \perp \Pi_{X+1}$	—
16	$\text{III}_{(X^2+z)(X^2+z^7)} \perp (\Pi_{X+1})^4$	—
16	$\text{III}_{(X^2+z)(X^2+z^7)} \perp \Pi_{X-1} \perp (\Pi_{X+1})^3$	—
16	$\text{III}_{(X^2+z)(X^2+z^7)} \perp (\Pi_{X-1})^2 \perp (\Pi_{X+1})^2$	—
16	$\text{III}_{(X^4+z)(X^4+z^7)}$	—
13	$\Pi_{X-1} \perp \Pi_{X-1} \perp \text{III}_{(X^3-X-1)(X^3+X^2-1)}$	—
9	$\Pi_{(X-1)^5} \perp \Pi_{(X-1)^3}$	—
9	$\text{I}_{(X-1)^4}$	—
9	$\Pi_{(X-1)^5} \perp \text{I}_{X-1} \perp \Pi_{X-1}$	—
9	$\Pi_{(X-1)^7} \perp \Pi_{X-1}$	—

Anhang B

Ein Beispielprogramm in GAP

Als Beispiel für die Implementierung der Algorithmen dieser Arbeit geben wir hier ein GAP-Programm an, das den Stabilisator eines Ovoids berechnet. Der Algorithmus ist in Abschnitt 4.5 beschrieben.

Es sei K ein endlicher Körper, $n \in \mathbb{N}$ und $V := K^n$ ein quadratischer Raum. Weiterhin sei $\mathcal{O}$ ein Ovoid von V , so dass $\dim \langle \mathcal{O} \rangle = n$ ist. Mit der Funktion *ovoidStabilisator* läßt sich nun der Stabilisator von $\mathcal{O}$ in $\text{PTO}(V)$ berechnen.

ovoidStabilisator

Eingabe: der Körper $field := K$; die quadratische Form $qForm$ auf V ; eine Liste $ovo = \{p_1, \dots, p_r\} \subseteq V$, so dass $\{\langle p_1 \rangle, \dots, \langle p_r \rangle\} = \mathcal{O}$ ist.
Ausgabe: eine Gruppe $G \leq \Gamma O(V)$ als Matrixgruppe über dem Primkörper von K , so dass $\overline{G} \leq \text{PTO}(V)$ der Stabilisator von $\mathcal{O}$ ist.

Die Hilfsprogramme

Die Funktion *ovoidStabilisator* verwendet die folgenden Hilfsprogramme:

fingerPrtS

Eingabe: die quadratische Form $qForm$ auf V ; $ovo = \{p_1, \dots, p_r\} \subseteq V$ und $pt \in V$, so dass $\mathcal{C} := \{\langle p_1 \rangle, \dots, \langle p_r \rangle, \langle pt \rangle\}$ ein Teilovoid von V ist.
Ausgabe: $\mathfrak{J}_{\text{fi}}(\mathcal{C}, \langle pt \rangle)$ wie in Definition 4.1.3.

fingerPrtSS

Eingabe: die quadratische Form $qForm$ auf V ; $ovo = \{p_1, \dots, p_r\} \subseteq V$ und $pt1, pt2 \in V$, so dass $\mathcal{C} := \{\langle p_1 \rangle, \dots, \langle p_r \rangle, \langle pt1 \rangle, \langle pt2 \rangle\}$ ein Teilovoid von V ist.
Ausgabe: $\mathfrak{J}_{\text{fi}}(\mathcal{C}, \langle pt1 \rangle, \langle pt2 \rangle)$ wie in Definition 4.1.3.

footPrtS

Eingabe: die quadratische Form $qForm$ auf V ; $ovo = \{p_1, \dots, p_r\} \subseteq V$ und $pt \in V$, so dass $\mathcal{C} := \{\langle p_1 \rangle, \dots, \langle p_r \rangle, \langle pt \rangle\}$ ein Teilovoid von V ist.

Ausgabe: $\mathfrak{I}_{\text{fo}}(\mathcal{C}, \langle pt \rangle)$ wie in Definition 4.2.1.

footPrtSS

Eingabe: die quadratische Form $qForm$ auf V ; $ovo = \{p_1, \dots, p_r\} \subseteq V$ und $pt1, pt2 \in V$, so dass $\mathcal{C} := \{\langle p_1 \rangle, \dots, \langle p_r \rangle, \langle pt1 \rangle, \langle pt2 \rangle\}$ ein Teilovoid von V ist.

Ausgabe: $\mathfrak{I}_{\text{fi}}(\mathcal{C}, \langle pt1 \rangle, \langle pt2 \rangle)$ wie in Definition 4.2.1.

semiLinMapByGens

Eingabe: ein K -Vektorraum $W1$ mit Basis $gens1$; eine Liste $gens2$ von Vektoren eines K -Vektorraums mit $|gens1| = |gens2| =: d$; ein Körperautomorphismus $\sigma := sig$ von K .

Ausgabe: Eine σ -semilineare Abbildung $\phi: W1 \rightarrow \langle gens2 \rangle$ mit $\phi(gens1_i) = gens2_i$ für $1 \leq i \leq d$, falls eine solche existiert, *fail* sonst.

semiLinMapMat

Eingabe: eine Basis $gens1$ von V ; eine Liste $gens2 \subseteq V$ mit $|gens1| = |gens2|$; ein Körperautomorphismus $\sigma := sig$ von K .

Ausgabe: Eine Matrix über dem Primkörper von K , die eine σ -semilineare Abbildung $\phi: V \rightarrow V$ mit $\phi(gens1_i) = gens2_i$ für $1 \leq i \leq d$ definiert, falls eine solche existiert, *fail* sonst.

extendEquiv (Algorithmus 4.4.2)

Eingabe: die quadratische Form $qForm$ auf V ; $ovo = \{p_1, \dots, p_r\} \subseteq V$, so dass $\mathcal{O} := \{\langle p_1 \rangle, \dots, \langle p_r \rangle\}$ ein Ovoid von V ist; eine Basis $\{b_1, \dots, b_n\} \subseteq ovo$ von V ; eine Liste $sim \subseteq V$; $i0$ mit $1 \leq i0 \leq n$.

Ausgabe: Eine Semiähnlichkeit ϕ von V mit $\phi(\mathcal{O}) = \mathcal{O}$ und $\phi(\langle b_i \rangle) = \langle sim_i \rangle$ für $1 \leq i \leq i0 - 1$, falls eine solche existiert, $\emptyset$ sonst.

stabilizerDim

Eingabe: die quadratische Form $qForm$ auf V ; $ovo = \{p_1, \dots, p_r\} \subseteq V$, so dass $\mathcal{O} := \{\langle p_1 \rangle, \dots, \langle p_r \rangle\}$ ein Ovoid von V ist; eine Basis $B \subseteq ovo$ von V .

Ausgabe: Eine Gruppe $G \leq \Gamma\mathcal{O}(V)$ als Matrixgruppe über dem Primkörper von K mit $\bar{G} = \{\gamma \in \text{P}\Gamma\mathcal{O}(V) \mid \gamma(\mathcal{O}) = \mathcal{O} \text{ und } \gamma(\langle b \rangle) = \langle b \rangle \text{ für } b \in B\}$

stabilizer_i0

Eingabe: $i0$ mit $0 \leq i0 < n$; die quadratische Form $qForm$ auf V ; $ovo = \{p_1, \dots, p_r\} \subseteq V$, so dass $\mathcal{O} := \{\langle p_1 \rangle, \dots, \langle p_r \rangle\}$ ein Ovoid von V ist; eine Basis $B = \{b_1, \dots, b_n\} \subseteq ovo$ von V ; eine Gruppe $stab \leq \Gamma\mathcal{O}(V)$, so dass $\overline{stab} = \{\gamma \in \text{P}\Gamma\mathcal{O}(V) \mid \gamma(\mathcal{O}) = \mathcal{O} \text{ und } \gamma(\langle b_i \rangle) = \langle b_i \rangle \text{ für } i \leq i0 + 1\}$ ist.

Ausgabe: eine Gruppe $stab \leq \Gamma\mathcal{O}(V)$ mit

$\overline{stab} = \{\gamma \in \text{P}\Gamma\mathcal{O}(V) \mid \gamma(\mathcal{O}) = \mathcal{O} \text{ und } \gamma(\langle b_i \rangle) = \langle b_i \rangle \text{ für } 1 \leq i \leq i0\}$.

```

ovoidStabilisator:= function(ovo, field, qForm)
  local  fingerPrtS, fingerPrtSS, footPrtS, footPrtSS,
         semiLinMapByGens, semiLinMapMat, extendEquiv,
         stabilizerDim, stabilizer_i0, invarS, invarSS, K,
         fieldBas, dim, ovoSp, B, b, invList, i, D_i, j,
         O_B, VBas, stab, i0;

  ##### Hilfsprogramme #####

  fingerPrtS:=function(ovo,pt,qForm)
    local  squares, sMat, i, j, b, qVec, k;

    squares:= Set(field,x->x^2);
    squares:= Difference(squares,[Zero(field)]);

    sMat:=[];
    for i in [1..Size(ovo)] do
      sMat[i]:=[];
      for j in [1..i-1] do
        sMat[i][j]:=sMat[j][i];
      od;
      sMat[i][i]:= 0;
      for j in [i+1..Size(ovo)] do
        sMat[i][j]:=qForm(ovo[i]+ovo[j]);
        if sMat[i][j] in squares then
          sMat[i][j]:= 1;
        else
          sMat[i][j]:=-1;
        fi;
      od;
    od;
    b:=[];
    for i in [1..Size(ovo)]do
      b[i]:= qForm(ovo[i]+pt);
      if b[i] in squares then
        b[i]:= 1;
      else
        b[i]:=-1;
      fi;
    od;
    qVec:=[];
    for k in [1..Size(ovo)] do
      qVec[k]:=0;
      for i in [1..Size(ovo)] do
        qVec[k]:=qVec[k]+b[i]*sMat[k][i];
      od;
      qVec[k]:=AbsInt(qVec[k]);
    od;
    return Collected(Flat(qVec));
  end;

```

```
#####
fingerPrtSS:=function(ovo,pt1,pt2,qForm)
  local  field, squares, fpr, k, b_k1, b_k2;

  field:= Field(Concatenation(ovo));
  squares:= Set(field,x->x^2);
  squares:= Difference(squares,[Zero(field)]);
  fpr:=0;
  for k in [1..Size(ovo)] do
    b_k1 := qForm(ovo[k]+pt1);
    b_k2 := qForm(ovo[k]+pt2);
    if b_k1 in squares then
      b_k1:= 1;
    else
      b_k1:=-1;
    fi;
    if b_k2 in squares then
      b_k2:= 1;
    else
      b_k2:=-1;
    fi;
    fpr:=fpr+b_k1 *b_k2;
  od;
  fpr:=AbsInt(fpr);
  return fpr;
end;

#####
footPrtS:= function(cap,pkt,qForm)
  local  bMat, bVec, i, j, inv;

  bMat:=[];
  bVec:=[];
  for i in [1..Size(cap)] do
    bVec[i]:= qForm(cap[i]+pkt);
    bMat[i]:=[];
    for j in [1..i-1] do
      bMat[i][j]:=bMat[j][i];
    od;
    bMat[i][i]:= 0;
    for j in [i+1..Size(cap)] do
      bMat[i][j]:=qForm(cap[i]+cap[j]);
    od;
  od;
  inv:=[];
  for i in [1..Size(cap)] do
    for j in [i+1..Size(cap)] do
      Add(inv,bMat[i][j]*(bVec[i]*bVec[j])^(-1));
    od;
  od;
  inv:=Collected(inv);
  Apply(inv,x->x[2]);
  return(SortedList(inv));
end;
```

```
#####
footPrtSS:= function(cap,p1,p2,qForm)
  local  bVec1, bVec2, i, b12, inv;

  bVec1:=[];
  bVec2:=[];
  for i in [1..Size(cap)] do
    bVec1[i]:= qForm(cap[i]+p1);
    bVec2[i]:= qForm(cap[i]+p2);
  od;
  b12:=qForm(p1+p2);
  inv:=[];
  for i in [1..Size(cap)] do
    Add(inv,bVec1[i]*(bVec2[i]*b12)^(-1));
  od;
  inv:=Collected(inv);
  Apply(inv,x->x[2]);
  return(SortedList(inv));
end;

#####
semiLinMapByGens:=function(W1,gens1,gens2,sig)
  local  d, W2, sigN, ind, i, bas1, bild, mat, map;

  d:= Dimension(W1);
  W2:=VectorSpace(LeftActingDomain(W1),gens2);
  if d<>Dimension(W2) then
    Print("-");
    return fail;
  fi;
  sigN:= ShallowCopy(sig);
  if Size(gens1)<>Size(gens2) then
    return fail;
  fi;
  ind:= [1];
  i:=2;
  while Size(ind)<d do
    if not gens1[i] in
      VectorSpace(LeftActingDomain(W1),gens1[ind]) then
      Add(ind,i);
    fi;
    i:= i+1;
  od;
  bas1:=gens1[ind];
  bild:=gens2[ind];
  if Size(bas1)=Size(bas1[1]) then
    mat:= List(bas1^(-1),v->List(v,a->a^sig))*bild;
    map:=x->List(x,a->a^sigN)*mat;
  else
    bas1:=Basis(W1,bas1);
    map:=x->List(Coefficients(bas1,x),a->a^sigN)*bild;
  fi;
end;

```

```

    if ForAny(Difference([1..Size(gens1)],ind),
        i->map(gens1[i])<>gens2[i]) then
        return fail;
    fi;
    return MappingByFunction(W1,W2,map);
end;

#####
semiLinMapMat:= function(V, gens1, gens2, sig)
    local sigMat, blocks, sigMatBU, map, mat, matBU, sig_mat;

    sigMat:=List(fieldBas,b-> Coefficients( fieldBas,b^sig));
    blocks:= List([1..dim], i->[i,i,sigMat]);
    sigMatBU:=BlockMatrix(blocks,dim,dim);
    map:=semiLinMapByGens(V, gens1, gens2, sig);
    mat:=List(VBas,b-> Coefficients(VBas,b^map));
    matBU:=BlownUpMat( fieldBas, mat );
    sig_mat:=sigMatBU*matBU;
    return sig_mat;
end;

#####
extendEquiv:=function(B, sim, i_0, ovo, qForm)
    local is010nTo02, isFeasSigma, invSSTest, sigmas, sig,
        multi, phi, i, lambda, W, map, im, Im, x,
        ovoDiff, phi_x;

    # testet, ob das Bild von 0 unter der sig-semilinearen
    # Abbildung sim gleich 0v2 ist.
    is010nTo02:= function(sim,sig,0_B,0v2)
        local Im, i, x;
        Im := [];
        for i in [1..Size(0_B)] do
            x:=0_B[i];
            Im[i]:=Sum([1..Size(sim)], j->x[j]^sig * sim[j]);
            Im[i]:=Im[i]*First(Im[i],k->k<>0*k)^(-1);
        od;
        if Set(Im)=Set(0v2) then
            return true;
        fi;
        return false;
    end;

    isFeasSigma:= function(sig,qForm, 0_B, B, 0v2, sim, i_0)
        local multi, phi, i, lambda;
        if i_0-1>=3 then
            multi:=qForm(B[2]+B[3])^sig *qForm(sim[1]+sim[2])
                *qForm(sim[1]+sim[3])
                /(qForm(B[1]+B[3])^sig *qForm(B[2]+B[1])^sig
                *qForm(sim[2]+sim[3]));
            phi:=[];
            phi[1]:=sim[1];
            for i in [2..i_0-1] do
                lambda:= multi*qForm(B[1]+B[i])^sig/qForm(sim[1]+sim[i]);

```

```

        phi[i] := lambda*sim[i];
    od;
    ## Definiert phi eine Semiähnlichkeit?:
    if ForAny([2..i_0-2], k-> qForm(phi[k]+phi[i_0-1])
        <> multi*qForm(B[k]+B[i_0-1])^sig) then
        return false;
    fi;
    return true;
end;

invSSTest:=function(inv_0,ovo,sim,i0,invarSS,qForm)
    local k,b1,b2,b3,s1,s2,s3;
    for k in [1..i0-1] do
        if invarSS(ovo,sim[i0],sim[k],qForm) <> inv_0[i0][k] then
            return false;
        fi;
    od;
    return true;
end;

sigmas:= Set(Group(FrobeniusAutomorphism(field)));
if i_0-1>=3 then
    sigmas:=
        Filtered(sigmas,sig->
            isFeasSigma(sig,qForm, 0_B, B, ovo, sim, i_0));
    if sigmas =[] then
        return [];
    fi;
fi;
if i_0 > Size(B) then
    # teste ob es einen Semiähnlichkeit phi gibt mit
    # phi(<B_i>)=sim(<B_i>), die ovo auf ovo abbildet?
    for sig in sigmas do
        multi:=qForm(B[2]+B[3])^sig *qForm(sim[1]+sim[2])
            *qForm(sim[1]+sim[3])
            /(qForm(B[1]+B[3])^sig *qForm(B[2]+B[1])^sig
            *qForm(sim[2]+sim[3]));
        phi:=[];
        phi[1]:=sim[1];
        for i in [2..i_0-1] do
            lambda:= multi*qForm(B[1]+B[i])^sig/qForm(sim[1]+sim[i]);
            phi[i] := lambda*sim[i];
        od;
        if is010nTo02(phi,sig,0_B,ovo) then
            W:= Subspace(field^dim,B);
            map:=semiLinMapByGens(W,B,phi,sig);
            im:= List(VBas,b->b^map);
            map:=semiLinMapMat
                (field^dim,VBas,im,sig);
            if map<> fail then
                return map;
            fi;
        fi;
    end;
fi;

```

```

        od;
        return[];
    fi;
    ## Die möglichen Fortsetzungen von sim werden gesucht:
    Im:= Difference(ovo,sim{[1..i_0-1]});
    for x in Im do
        sim[i_0]:=x;
        ovoDiff:=Difference(ovo,sim{[1..i_0]});
        if invSSTest(invList[3],ovoDiff,sim,i_0,invarSS,qForm) then
            if i_0>1
                or invarS(ovoDiff,x,qForm)= invList[1][i_0] then
                    sim[i_0]:=x;
                    phi_x := extendEquiv(B, sim, i_0+1, ovo,qForm);
                    if phi_x <> [] then
                        return phi_x;
                    fi;
                fi;
            fi;
        od;
        return[];
    end;

#####
stabilizerDim:= function(ovo,B,qForm)
    local ptMapToMaps, stab_dim, phi_sigList, phiSig, phi,
        sig, map, ovoIm, mat;

    # Bestimmt die Semiähnlichkeiten die B[i] auf sim[i]
    # abbilden für 0<=i<=Size(B)
    ptMapToMaps:= function(B,sim,qForm)
        local sigmas, bForm, maps, sig, multi, phi, i, lambda;

        sigmas:= Group(FrobeniusAutomorphism(field));
        bForm:= function(x,y)
            return qForm(x+y)-qForm(x)- qForm(y);
        end;
        if ForAny([2..Size(sim)],
            i->bForm(sim[1],sim[i])=Zero(field)) then
            return [];
        fi;
        maps:=[];
        for sig in sigmas do
            multi:=bForm(B[2],B[3])^sig *bForm(sim[1],sim[2])
                *bForm(sim[1],sim[3])
                / ( bForm(B[1],B[3])^sig *bForm(B[2],B[1])^sig
                    *bForm(sim[2],sim[3]) );
            phi:=[];
            phi[1]:=sim[1];
            for i in [2..Size(sim)] do
                lambda:= multi*bForm(B[1],B[i])^sig/bForm(sim[1],sim[i]);
                phi[i]:= lambda*sim[i];
            od;
            ## Definiert phi eine Semiähnlichkeit?:
            if ForAll(Combinations([1..Size(sim)],2), k->

```

```

        bForm(phi[k[1]],phi[k[2]])
        = multi*bForm(B[k[1]],B[k[2]])^sig)
    and ForAll([1..Size(sim)], i->
        qForm(phi[i])= multi*qForm(B[i])^sig) then
        Add(maps, [phi,sig, multi]);
    fi;
od;
return maps;
end;

ovo:= List(ovo, p->p*First(p,a->a<>0*a)^-1);
stab_dim:=[];
phi_sigList:= ptMapToMaps(B,B,qForm);
for phiSig in phi_sigList do
    phi:= phiSig[1];
    sig:= phiSig[2];
    map:=semiLinMapByGens(field^dim,B,phi,sig);
    ovoIm:= List(ovo,p->p^map);
    ovoIm:= List(ovoIm, p->p*First(p,a->a<>0*a)^-1);
    if Set(ovoIm)=Set(ovo) then
        mat:= semiLinMapMat(field^dim,B,phi,sig);
        Add(stab_dim,mat);
    fi;
od;
return Group(stab_dim);
end;

#####
stabilizer_i0:= function(ovo,B,stab,qForm,i0)
    local orbitsSemiGrpOnLines, orbs, gens, o, p, sim, map_o;
    orbitsSemiGrpOnLines:= function(grp,set)
        local bdVec, basV, orbs;
        bdVec:= function(v, fieldBas)
            local e, d, w, i, w_i;
            e:= CanonicalBasis(field^dim);
            d:= Size(fieldBas);
            w:=[];
            for i in [1..dim] do
                w_i:=v{[(i-1)*d+1..i*d]};
                w[i]:= Sum([1..d],j->fieldBas[j]*w_i[j]);
            od;
            w:= Sum([1..dim], i->e[i]*w[i]);
            w:= w*First(w,a->a<>0*a)^-1;
            return w;
        end;
        basV:= CanonicalBasis(field^dim);
        set:= List(set,v->BlownUpVector( fieldBas, v));
        orbs:=Orbits(grp, set,OnLines);
        orbs:= Set(orbs, ob-> Set(ob,v -> bdVec(v, fieldBas)));
        return orbs;
    end;
    orbs:= orbitsSemiGrpOnLines(stab,ovo);
    gens:= ShallowCopy(GeneratorsOfGroup(stab));
    orbs:= Difference(orbs, List(B{[1..i0]},x->[x]));

```

```

    for o in orbs do
        p:= o[1];
        sim:=Concatenation(B{[1..i0]}, [p]);
        map_o:=extendEquiv(B,sim,i0+2,ovo, qForm);
        if map_o<>[] then
            Add(gens, map_o);
        fi;
    od;
    return Group(gens);
end;

##### Hauptprogramm: #####
if Characteristic(field)=2 then
    invarS:= footPrtS; invarSS:= footPrtSS;
else
    invarS:= fingerPrtS; invarSS:= fingerPrtSS;
fi;
K:= PrimeField(field);
fieldBas:= Basis(VectorSpace(K,Set(field)));
dim:= Size(ovo[1]);
ovo:= List(ovo,x->x*First(x, a->a<>0*a)^-1);
ovoSp:=VectorSpace(field,ovo);
B:=[];
while Size(B)< dim do
    b:=First(ovo, p -> not p in Subspace(field^dim,B));
    if b=fail then Error(); fi;
    Add(B,b);
od;
invList:=([],[],[]);
for i in [1..Size(B)] do
    D_i:=Difference(ovo,B{[1..i]});
    invList[1][i]:=invarS(D_i,B[i],qForm);
    invList[3][i]:=[];
    for j in [1..i-1] do
        invList[3][i][j]:=invarSS(D_i,B[i],B[j],qForm);
    od;
od;
B:= Basis(VectorSpace(field,B),B);
O_B:= List(ovo,x->Coefficients(B,x));
VBas:= CanonicalBasis(field^dim);
stab:= stabilizerDim(ovo,B,qForm);
i0:=dim-1;
while i0>=0 do
    stab:=stabilizer_i0(ovo,B,stab,qForm,i0);
    i0:=i0-1;
od;
return stab;
end;

```

Literaturverzeichnis

- [BM95] BLOKHUIS, A. und G.E. MOORHOUSE: *Some p -ranks related to orthogonal spaces*. Journal of Algebraic Combinatorics., 4(4):295–316, 1995.
- [Cam00] CAMERON, P.J.: *Projective and Polar Spaces*. QWM Math Notes 13, 2nd Edition, 2000. <http://www.maths.qmul.ac.uk/~pjc/pps/>.
- [CD98] CHARNES, C. und U. DEMPWOLFF: *The Translation Planes of Order 49 and their Automorphism Groups*. Mathematics of Computation, 67(223):1207–1224, 1998.
- [CD00] CHARNES, C. und U. DEMPWOLFF: *The Eight Dimensional Ovoids Over $\text{GF}(5)$* . Mathematics of Computation, 70(234):853–861, 2000.
- [CKW88] CONWAY, J.H., P.B. KLEIDMAN und R.A. WILSON: *New families of ovoids in O_8^+* . Geometriae Dedicata, 26(2):157–170, 1988.
- [Coo90] COOPERSTEIN, B.N.: *A sporadic ovoid in $\Omega^+(8, 5)$ and some non-Desarguesian translation planes of order 25*. Journal of Combinatorial Theory. Series A, 54(1):135–140, 1990.
- [CPT06] CARDINALI, I., O. POLVERINO und R. TROMBETTI: *Semifield planes of order q^4 with kernel F_{q^2} and center F_q* . European Journal of Combinatorics, 27(6):940–961, 2006.
- [CW99] CORDERO, M. und G.P. WENE: *A survey of finite semifields*. Discrete Mathematics, 208–209:125–137, 1999.
- [Dema] DEMPWOLFF, U. http://www.mathematik.uni-kl.de/~dempw/dempw_49.html.
- [Demb] DEMPWOLFF, U.: *Semifield Planes of Order 81*. http://www.mathematik.uni-kl.de/~dempw/81_semi_FILES/keim.ps. Preprint.
- [Dye77] DYE, R.H.: *Partitions and their stabilizers for line complexes and quadratics*. Annali di Matematica Pura ed Applicata. Serie Quarta, 114:173–194, 1977.

- [FJ84] FOULSER, D.A. und N.L. JOHNSON: *The translation planes of order q_2 that admit $\text{SL}(2, q)$ as a collineation group. I: Even order.* Journal of Algebra, 86:385–406, 1984.
- [GM97] GUNAWARDENA, A. und G.E. MOORHOUSE: *The non-existence of ovoids in $\text{O}_9(q)$.* European Journal of Combinatorics, 18(2):171–173, 1997.
- [Gro02] GROVE, L.C.: *Classical Groups and Geometric Algebra.* American Mathematical Society, 2002.
- [Gun00] GUNAWARDENA, A.: *Primitive ovoids in $\text{O}_8^+(q)$.* Journal of Combinatorial Theory. Series A, 89(1):70–76, 2000.
- [HJ90] HUANG, H. und N.L. JOHNSON: *8 semifield planes of order 8^2 .* Discrete Mathematics, 80(1):69–79, 1990.
- [HP73] HUGHES, D.R. und F.C. PIPER: *Projective Planes*, Band 6 der Reihe *Graduate Texts in Mathematics*. Springer, 1973.
- [Hup70] HUPPERT, B.: *Singer-Zyklen in klassischen Gruppen.* Mathematische Zeitschrift, 117:141–150, 1970.
- [Hup80a] HUPPERT, B.: *Isometrien von Vektorräumen 1.* Arch. Math, 1980.
- [Hup80b] HUPPERT, B.: *Isometrien von Vektorräumen II.* Mathematische Zeitschrift, 175(175):5–20, 1980.
- [Kan82a] KANTOR, W.M.: *Ovoids and Translation Planes.* Can. J. Math., XXXIV(5):1195–1207, 1982.
- [Kan82b] KANTOR, W.M.: *Spreads, Translation Planes and Kerdock Sets.* SIAM J. Alg. Disc. Meth., 3(2):151–165, 1982.
- [Kan82c] KANTOR, W.M.: *Translation planes of order q^6 admitting $\text{SL}(2, q^2)$.* Journal of Combinatorial Theory, Series A, 32:299–302, 1982.
- [Kle88] KLEIDMAN, P.B.: *The 2-transitive ovoids.* Journal of Algebra, 117(1):117–135, 1988).
- [Knu65] KNUTH, D.E.: *Finite Semifields and Projective Planes.* Journal of Algebra, 2:182–217, 1965.
- [Lün80] LÜNEBURG, H.: *Translation Planes.* Springer, 1980.
- [Moo93a] MOORHOUSE, G.E.: *Ovoids from the E_8 Root Lattice.* Geometriae Dedicata, 1993.

- [Moo93b] MOORHOUSE, G.E.: *Root lattice constructions of ovoids*. In: DE CLERCK, F. et al. (Herausgeber): *Finite geometry and combinatorics*, Band 191 der Reihe *Lond. Math. Soc. Lect. Notes*, Seiten 269–275. The 2nd international conference at Astene-Deinze, Belgium 31 May - 6 June 1992, Cambridge University Press, 1993.
- [MR95] MATHON, R. und G.F. ROYLE: *The translation planes of order 49*. *Designs, Codes and Cryptography*, 5(1):57–72, 1995.
- [Mwe76] MWENE, B.: *On the Subgroups of the Group $\text{PSL}_4(2^m)$* . *Journal of Algebra*, 41:79–107, 1976.
- [Shu85] SHULT, E.E.: *A sporadic ovoid in $\Omega^+(8, 7)$* . *Algebras, Groups and Geometries*, 2:495–513, 1985.
- [Tay92] TAYLOR, D.E.: *The Geometry of the Classical Groups*. Heldermann Verlag Berlin, 1992.
- [Tha81] THAS, J.A.: *Ovoids and Spreads of Finite Classical Polar Spaces*. *Geometriae Dedicata*, Seiten 135–143, 1981.
- [Tha01] THAS, J.A.: *Ovoids, spreads and m-systems of finite classical polar spaces*. In: HIRSCHFELD, J. W. P. (Herausgeber): *Surveys in combinatorics, 2001*, London Math. Soc. Lect. Note Ser. 288, Seiten 241–267. Cambridge University Press, 2001.
- [Tit61] TITS, J.: *Les groupes simples de Suzuki et de Ree*. In: *Sem. Bourbaki*, Band 6. Société Mathématique de France, Paris, 1960/61.
- [Wal63a] WALKER, R.J.: *Determination of division algebras with 32 elements*. In: *Proc. Sympos. Appl. Math.*, Band 15, Seiten 83–85, 1963.
- [Wal63b] WALL, G.E.: *On the conjugacy classes in the unitary, symplectic and orthogonal groups*. *Journal of the Australian Mathematical Society*, 3:1–62, 1963.
- [Wil99] WILLIAMS, B.: *Ovoids of parabolic and hyperbolic spaces*. Doktorarbeit, University of Western Australia, 1999. <http://cage.rug.ac.be/geometry/Theses/33/bwilliams.pdf>.
- [Zas58] ZASSENHAUS, H.: *On a normal form of the orthogonal transformation. I–III*. *Can. Math. Bull.*, 1:31–39, 101–111, 183–191, 1958.

Werdegang der Verfasserin

1984 – 1993 Gymnasium der Alfred-Delp-Schule Hargesheim

1993 – 2001 Universität Kaiserslautern

Studium der Mathematik mit Anwendungsfach Informatik

Diplomarbeit: „Beschreibung und Implementierung eines Algorithmus zur Berechnung von Äquisingularitätsstrata“

1996 – 1998 Universität Kaiserslautern

Wissenschaftliche Hilfskraft (Übungsleiterin) am Fachbereich Mathematik

2001 – 2006 Universität Kaiserslautern

Wissenschaftliche Mitarbeiterin am Fachbereich Mathematik

About the author

2001 – 2006 University of Kaiserslautern

Research associate at the Department of Mathematics

1993 – 2001 University of Kaiserslautern

Studies of Mathematics with minor subject Computer Science

Diploma thesis: „Beschreibung und Implementierung eines Algorithmus zur Berechnung von Äquisingularitätsstrata“

1984 – 1993 Alfred-Delp-Schule, Hargesheim