Konstruktion von PG(d, p^k) mit Singer Differenzenmengen

Ausarbeitung zum Seminar Diskrete Mathematik bei Prof. W. Hochstättler
im Sommersemester 2011 an der FernUniversität in Hagen

von Timo Bingmann

Zusammenfassung

Die Entwicklung von Differenzenmengen in der Design Theorie begann 1938 mit einer algebraischen Untersuchung endlicher projektiver Geometrien von James Singer. Nach Einführung der wichtigsten Grundbegriffe der Design Theorie und projektiver Geometrien werden in dieser Ausarbeitung die beiden Resultate von Singer entwickelt. Die Existenz einer Kollineation mit Periode $\frac{n^{d+1}-1}{n-1}$ führt zur Definition von Differenzenmengen und beide Ergebnisse liefern elegante Konstruktionsverfahren für PG(d, p^k).

1 Motivation und Geschichte der Design Theorie

Zu den Grundinteressen eines Mathematiker gehört zweifelsohne möglichst viele Aussagen über Strukturen zu treffen, die einige wenige, genau vorgegebene Eigenschaften erfüllen. Beispiele hierfür sind die Peano-Axiome für die natürlichen Zahlen oder die Axiome der euklidischen Geometrie. In der Design Theorie werden solche Untersuchungen für diskrete endliche Mengen streng formalisiert und eine Vielzahl verschiedenster endlicher Konstruktionen mit Begriffen und Parametern klassifiziert. Ein kombinatorisches Design ist hierbei in der allgemeinsten Definition nichts anderes als eine nach festgelegten Regeln getroffene Auswahl von Teilmengen einer Grundmenge.

4	9	2
3	5	7
8	1	6

Die Ursprünge der Design Theorie liegen eher in überraschenden mathematischen Besonderheiten und kombinatorischen Rätseln als in zielgerichteten Untersuchungen [ACDG06]. So ist das „Magische“ 3×3 Quadrat, das alle Zahlen von eins bis neun enthält und in allen Zeilen, Spalten und Diagonalen die Summe 15 ergibt, in China mindestens seit dem fünften bis dritten Jahrhundert v. Chr. bekannt und tritt unter dem Namen „Luo-Shu“ auf [Swe08]. Beschäftigung mit diesem und vergleichbaren Zahlenmustern sind leider oft weniger von Interesse an kombinatorischer Mathematik als von religiösen Mystizismus und Numerologie geprägt.

Zu den geschichtlich alten kombinatorischen Strukturen zählen auch *Lateinische Quadrate*, die in jeder Zeile und Spalte alle Elemente einer Grundmenge genau einmal enthalten. Bei dem folgenden Rätsel treten zwei spezielle Lateinische Quadrate auf:

> Gegeben sind die 16 Karten eines französischen Kartenblatts mit den vier Werten As, König, Dame und Bube in den vier Farben Herz, Karo, Pik und Kreuz. Diese Karten sollen auf den Tisch in ein 4×4 Quadrat gelegt werden, so dass in jeder Zeile und Spalte jede Kartenfarbe und jeder Kartenwert genau einmal auftritt.

In der folgenden Abbildung ist eine von vielen Lösungen gezeigt. Die Lösung besteht aus zwei Lateinischen Quadraten, die übereinander gelegt die Eigenschaft haben, dass jedes Paar Kartenwert und Kartenfarbe, also jede Karte genau einmal vorkommt. Ein Paar solcher Lateinischer Quadrate nennt man *orthogonal*.

A♡$_1$	Q♢$_2$	J♠$_3$	K♣$_4$
K♠$_2$	J♣$_1$	Q♡$_4$	A♢$_3$
Q♣$_3$	A♠$_4$	K♢$_1$	J♡$_2$
J♢$_4$	K♡$_3$	A♣$_2$	Q♠$_1$

Überraschenderweise kann man zu den orthogonalen Eigenschaften Kartenwert und Kartenfarbe eine weitere unabhängige Variable hinzufügen, in der Abbildung einfach die Zahlen eins bis vier, so dass wieder jedes Paar Kartenwert und Zahl, sowie Kartenfarbe und Zahl genau einmal auftritt. Diese Eigenschaft von paarweise orthogonalen Lateinischen Quadraten wird beispielsweise in der experimentellen Statistik verwendet, um drei unabhängige Variablen mit nur 16 Versuchsanordnungen zu prüfen.

Ein weitaus schwierigeres Rätsel ist das von Kirkman 1850 gestellte „Fünfzehn Schulmädchen Problem“:

> Fünfzehn Schulmädchen gehen an jedem Tag der Woche zu dritt spazieren. Wie kann man die Gruppen anordnen, sodass jedes Mädchen nur einmal in der Woche mit jedem anderen Mädchen unterwegs ist.

Der erste Schritt zur Lösung dieser Aufgabe besteht darin, aus einer Menge mit 15 Elementen Teilmengen der Größe 3 zu wählen, so dass jedes Paar der Grundmenge in genau einer Teilmenge enthalten ist. Heute nennt man eine solche Struktur ein ***Steiner Tripel System***, das ein Sonderfall allgemeinerer *Block-Designs* darstellt. Um die Aufgabe jedoch zu lösen, muss das Steiner Tripel System weiter aus genau 7 Teilmengen von Tripeln bestehen, in denen jedes Element genau einmal vorkommt.

Statt einer Vertiefung in dieses spezielle Problem (siehe [Col06; Bal26] für Lösungen und Konstruktionsmethoden), wenden wir uns der allgemeineren Theorie solcher Auswahlkriterien zu.

2 Grundlagen der Design Theorie

Definition 1. Ein ***Block-Design*** ist eine Auswahl $\mathcal{B}$ von Teilmengen einer Grundmenge S, so dass alle Teilmengen $B \in \mathcal{B}$ eine feste Größe k haben. Die Mengen B heißen dann auch die ***Blöcke*** von $\mathcal{B}$.

Ein Block-Design $\mathcal{B}$ über S kann man auch als ein Inzidenzsystem mit Relation $I \subseteq S \times \mathcal{B}$ auffassen. Hierbei wird schlicht ein Element $s \in S$ als inzident zur Teilmenge $B \in \mathcal{B}$ gezählt, falls $s \in B$.

Als erste einfache Bedingung an ein Design kann man die Vorgabe stellen, dass jedes Element $s \in S$ in den Blöcken als Ganzes gleich häufig vorkommt. Solch ein Design heißt auch *regulär* mit Parameter r, der konstanten Häufigkeit eines Elements. Stellt man noch eine weitere Bedingung an die Paare von S, so erhält man folgende viel studierte Familie von Designs.

Definition 2. Ein ***balanciertes unvollständiges Block-Design*** (BIBD) ist ein Block-Design $\mathcal{B}$ über S, in dem kein Block $B \in \mathcal{B}$ identisch S ist, jedes Element $s \in S$ in genau r Blöcken vorkommt und für jedes Paar $x, y \in S$ mit $x \neq y$ die Anzahl der Blöcke, die sowohl x als auch y enthalten, eine Konstante λ ist.

Dann heißt $\mathcal{B}$ ein (v, b, r, k, λ)-BIBD, wobei $v = |S|$ die Anzahl der Grundelemente, $b = |\mathcal{B}|$ die Anzahl der Blöcke aus der Grundmenge, $r = |\{B \in \mathcal{B} \mid s \in B\}|$ die konstante Anzahl der Blöcke die $s \in S$ enthalten, $k = |B|$ die konstante Mächtigkeit aller $B \in \mathcal{B}$ und $\lambda = |\{B \in \mathcal{B} \mid x, y \in B, x \neq y\}|$ die konstante Anzahl von Blöcken ist, die ein Paar $x, y \in S$ mit $x \neq y$ enthalten.

Die Bezeichnung *balanciert* bezieht sich auf die Eigenschaft, dass alle Paare aus S gleich häufig vorkommen. Dahingegen hebt die Bezeichnung *unvollständig* hervor, dass kein Block gleich S ist, denn sonst würde $\mathcal{B} = \{S\}$ folgen. Besonders interessant sind ***symmetrische*** BIBDs, in denen $v = b$ und damit $r = k$ gilt.

Die Aufgabe der Design Theorie besteht nun darin festzustellen, für welche Parameter ein Design existiert und gegebenenfalls eines anzugeben. Hierfür gibt es keine allgemeine Theorie, vielmehr werden durch verschiedene Konstruktionsverfahren Designs erzeugt oder es treten bei vorgegebenen Problemstellungen auf natürliche Art Designs mit bestimmten Parametern hervor. Dies ist beispielsweise bei endlichen Geometrien der Fall.

3 Synthetische endliche Geometrie

Die Design Theorie ist eng mit der Theorie endlicher Geometrien verwandt. Im Gegensatz zur euklidischen Geometrie besteht eine endliche Geometrie aus einer nur endlichen Anzahl von Punkten und Geraden. Solche Konstruktionen kommen erstmals in den Werken von Karl Georg Christian von Staudt (1856) und Gino Fano (1892) vor [Hir79]. Folgende erste allgemeine Definition stellt eine endliche Geometrie als Inzidenzsystem vor.

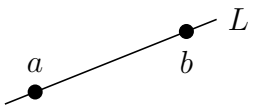
Definition 3. Eine ***endliche Geometrie*** $\mathcal{G} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ besteht aus einer endlichen Menge $\mathcal{P}$, den „Punkten“, einer endlichen Menge $\mathcal{L}$, den „Geraden“, und einer Inzidenzrelation $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$ zwischen diesen beiden Mengen. Anschaulich „liegt“ ein Punkt $a \in \mathcal{P}$ auf einer Geraden $L \in \mathcal{L}$, wenn $(a, L) \in \mathcal{I}$. Wir schreiben hierfür auch intuitiv $a \in L$.

Speziellere Ausprägungen endlicher Geometrien werden aus diesem allgemeinen Inzidenzsystem durch Restriktion der Relation in Form von Axiomen gebildet. Hier tritt die Verbindung der endlichen Geometrie zur Design Theorie direkt hervor: die vorausgesetzten Axiome entsprechen den Vorgaben bei der Auswahl von Teilmengen zu einem Design. Endliche Geometrien dienen daher hervorragend als Illustrationen von kombinatorischen Konfigurationen und umgekehrt.

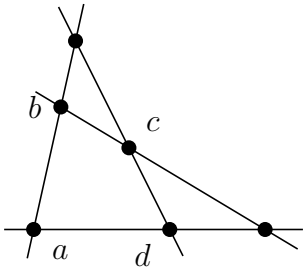
Es gibt zwei wichtige Ausprägungen endlicher Geometrien: *affine Geometrien*, in denen der euklidische Begriff von parallelen Geraden erhalten bleibt, und *projektive Geometrien*, in denen jedes Paar Geraden einen Schnittpunkt hat, es also keine parallelen Geraden gibt.

In dieser Ausarbeitung werden ausschließlich endliche projektive Geometrien betrachtet und konstruiert. Die erste systematische Untersuchung endlicher projektiver Geometrien wird Veblen und Young [VY10] angerechnet. Diese geben zwei Definitionen an: eine synthetische bestehend aus Axiomen an die Inzidenzrelation und eine analytische Definition, die konstruktiv aus einem Vektorraum über einem endlichen Körper die Geometrie erzeugt.

Definition 4. Eine ***synthetische projektive Geometrie*** ist eine endliche Geometrie $\mathcal{G} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, so dass folgende Axiome erfüllt sind:



(i) Zu je zwei verschiedenen Punkten $a, b \in \mathcal{P}$ existiert genau eine Gerade $L \in \mathcal{L}$, die beide Punkte enthält: $\{a, b\} \subset L$. Diese wird auch mit $[a, b] \in \mathcal{L}$ bezeichnet.



(ii) (*Axiom von Veblen-Young*)
Seien $a, b, c, d \in \mathcal{P}$ vier verschiedene Punkte, von denen keine drei auf einer Geraden liegen. Schneiden sich die Geraden $[a, b]$ und $[c, d]$ in einem Punkt, dann schneiden sich auch die Geraden $[a, d]$ und $[b, c]$.

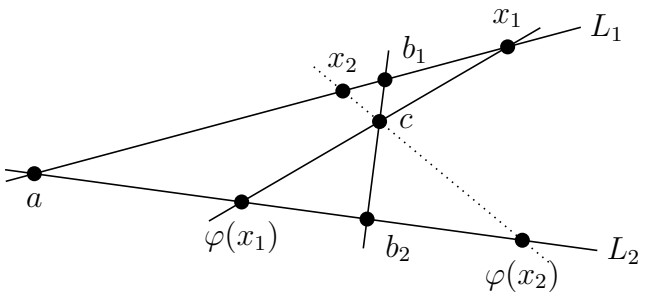
(iii) Jede Gerade enthält mindestens drei Punkte.

Wir wenden nun in folgendem Satz diese Axiome an, mit welchem dann die *Ordnung* einer projektiven Geometrie definiert wird.

Satz 1. Sind L_1 und L_2 zwei Geraden einer synthetischen projektiven Geometrie, dann gibt es eine bijektive Abbildung $\varphi : L_1 \to L_2$, also eine Abbildung zwischen den Punkten beider Geraden.

Beweis (nach [BR04, S. 22]). Wir können annehmen, dass $L_1 \neq L_2$ ist. Es gibt zwei Fälle zu unterschieden:

1. Fall: Die Geraden L_1 und L_2 schneiden sich in einem Punkt a. Seien b_1 und b_2 jeweils ein weiterer Punkt auf L_1 bzw. L_2. Nach dem dritten Axiom gibt es auf der Geraden $[b_1, b_2]$ einen weiteren Punkt c, der nicht auf L_1 oder L_2 liegt, sonst wäre $L_1 = L_2$. Betrachte nun einen weiteren Punkt x_1 auf L_1, so liegen die vier Punkte a, x_1, b_2, c nicht alle auf einer Geraden und $[a, x_1]$ schneidet $[c, b_2]$ im Punkt b_1. Mit dem zweiten Axiom folgt nun die Existenz eines Punktes im Schnitt der Geraden $[a, b_2]$ und $[x_1, c]$, der $\varphi(x_1)$ genannt wird und auf $[a, b_2] = L_2$ liegt. Mit dieser Konstruktion kann nun für jeden Punkt $x_i \in L_1 \setminus \{a\}$ genau ein Punkt $\varphi(x_i)$ auf L_2 bestimmt werden. Setzt man diese Abbildung für den Schnittpunkt a durch $\varphi(a) = a$ fort, erhält man die gesuchte Bijektion zwischen L_1 und L_2.



2. Fall: Die Geraden L_1 und L_2 schneiden sich nicht. Seien $a_1 \in L_1$ und $a_2 \in L_2$ zwei Punkte von L_1 bzw. L_2, dann gibt es nach dem ersten Axiom eine Gerade $[a_1, a_2]$, die L_1 und L_2 scheidet. Aus dem ersten Fall folgt, dass eine Bijektion $\varphi_1 : L_1 \to [a_1, a_2]$ und eine Bijektion $\varphi_2 : [a_1, a_2] \to L_2$ existieren, womit dann eine Bijektion $\varphi = \varphi_2 \circ \varphi_1 : L_1 \to L_2$ gefunden ist. □

Definition 5. Aus Satz 1 folgt unmittelbar: alle Geraden einer projektiven Geometrie enthalten gleich viele Punkte. Sei $q \in \mathbb{N}$ derart, dass jede Gerade $q+1$ Punkte enthält, so ist wegen Axiom drei $q \geq 2$. Diese Zahl q heißt die ***Ordnung*** der projektiven Geometrie.

4 Konstruktion und Design endlicher Geometrien

Die vorausgehende synthetische Definition schließt sich der traditionellen Axiomatik der euklidischen Geometrie an, wohingegen folgende analytische Definition eine Geometrie durch explizite Angabe eines Koordinatensystems konstruiert.

Definition 6. Mit folgender Konstruktion erhält man eine ***analytische projektive Geometrie* PG(d, n)** der Dimension $d \in \mathbb{N}_1$ über dem endlichen Körper GF(n) für eine Primzahlpotenz $n = p^k$. Eine analytische projektive Geometrie der Dimension $d = 2$ heißt auch ***endliche projektive Ebene***.

Sei $V = \mathrm{GF}(n)^{d+1}$ der $(d+1)$-dimensionale Vektorraum über GF(n), dann definiert man die 1-dimensionalen Untervektorräume als Punkte $\mathcal{P}$, die 2-dimensionalen Untervektorräume als Geraden $\mathcal{L}$ und setzt einen Punkt $p \in \mathcal{P}$ inzident zu einer Gerade $L \in \mathcal{L}$, falls $p \subset L$ als Untervektorräume von V [BR04, S. 54].

Diese Definition verlangt einige Erläuterungen. Um die Objekte besser handhaben zu können, entwickeln wir erst ein Koordinatensystem zur Beschreibung bestimmter Untervektorräume.

Betrachte die 1-dimensionalen Untervektorräume. Diese werden durch Angabe eines vom Nullvektor verschiedenen Vektors vollständig bestimmt. Da Vektoren, die Vielfache voneinander sind, denselben Untervektorraum beschreiben, konstruieren wir hierfür eine Äquivalenzrelation $\sim \subseteq V \times V$ durch

$$(x_0, \ldots, x_d) \sim (y_0, \ldots, y_d) \quad :\Longleftrightarrow \quad \exists\, \alpha \in \mathrm{GF}(n) \;:\; (\alpha x_0, \ldots, \alpha x_d) = (y_0, \ldots, y_d)$$

Nun kann man die Menge der Punkte angeben als $\mathcal{P} = (\mathrm{GF}(n)^{d+1} \setminus \{0\}) \,/\, \sim$, also als Menge aller $(d+1)$-dimensionalen Vektoren über $\mathrm{GF}(n)$ ohne den Nullvektor und identifiziert alle Vektoren, die skalare Vielfache voneinander sind.

Eine bequeme, normalisierte Schreibweise von $\mathcal{P}$ erhält man, wenn man mit den Repräsentanten der Gestalt $(0, \ldots, 0, 1, *, \ldots, *) \in \mathcal{P}$ arbeitet, wobei die führende Eins vorhanden sein muss, die Folge Nuller auch leer sein kann und $*$ beliebige Elemente des endlichen Körpers sind. Diese Darstellungen heißen auch die ***homogenen Koordinaten*** der Punkte.

Ein 2-dimensionaler Untervektorraum kann durch zwei linear unabhängige Vektoren aus V bestimmt werden. Daher ist eine Gerade L durch zwei Punkte mit verschiedenen homogenen Koordinaten eindeutig bestimmt, was unmittelbar dem ersten Axiom einer synthetischen projektiven Geometrie entspricht.

Der Zusammenhang zwischen den beiden Definitionen projektiver Geometrien wurde von Veblen und Bussy in 1906 [VB06] herausgearbeitet (auch [BR04, S. 54f]). Sie zeigen, dass alle analytische projektive Geometrien $\mathrm{PG}(d, p^k)$ für eine Primzahlpotenz p^k der synthetischen Definition genügen und in diesen das Theorem von Desargues gilt. Weiter zeigen Sie, dass für gegebene Zahlen $n = p^k$ und Dimension $d > 2$ es genau eine endliche projektive Geometrie nämlich $\mathrm{PG}(d, n)$ gibt. Dies ist für $d = 2$ nicht richtig: es sind mehrere nicht-desarguesche projektive Ebenen bekannt. In dieser Ausarbeitung werden im Weiteren nur die analytischen projektiven Geometrien $\mathrm{PG}(d, n)$ verwendet.

Neben Punkten und Geraden kann man in projektiven Geometrien analog zur euklidischen Geometrie auch höhere Objekte wie Ebenen (durch drei Punkte bestimmt) und Hyperebenen (durch d Punkte bestimmt) betrachten, sofern dies für die Dimension d sinnvoll ist. Diese lassen sich bei der analytischen Definition über $V = \mathrm{GF}(n)^{d+1}$ direkt angeben: jeder 3-dimensionale Untervektorraum von V ist eine ***Ebene***, jeder $(d-1)$-dimensionale Untervektorraum heißt auch ***Sekundum*** und jeder d-dimensionale Untervektorraum heißt ***Primum*** oder auch ***Hyperebene*** von $\mathrm{PG}(d, n)$ [Hir79]. Allgemein heißt ein $(h+1)$-dimensionaler Untervektorraum von V ein ***h-Flach*** der Geometrie. Ein 1-Flach ist also eine Gerade und ein $(d-1)$-Flach eine Hyperebene.

Von diesen Objekten werden die Hyperebenen im Folgenden gesondert behandelt. Eine Hyperebene in V kann man wie in der euklidischen Geometrie als Lösungsmenge einer bestimmten linearen, nicht-trivialen Gleichung angeben. Zu vorgegebenen Koeffizienten $a_0, \ldots, a_d \in \mathrm{GF}(n)$, die nicht alle Null sind, ist die dazugehörige Hyperebene also

$$H_{(a_0,\ldots,a_d)} := \{(x_0, \ldots, x_d) \in \mathcal{P} \mid a_0 x_0 + \cdots + a_d x_d = 0\}$$

und so erhält man die Menge aller Hyperebenen als

$$\mathcal{H} := \{H_{(a_0,\ldots,a_d)} \mid (a_0, \ldots, a_d) \in \mathrm{GF}(n)^{d+1} \setminus \{0\}\}$$

Da der Schnitt von zwei verschiedenen Hyperebenen ein $(d-1)$-dimensionaler Untervektorraum ist, kann man ein Sekundum als die Punkte angeben, die beide Hyperebenengleichungen

erfüllen. Analog kann man kleinere Objekte durch mehr Gleichungen bestimmen: ein h-Flach ist die Lösungsmenge von $(d-h)$ verschiedenen nicht-trivialen linearen Gleichungen.

Im Fall einer projektiven Ebene $d = 2$ ist eine Hyperebene nichts andere als eine Gerade, daher kann man jede Gerade durch nur eine Hyperebenengleichung beschreiben.

Beispiel 1. Als Beispiel betrachte die projektive Geometrie $\mathrm{PG}(2,2)$ mit Dimension $d = 2$ und $n = 2^1$. Die Punktmenge besteht nach Konstruktion in der normalisierten Darstellung aus den Vektoren $\mathcal{P} = \{(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\} \subset \mathrm{GF}(2)^3$. Die Geraden werden durch folgende sieben Hyperebenengleichungen über $\mathcal{P}$ gebildet. $\mathrm{PG}(2,2)$ ist die kleinste projektive Ebene und heißt auch ***Fano-Ebene***.

Gleichung	Punkte auf der Geraden
$0x_0 + 0x_1 + 1x_2 = 0$	$(0,1,0),(1,0,0),(1,1,0)$
$0x_0 + 1x_1 + 0x_2 = 0$	$(0,0,1),(1,0,0),(1,0,1)$
$0x_0 + 1x_1 + 1x_2 = 0$	$(0,1,1),(1,0,0),(1,1,1)$
$1x_0 + 0x_1 + 0x_2 = 0$	$(0,0,1),(0,1,0),(0,1,1)$
$1x_0 + 0x_1 + 1x_2 = 0$	$(0,1,0),(1,0,1),(1,1,1)$
$1x_0 + 1x_1 + 0x_2 = 0$	$(0,0,1),(1,1,0),(1,1,1)$
$1x_0 + 1x_1 + 1x_2 = 0$	$(0,1,1),(1,0,1),(1,1,0)$

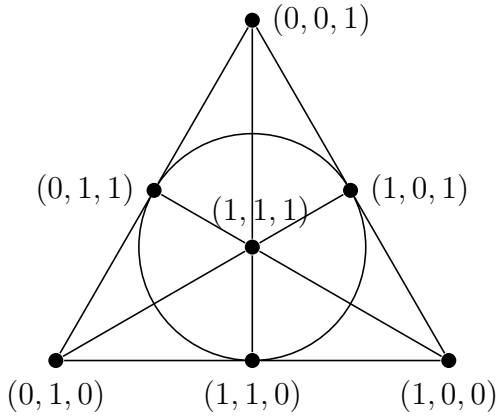


Abbildung 1: Konstruktion der Fano-Ebene $\mathrm{PG}(2,2)$

Um die Verbindung von endlichen Geometrien zur Design Theorie herzustellen, benötigen wir folgenden Satz, um die Objekte in $\mathrm{PG}(d,n)$ abzuzählen.

Satz 2. Ist $V = \mathrm{GF}(n)^d$ ein d-dimensionaler Vektorraum über dem endlichen Körper $\mathrm{GF}(n)$, dann enthält V für $0 \le k \le n$ genau $\begin{bmatrix} d \\ k \end{bmatrix}_n$ Untervektorräume der Dimension k, wobei

$$\begin{bmatrix} d \\ k \end{bmatrix}_n := \frac{(n^d-1)(n^{d-1}-1)\cdots(n^{d-k+1}-1)}{(n-1)(n^2-1)\cdots(n^k-1)} = \prod_{i=0}^{k-1} \frac{n^{d-i}-1}{n^{i+1}-1}$$

die ***Gauß-Binomial-Koeffizienten*** heißen.

Beweis. Ein k-dimensionaler Untervektorraum von V kann durch k linear unabhängige Vektoren $v_1, \ldots, v_k$ eindeutig bestimmt werden. Den ersten Vektor v_1 kann man aus allen $n^d - 1$ Vektoren ungleich Null wählen. Den zweiten v_2 nur noch aus $n^d - n$, da Null ausgeschlossen ist und die $n - 1$ Vielfachen von v_1 linear abhängig sind. Setzt man dies fort, gibt es für den Vektor v_i genau $n^d - n^{i-1}$ linear unabhängige Vektoren zur Wahl und so insgesamt $(n^d-1)(n^d-n)(n^d-n^2)\cdots(n^d-n^{k-1})$ verschiedene Arten k linear unabhängige Vektoren zu wählen.

Die k linear unabhängigen Vektoren erzeugen aber nicht jeweils verschiedene Untervektorräume, denn Vielfache von denselben Vektoren erzeugen den gleichen Raum. Daher muss man nun durch die Anzahl der möglichen Basen eines k-dimensionalen Untervektorraums teilen. Hierzu zählt man mit der gleichen Argumentation wie oben die Anzahl k linear unabhängiger Vektoren eines k-dimensionalen Vektorraums ab, also $(n^k-1)(n^k-n)\cdots(n^k-n^{k-1})$. Der Quotient der beiden Produkte ist die gesuchte Anzahl k-dimensionaler Untervektorräume von V. □

Satz 3. Sei eine projektive Geometrie $\mathrm{PG}(d,n)$ gegeben. Verwendet man die Punkte als Grundmenge $S=\mathcal{P}$ und die h-Flachs als Blöcke $\mathcal{B}$, so bilden diese ein [Sto06; BJL99]

$$\left(v=\begin{bmatrix} d+1 \\ 1 \end{bmatrix}_n,\ b=\begin{bmatrix} d+1 \\ h+1 \end{bmatrix}_n,\ r=\begin{bmatrix} d \\ h \end{bmatrix}_n,\ k=\begin{bmatrix} h+1 \\ 1 \end{bmatrix}_n,\ \lambda=\begin{bmatrix} d-1 \\ h-1 \end{bmatrix}_n\right)\text{-BIBD}$$

Da für alle Primzahlpotenzen $n=p^k$ und Dimensionen $d\geq 2$ jeweils eine $\mathrm{PG}(d,n)$ existiert, gibt es diese BIBD für alle solche Parameter und $h=1,\ldots,d$.

Beweis. Die 1-dimensionalen Untervektorräume von $V=\mathrm{GF}(n)^{d+1}$ sind die Punkte $\mathcal{P}=S$, also ist $v=|\mathcal{P}|=\begin{bmatrix} d+1 \\ 1 \end{bmatrix}_n$. Die h-Flachs sind die $(h+1)$-dimensionalen Untervektorräume von V, also ist $b=|\mathcal{B}|=\begin{bmatrix} d+1 \\ h+1 \end{bmatrix}_n$. Jedes h-Flach enthält als $(h+1)$-dimensionaler Vektorraum selbst $\begin{bmatrix} h+1 \\ 1 \end{bmatrix}_n$ Untervektorräume der Dimension 1, also ebenso viele Punkte aus $\mathcal{P}$ und so ist $k=\begin{bmatrix} h+1 \\ 1 \end{bmatrix}_n$. Für Parameter r betrachtet man einen beliebigen Punkt v_1, also einen 1-dimensionalen Untervektorraum von V bestimmt durch v_1. Dieser lässt sich durch Hinzunahme von h weiteren linear unabhängigen Vektoren zu einem $(h+1)$-dimensionalen Untervektorraum erweitern, also zu einem h-Flach. Diese h linear unabhängigen Vektoren können frei aus dem d-dimensionalen Quotientenraum $V\,/\,\langle v_1\rangle$ gewählt werden. Ein Punkt v_1 ist damit in genau $r=\begin{bmatrix} d \\ h \end{bmatrix}_n$ verschiedenen h-Flachs enthalten.

Analog berechnet man λ. Seien v_1 und v_2 zwei verschiedene Punkte, dann erweitert man den 2-dimensionalen Untervektorraum $\langle v_1,v_2\rangle$ durch $(h-1)$ linear unabhängige Vektoren aus dem $(d-1)$-dimensionalen Quotientenraum $V/\langle v_1,v_2\rangle$ zu einem $(h+1)$-dimensionalen Untervektorraum. Zwei verschiedene Punkte v_1 und v_2 sind also in genau $\lambda=\begin{bmatrix} d-1 \\ h-1 \end{bmatrix}_n$ h-Flachs enthalten. □

Korollar 4. Für $h=d-1$ folgt aus Satz 3 die Existenz der symmetrischen

$$\left(v=\frac{n^{d+1}-1}{n-1},\ b=\frac{n^{d+1}-1}{n-1},\ r=\frac{n^d-1}{n-1},\ k=\frac{n^d-1}{n-1},\ \lambda=\frac{n^{d-1}-1}{n-1}\right)\text{-BIBD}$$

Beweis. $\begin{bmatrix} d+1 \\ 1 \end{bmatrix}_n=\begin{bmatrix} d+1 \\ d \end{bmatrix}_n=\frac{n^{d+1}-1}{n-1}$, $\begin{bmatrix} d \\ d-1 \end{bmatrix}_n=\frac{n^d-1}{n-1}$, $\begin{bmatrix} d-1 \\ d-2 \end{bmatrix}_n=\frac{n^{d-1}-1}{n-1}$. □

5 Kollineationen und der Satz von Singer

Ziel ist es nun eine einfachere Konstruktionsweise für $\mathrm{PG}(d,n)$ und gleichzeitig für eine ganze Reihe von BIBDs zu entwickeln. Für die weitere Untersuchung wird die Übertragung des Isomorphismusbegriffs auf Geometrien benötigt.

Definition 7. Eine ***Kollineation*** ist eine Abbildung $f:\mathcal{G}\to\mathcal{G}'$ zwischen zwei projektiven Geometrien $\mathcal{G}=(\mathcal{P},\mathcal{L},\mathcal{I})$ und $\mathcal{G}'=(\mathcal{P}',\mathcal{L}',\mathcal{I}')$, so dass

(i) die Komponentenabbildungen $f:\mathcal{P}\to\mathcal{P}'$ auf den Punkten und $f:\mathcal{L}\to\mathcal{L}'$ auf den Geraden beide bijektiv sind und

(ii) diese die Inzidenzrelation erhalten: $(a,L)\in\mathcal{I}$ genau dann, wenn $(f(a),f(L))\in\mathcal{I}'$.

Definition 8. Eine Kollineation zwischen derselben projektiven Geometrie heißt auch ein ***Automorphismus***. Die Automorphismen einer endlichen projektiven Geometrie bilden mit der Komposition eine endliche Gruppe, die auch ***Kollineationsgruppe*** genannt wird.

Wir bemerken hier ohne Beweis, dass eine Kollineation h-Flachs auf h-Flachs abbildet, also insbesondere Geraden auf Geraden und Hyperebenen auf Hyperebenen.

Definition 9. Die ***Periode*** einer Kollineation $f : \mathcal{G} \to \mathcal{G}$ ist die Ordnung von f in der Kollineationsgruppe, also ist die kleinste Zahl q, für die $f^q = \mathrm{id}_{\mathcal{G}}$.

Beispiel 2. Sei $\mathcal{G} = \mathrm{PG}(2,2)$ die Fano-Ebene. Betrachte die Abbildung $f : \mathcal{G} \to \mathcal{G}$, welche durch $f : \mathcal{P} \to \mathcal{P}$, $(x_0, x_1, x_2) \mapsto (x_1, x_2, x_0)$ und ebenso auf den Punktmengen der Geraden definiert ist. Durch die Fortsetzung derselben Abbildung auf die Punktmengen der Geraden ist f eine Kollineation von $\mathcal{G}$ mit Periode 3. Anschaulich verschiebt diese Abbildung die Koordinatenvektoren zyklisch eine Komponente nach links, wodurch die Koordinaten der Fano-Ebene in Abbildung 1 einmal im Uhrzeigersinn mit Periode drei gedreht werden.

Satz 5. Jede bijektive lineare Abbildung auf $\mathrm{GF}(n^{d+1})$ induziert eine Kollineation auf $\mathrm{PG}(d,n)$.

Beweis. Sei $f : \mathrm{GF}(n^{d+1}) \to \mathrm{GF}(n^{d+1})$ ein bijektive lineare Abbildung, also ein Vektorraum-Isomorphismus. Als Isomorphismus von $\mathrm{GF}(n^{d+1})$ bildet f linear unabhängige Vektormengen auf linear unabhängige Vektormengen ab, also auch jeden k-dimensionalen Untervektorraum auf einen k-dimensionalen Untervektorraum isomorph ab. Insbesondere also die 1- und 2-dimensionalen, welche die Punkte und Geraden von $\mathrm{PG}(d,n)$ sind. Die Inzidenzrelation wird dadurch erhalten, dass die Geraden und die darin enthaltene Punkte von derselben Funktion f abgebildet werden. □

Nach diesen Vorbetrachtungen von Automorphismen auf projektiven Geometrien kommen wir nun zu dem zentralen Satz dieser Ausarbeitung, der 1938 von James Singer [Sin38] gezeigt wurde.

Satz 6 (Singer)**.** Es gibt in jeder analytischen projektiven Geometrie $\mathrm{PG}(d,n)$ mit $n = p^k$ eine Kollineation mit Periode $q = \frac{n^{d+1}-1}{n-1} = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_n$.

Der Beweis zu diesem Satz verlangt einige Grundlagen aus der Algebra endlicher Körper. In folgendem Satz sind alle wesentlichen Aussagen einschlägiger Lehrbücher (z.B. [Bos04, S. 127]) zusammengefasst.

Satz 7 (Struktursatz für endliche Körper)**.**

(i) Ist p eine Primzahl, dann existiert zu jedem $k \in \mathbb{N}_1$ ein Körper $\mathrm{GF}(p^k) := \mathbb{F}_{p^k}$ mit p^k Elementen. Dieser ist Erweiterungskörper von $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

(ii) Der Körper $\mathbb{F}_{p^k}$ ist bis auf Isomorphie eindeutig als Zerfällungskörper des Polynoms $X^{p^k} - X \in \mathbb{F}_p[X]$ charakterisiert und besteht gerade aus den p^k Nullstellen von $X^{p^k} - X$.

(iii) Ist $f \in \mathbb{F}_p[X]$ ein irreduzibles Polynom mit $\mathrm{Grad}(f) = k$, dann ist $\mathbb{F}_{p^k} \cong \mathbb{F}_p[X]/(f)$. Jede Nullstelle x von f in $\mathbb{F}_{p^k}$ ist primitives Element der Körpererweiterung $\mathbb{F}_{p^k} \supset \mathbb{F}_p$.

(iv) Die multiplikative Gruppe $\mathbb{F}_{p^k}^* := (\mathbb{F}_{p^k} \setminus \{0\}, \cdot)$ eines endlichen Körpers ist zyklisch von der Ordnung $p^k - 1$.

Wir verweisen auf die Beweise in den Lehrbüchern und verwenden im Folgenden wieder die Schreibweise $\mathrm{GF}(n)$ statt $\mathbb{F}_n$. Mit diesen Aussagen lässt sich nun eine Kollineation mit Periode $q = \frac{n^{d+1}-1}{n-1}$ konstruieren.

Beweis zu Satz 6 (nach [Sin38] und [Wal07, S. 79-81]).

Seien $n = p^k$ und $d \in \mathbb{N}_1$ die Parameter der analytischen projektiven Geometrie $\mathrm{PG}(d, n)$.

Der Beweis dieses Satzes ist sehr lang und lässt sich in drei Teile untergliedern. Im ersten Teil wird eine Projektion von $\mathrm{GF}(n^{d+1})^*$ auf die Punkte von $\mathrm{PG}(d, n)$ bestimmt. Diese ist nicht injektiv, daher werden im zweiten Teil die Mehrfachzuordnungen dieser Projektion untersucht. Im dritten Teil wird dann die gesuchte Kollineation als Abbildung konstruiert und deren Eigenschaften nach Definition 7 überprüft.

Teil 1: Konstruktion der Projektion $\mathrm{GF}(n^{d+1})^* \to \mathcal{P}$

Betrachte den endlichen Körper $\mathrm{GF}(n^{d+1}) = \mathrm{GF}(p^{k^{d+1}})$. Dieser lässt sich nach Satz 4 (iii) mit einem irreduziblen Polynom $f \in \mathrm{GF}(n)[X]$ von Grad $d+1$ durch Quotientenbildung konstruieren: $\mathrm{GF}(n^{d+1}) \cong \mathrm{GF}(n)[X]/(f)$. $\mathrm{GF}(n) = \mathrm{GF}(p^k)$ wiederum kann über $\mathrm{GF}(p)$ durch Quotientenbildung erzeugt werden. $\mathrm{GF}(n^{d+1})$ entspricht also einer zweimaligen Anwendung der Konstruktion in Satz 7 (iii). Für die weitere Untersuchung sei das irreduzible Polynom

$$f = c_0 + c_1 X + \cdots + c_d X^d + X^{d+1} \in \mathrm{GF}(n)[X] \tag{1}$$

Jedes irreduzible Polynom ist normiert und es gilt $c_0 \neq 0$, da sonst X ein Teiler von f wäre.

Sei $\lambda \in \mathrm{GF}(n^{d+1})$ eine Nullstelle des Polynoms f, dann ist λ primitives Element der Körpererweiterung und als solches erzeugt es alle Elemente der multiplikativen Gruppe $\mathrm{GF}(n^{d+1})^*$. Da $\mathrm{GF}(n^{d+1})^* = \mathrm{GF}(n^{d+1}) \setminus \{0\}$ und zyklisch von Ordnung $n^{d+1} - 1$ ist, kann man also schreiben

$$\mathrm{GF}(n^{d+1}) = \{0, \lambda^0, \lambda^1, \ldots, \lambda^{n^{d+1}-2}\}$$

Da $f(\lambda) = 0$ vorausgesetzt ist, folgt mit (1) durch Umformung

$$\lambda^{d+1} = -c_0 - c_1\lambda - \cdots - c_d\lambda^d \tag{2}$$

Mit dieser Gleichung kann man aber jede Potenz λ^i mit $i \geq d+1$ durch $\lambda^i = \lambda^{d+1}\lambda^{i-(d+1)}$ reduzieren und damit jedes λ^i mit $i \geq 0$ als Linearkombination

$$\lambda^i = \alpha_{i,0} + \alpha_{i,1}\lambda + \cdots + \alpha_{i,d}\lambda^d \tag{3}$$

darstellen mit $\alpha_{i,j} \in \mathrm{GF}(n)$. Für die ersten $i = 1, \ldots, d$ ist einfach $\alpha_{i,i} = 1$ und $\alpha_{i,j} = 0$ für $j \neq i$. Für höhere Potenzen reduziert man λ^i durch die Gleichung 2.

So kann jeder Potenz λ^i ein Vektor $(\alpha_{i,0}, \ldots, \alpha_{i,d}) \in \mathrm{GF}(n)^{d+1}$ zuordnen werden. Wir nennen

$$\pi : \mathrm{GF}(n^{d+1})^* \to \mathrm{GF}(n)^{d+1} \setminus \{0\}, \quad \lambda^i \mapsto (\alpha_{i,0}, \ldots, \alpha_{i,d})$$

Umkehrt kann man jedem Vektor $(\alpha_{i,0}, \ldots, \alpha_{i,d}) \in \mathrm{GF}(n)^{d+1}$ außer dem Nullvektor durch (3) eine Potenz $\lambda^i \in \mathrm{GF}(n^{d+1})^*$ zuordnen, da sich jedes Element als solche Potenz darstellen lässt. Der Nullvektor kann nicht repräsentiert werden, da $\lambda^i \neq 0$ für alle i. Diese Zuordnungen sind offensichtlich durch (2) und (3) invers zueinander, π ist also bijektiv. Insbesondere gibt es $n^{d+1} - 1$ verschiedene Vektoren in $\mathrm{GF}(n)^{d+1} \setminus \{0\}$ und ebenso existieren $n^{d+1} - 1$ verschiedene Potenzen λ^i in $\mathrm{GF}(n^{d+1})^*$.

Nach Konstruktion von $\mathrm{PG}(d, n)$ entspricht die Punktmenge $\mathcal{P} = (\mathrm{GF}(n)^{d+1} \setminus \{0\}) / \sim$ mit der Äquivalenzrelation $\sim$, die Vielfache von Vektoren gleich setzt. Man kann also die Potenzen λ^i, nach Darstellung als Vektoren über $\mathrm{GF}(n)$, durch Identifikation von Vektor-Vielfachen als Punkte der $\mathrm{PG}(d, n)$ betrachtet.

Ordnet man nun noch jeder natürlichen Zahl $i \in \mathbb{N}_0$ eine Potenz λ^i zu, so ergeben die drei Zuordnungen folgende Abbildungskette.

$$\begin{array}{ccccccc} \mathbb{N}_0 & \longrightarrow & \mathrm{GF}(n^{d+1})^* & \overset{\pi}{\longleftrightarrow} & \mathrm{GF}(n)^{d+1} \setminus \{0\} & \longrightarrow & \left((\mathrm{GF}(n)^{d+1} \setminus \{0\}) \,/\, \sim\right) = \mathcal{P} \\ i & \longmapsto & \lambda^i & \longmapsto & (\alpha_{i,0}, \ldots, \alpha_{i,d}) & \longmapsto & (\alpha_{i,0}, \ldots, \alpha_{i,d}) \,/\, \sim \end{array}$$

Insgesamt kann man also einer natürlichen Zahl i, durch den homogenen Koordinatenvektor $(\alpha_{i,0}, \ldots, \alpha_{i,d}) \,/\, \sim$ von λ^i einen Punkt der projektiven Geometrie zuordnen.

Teil 2: Mehrfachzuordnungen der Projektion $\mathrm{GF}(n^{d+1})^* \to \mathcal{P}$

Betrachte nun die Mehrfachzuordnungen bezüglich der Äquivalenzrelation $\sim$ in der dritten Abbildung. Hierfür sei $q = \frac{n^{d+1}-1}{n-1} = n^d + n^{d-1} + \cdots + 1$ die Periode aus der Voraussetzung.

Behauptung: $(\lambda^{sq})^n = \lambda^{sq}$ für alle $s \in \mathbb{N}_0$.

$$\begin{aligned} (\lambda^{sq})^n = (\lambda^{nq})^s = (\lambda^{n(n^d+n^{d-1}+\cdots+1)})^s \\ = (\lambda^{n^{d+1}+n^d+\cdots+n})^s = (\lambda^{n^{d+1}} \lambda^{n^d} \cdots \lambda^n)^s = (\lambda^1 \lambda^{n^d} \cdots \lambda^n)^s = (\lambda^q)^s \end{aligned}$$

Damit sind $0, 1, \lambda^q, \lambda^{2q}, \ldots, \lambda^{(n-2)q}$ die n verschiedenen Nullstellen des Polynoms $Y^n - Y$. Nach dem Struktursatz für endliche Körper, Satz 7 (ii), bilden diese Elemente einen Körper $\mathrm{GF}(n)$ mit den Rechenoperationen von $\mathrm{GF}(n^{d+1})$. Dieser Teilkörper $\mathrm{GF}(n) \subset \mathrm{GF}(n^{d+1}) = \mathrm{GF}(n)[X]/(f)$ ist aber gleichzeitig der Grundkörper und daraus folgt insbesondere, dass $\lambda^{sq} \in \mathrm{GF}(n)$ für jedes $s \in \mathbb{N}_0$ ist. Man beachte, dass im Allgemeinen nur $\lambda^i \in \mathrm{GF}(n^{d+1})$ gilt.

Weiter gilt für jedes $s \in \mathbb{N}_0$

$$\lambda^{i+sq} = \lambda^i \lambda^{sq} = (\lambda^{sq} \alpha_{i,0}) + (\lambda^{sq} \alpha_{i,1})\lambda + \cdots + (\lambda^{sq} \alpha_{i,d})\lambda^d$$

Aus dieser Gleichung folgt, dass der zu λ^{i+sq} gehörige Vektor gerade $(\lambda^{sq}\alpha_{i,0}, \ldots, \lambda^{sq}\alpha_{i,d})$ ist, denn λ^{sq} ist im Teilkörper $\mathrm{GF}(n)$ enthalten und kann daher als Teil der Koeffizienten gelten. Dieser Vektor ist aber ein Vielfaches von $(\alpha_{i,0}, \ldots, \alpha_{i,d})$, welcher bereits λ^i entspricht. Damit folgt, dass λ^i und λ^{i+sq} in $\mathrm{PG}(d, n)$ derselbe Punkt sind. Allgemeiner sind λ^i und λ^j genau dann derselbe Punkt, wenn $i \equiv j \bmod (q)$ und wir schreiben im Folgenden hierfür schlicht $\lambda^i \equiv \lambda^j$.

Man kann also die q Punkte der $\mathrm{PG}(d, n)$ mit den ersten q Potenzen λ^i für $i = 0, \ldots, q-1$ identifizieren. Weiter werden im Folgenden zur besseren Darstellung gelegentlich auch die Zahlen $i = 0, \ldots, q-1$ durch die Potenz λ^i mit den entsprechenden eindeutig bestimmten Punkten in $\mathrm{PG}(d, n)$ identifiziert.

Teil 3: Konstruktion der Kollineation

Als dritten Schritt dieser Konstruktion erhält man nun eine Kollineation mit Periode q: diese ist schlicht die Multiplikation mit λ, also die Abbildung $\varphi : \mathrm{GF}(n^{d+1})^* \to \mathrm{GF}(n^{d+1})^*$, $\lambda^i \mapsto \lambda^{i+1}$.

Die Abbildung φ ist bijektiv, da sie eine einfache Multiplikation mit λ ist und $(\mathrm{GF}(n^{d+1})^*, \cdot)$ zyklisch ist. Weiter bildet φ offensichtlich die Punkte von $\mathrm{PG}(d, n)$ bijektiv ab, denn diese entsprechen gerade den ersten q Potenzen λ^i und $\lambda^q \equiv \lambda^0$. Die Abbildung φ ist auf den Punkten nach Konstruktion zyklisch mit Periode q, da $\lambda^{i+q} \equiv \lambda^i$.

Sei $\overline{\varphi} = \pi \circ \varphi \circ \pi^{-1}$, also die Abbildung φ auf den Vektordarstellungen der Potenzen, so ist $\overline{\varphi}$ als Komposition von bijektiven Abbildungen selber bijektiv.

Bleibt zu zeigen, dass φ in $\mathrm{PG}(d, n)$ alle Punkte einer Geraden auf die Punkte einer bestimmten anderen Geraden abbildet.

Betrachte dazu wie φ auf der Vektordarstellung $(\alpha_{i,0}, \ldots, \alpha_{i,d})$ von λ^i operiert

$$\begin{aligned}\varphi(\lambda^i) = \lambda^{i+1} = \lambda\,\lambda^i &\overset{(3)}{=} \lambda(\alpha_{i,0} + \alpha_{i,1}\lambda + \cdots + \alpha_{i,d-1}\lambda^{d-1} + \alpha_{i,d}\lambda^d) \\ &= \alpha_{i,0}\lambda + \alpha_{i,1}\lambda^2 + \cdots + \alpha_{i,d-1}\lambda^d + \alpha_{i,d}\lambda^{d+1} \\ &\overset{(2)}{=} \alpha_{i,0}\lambda + \alpha_{i,1}\lambda^2 + \cdots + \alpha_{i,d-1}\lambda^d + \alpha_{i,d}(-c_0 - c_1\lambda - \cdots - c_d\lambda^d) \\ &= -c_0\alpha_{i,d} + (\alpha_{i,0} - c_1\alpha_{i,d})\lambda + \cdots + (\alpha_{i,d-1} - c_d\alpha_{i,d})\lambda^d\end{aligned}$$

Für einen Vektor $(x_0, \ldots, x_d) \in \mathrm{GF}(n)^{d+1} \setminus \{0\}$ der $\mathrm{PG}(d, n)$ entspricht φ also der Abbildung

$$\overline{\varphi}(x_0, \ldots, x_d) = (-c_0 x_d,\ x_0 - c_1 x_d,\ \ldots,\ x_{d-1} - c_d x_d) \tag{4}$$

Weiter ist $\overline{\varphi}$ eine lineare Abbildung, denn für alle $(x_0, \ldots, x_d), (y_0, \ldots, y_d) \in \mathrm{GF}(n)^{d+1} \setminus \{0\}$ und $\mu, \nu \in \mathrm{GF}(n)$ ist

$$\begin{aligned}&\overline{\varphi}(\mu(x_0, \ldots, x_d) + \nu(y_0, \ldots, y_d)) = \overline{\varphi}(\mu x_0 + \nu y_0, \ldots, \mu x_d + \nu y_d) \\ &\quad= (-c_0[\mu x_d + \nu y_d],\ [\mu x_0 + \nu y_0] - c_1[\mu x_d + \nu y_d], \ldots, [\mu x_{d-1} + \nu y_{d-1}] - c_d[\mu x_d + \nu y_d]) \\ &\quad= (\mu(-c_0 x_d) + \nu(-c_0 y_d),\ \mu(x_0 - c_1 x_d) + \nu(y_0 - c_1 y_d), \ldots, \mu(x_{d-1} - c_d x_d) + \nu(y_{d-1} - c_d y_d)) \\ &\quad= \mu\overline{\varphi}(x_0, \ldots, x_d) + \nu\overline{\varphi}(y_0, \ldots, y_d)\end{aligned}$$

Nach Satz 5 induziert $\overline{\varphi}$ eine Kollineation $\widetilde{\varphi}$ von $\mathrm{PG}(d, n)$, da $\overline{\varphi}$ eine lineare, bijektive Abbildung also ein Vektorraum-Isomorphismus ist. Die Kollineation $\widetilde{\varphi}$ hat nach Konstruktion Periode q auf $\mathrm{PG}(d, n)$. □

Das Ergebnis des Satzes von Singer kann verwendet werden, um alle Hyperebenen von $\mathrm{PG}(d, n)$ zu konstruieren. Hierzu muss man die Punkte der Geometrie als Potenzen λ^i ausdrücken, wodurch die Kollineation φ einfach der Erhöhung der Potenz um eins entspricht. Um alle Hyperebene der Geometrie zu erzeugen, braucht man in dieser Darstellung nur eine initiale Hyperebene bestimmen, etwa durch eine nicht-triviale lineare Gleichung oder durch d linear unabhängiger Punkte. Die Kollineation mit Periode $q = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_n = \begin{bmatrix} d+1 \\ d \end{bmatrix}_n$ liefert dann alle anderen Hyperebenen schlicht durch Erhöhung der Potenzordnung. Siehe hierzu auch die Konstruktion von $\mathrm{PG}(2, 3)$ in Beispiel 4 oder $\mathrm{PG}(3, 2)$ im Anhang A.

6 Konstruktion von PG(2, n) mittels Differenzenmengen

Im letzten Abschnitt wurde der Satz von Singer beweisen, der in jeder projektiven Geometrie $\mathrm{PG}(d, n)$ eine Kollineation mit Periode $q = \frac{n^{d+1}-1}{n-1}$ liefert. Durch die Kollineation ist gleichzeitig ein praktisches Konstruktionsverfahren gegeben, das wir nun genauer für den Spezialfall $d = 2$, also für projektive *Ebenen* $\mathrm{PG}(2, n)$, betrachten wollen, da hier die Hyperebenen genau die Geraden der Geometrie sind. Hierbei verwenden wir die im Beweis von Satz von Singer eingeführten Bezeichnungen für das primitive Element λ und die Kollineation φ weiter.

Die Grundidee des oben vorgestellten allgemeinen Konstruktionsverfahrens ist für projektive Ebenen folgende: Es gibt $v = \begin{bmatrix} 3 \\ 1 \end{bmatrix}_n = \frac{n^3-1}{n-1} = n^2 + n + 1$ verschiedene Potenzen und ebenso viele Punkte in der projektiven Ebene. Jede Gerade der projektiven Ebene enthält genau $r := \frac{n^2-1}{n-1} = n + 1$ Punkte (Satz 3). Hat man die r Punkte irgendeiner Gerade als Potenzen von λ gegeben, so kann man durch $(q-1)$-malige Anwendung der Kollineation φ alle $q = \frac{n^3-1}{n-1} = n^2 + n + 1$ verschiedenen Geraden der projektiven Ebene bestimmten.

Wir untersuchen diese Idee genauer: sind durch r Potenzen $\lambda^{i_0}, \ldots, \lambda^{i_{r-1}}$ ebenso viele Punkte vorgegeben, wobei wir $i_0 = 0$ und $i_1 = 1$ voraussetzen dürfen, dann ergibt $(q-1)$-malige

Anwendung der Kollineation folgende Matrix von Punkten, wobei wir hier statt der Potenz λ^i schlicht i schreiben.

$$\begin{array}{ccccccc} i_0 & i_0+1 & i_0+2 & \cdots & i_0+(q-2) & i_0+(q-1) \\ i_1 & i_1+1 & i_1+2 & \cdots & i_1+(q-2) & i_1+(q-1) \\ i_2 & i_2+1 & i_2+2 & \cdots & i_2+(q-2) & i_2+(q-1) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ i_{r-1} & i_{r-1}+1 & i_{r-1}+2 & \cdots & i_{r-1}+(q-2) & i_{r-1}+(q-1) \end{array} \tag{5}$$

Da $\lambda^{i+q} \equiv \lambda^i$, muss man obige Matrix modulo q betrachten und so enthält jede Zeile genau alle q Punkte. In dieser Darstellung entspricht jede Spalte der Matrix potenziell der Punktmenge einer Geraden. Damit jedoch die durch diese Spalten definierten Geraden den Axiomen einer projektiven Geometrie genügen, müssen die *Initialwerte* besondere Eigenschaften haben. Als erste Bedingung müssen die r Anfangswerte $i_0, \ldots, i_{r-1}$ alle verschieden sein.

Nach dem ersten Axiom projektiver Geometrien sind zwei Geraden gleich, falls sie zwei verschiedene Punkte gemeinsam haben. Hieraus folgt unmittelbar für die obige Matrix, dass zwei verschiedene Spalten nur höchstens eine Zahl gemeinsam haben dürfen.

Durch diese Beobachtung und der zyklischen Struktur der Spalten folgt weiter, dass die erste Spalte höchstens ein Paar aufeinanderfolgender Zahlen enthalten kann. Ohne Beschränkung der Allgemeinheit sind dies bereits die vorgegeben $i_0 = 0$ und $i_1 = 1$. Denn wären $i_a = a$ und $a+1$ zwei weitere Werte der ersten Spalte, so würden durch die Kollineation die Zahlen $i_0 + 1 = 1$ und $i_a + 1 = a + 1$ in der zweiten Spalte stehen. Da aber zwei Spalten höchstens eine Zahl gemeinsam haben dürfen, folgt dass die erste und damit jede Spalte höchstens ein Paar aufeinanderfolgender Zahlen enthalten kann.

Aus der letzten Bedingung folgt dann aber, dass alle Spalten paarweise verschieden sein müssen. Denn wären $j \neq k$ zwei gleiche Spalten, dann betrachte die ersten beiden Zeilen dieser Spalten: wäre $i_0 + j \equiv i_\alpha + k \bmod (q)$ und $i_1 + j \equiv i_\beta + k \bmod (q)$, so folgt durch Subtraktion $i_\alpha - i_\beta \equiv i_1 = 1 \bmod (q)$. Da $i_\alpha = j - k \not\equiv 0 \bmod (q)$, wären dann aber i_α und i_β zwei weitere aufeinanderfolgende Zahlen in der ersten Spalte.

Damit sind alle q Spalten paarweise verschieden und enthalten paarweise höchstens ein gemeinsames Element. Die gesamte Matrix entspricht daher einer Darstellung der Geraden von $\mathrm{PG}(d, n)$.

Betrachte man nun nur die Spalten der Matrix, die das Element $0 = i_0$ enthalten. Diese entsprechen allen Geraden, die den Punkt 0 enthalten, und die Matrix lässt sich durch Umordnen auf die folgende Form bringen.

$$\begin{array}{ccccccc} i_0 - i_0 & i_0 - i_1 & i_0 - i_2 & \cdots & i_0 - i_{r-1} \\ i_1 - i_0 & i_1 - i_1 & i_1 - i_2 & \cdots & i_1 - i_{r-1} \\ i_2 - i_0 & i_1 - i_1 & i_1 - i_2 & \cdots & i_1 - i_{r-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ i_{r-1} - i_0 & i_{r-1} - i_1 & i_{r-1} - i_2 & \cdots & i_{r-1} - i_{r-1} \end{array} \tag{6}$$

Diese $(r \times r)$-Matrix hat in der Diagonalen Nullen und die übrigen $r(r-1)$ Elemente sind alle verschieden, da je zwei Spalten höchstens eine gemeinsame Zahl enthalten. Es gibt also $r(r-1) = n^2 + n$ verschiedene Elemente ungleich Null in obiger Matrix. Da die Elemente aber nur aus den $q = n^2 + n + 1$ verschiedenen Potenzen von λ gewählt werden können, muss jedes dieser Elemente genau einmal vorkommen.

Da aber für jede Primzahlpotenz $n = p^k$ alle den Punkt 0 enthaltende Geraden der $\mathrm{PG}(2, n)$ in einer solchen Matrix angeordnet werden können und eben obige Eigenschaften haben, existiert für n immer eine solche Matrix.

Singer hat 1938 diesen Umstand in folgendem zahlentheoretischen Satz fest gehalten:

Satz 8. Ist $n = p^k$ eine Primzahlpotenz, dann gibt es $n+1$ natürliche Zahlen $d_0, \ldots, d_n$, so dass die n^2+n verschiedenen Differenzen $(d_i - d_j) \bmod (n)$ für $i \neq j$, $i, j = 0, \ldots, n$ kongruent zu den Zahlen $1, \ldots, n^2+n$ sind.

Er nannte diese Zahlen $d_0, \ldots, d_n$ eine ***perfekte Differenzenmenge*** der Ordnung $n+1$. Dies war Ausgangspunkt einer auf dem Gebiet der Design Theorie sehr ertragreichen Behandlung von Differenzenmengen (siehe z.B. [BJL99, S. 297-509]). Auf dieser Struktur basiert eine sehr ergiebige Konstruktionsmethode für balancierte unvollständige Block-Designs. Wir wollen mit folgender modernen Definition von Differenzenmengen weiter arbeiten.

Definition 10. Eine ***(v, k, λ)-Differenzenmenge*** ist eine Teilmenge $B \subset G$ mit $|B| = k$ aus einer abelschen Gruppe G mit $|G| = v$, so dass für jedes nicht-neutrale Elemente $g \in G$ es genau λ geordnete Paare $(x, y) \in B \times B$ gibt mit $x - y = g$. Jedes Element der Gruppe G kann also auf genau λ Arten als Differenz zweier Elemente von B dargestellt werden.

Eine perfekte Differenzenmenge ist also der Spezialfall einer $(n^2+n+1, n+1, 1)$-Differenzenmenge über $\mathbb{Z}_{n^2+n+1}$.

Ein allgemeineres Ergebnis erhält man, wenn man die Kollineation aus dem Satz von Singer als Verknüpfung auf $\mathbb{Z}_q$ verwendet:

Satz 9. Es gibt zu jeder Primzahlpotenz $n = p^k$ und natürlichen Zahl $d \geq 2$ eine

$$\left(\frac{n^{d+1}-1}{n-1}, \frac{n^d-1}{n-1}, \frac{n^{d-1}-1}{n-1} \right) \text{-Differenzenmenge}$$

Beweis. Für die Parameter n und d existiert eine projektive Geometrie $\mathrm{PG}(d, n)$ mit $q = \frac{n^{d+1}-1}{n-1}$ Punkten. Wir setzen $G = \{0, \ldots, q-1\}$ und identifizieren die Zahlen $i = 0, \ldots, q-1$ über die Konstruktion im Satz von Singer mit den Punkten λ^i der projektiven Geometrie. Zwei gegebenen Punkten λ^i und λ^j kann durch j-malige Anwendung der Kollineation auf λ^i ein neuer Punkt zugeordnet werden: dies ist genau $\varphi^j(\lambda^i) = \lambda^{i+j}$. Diese Verknüpfung auf den Potenzzahlen $0, \ldots, q-1$ entspricht genau der bekannten Addition, also ist $G \cong (\mathbb{Z}_q, +)$.

Betrachte nun eine beliebige Hyperebene H. Diese enthält nach Satz 2 genau $r = \begin{bmatrix} d \\ 1 \end{bmatrix}_n = \frac{n^d-1}{n-1}$ Punkte und wird durch d verschiedene linear unabhängige Punkte eindeutig bestimmt.

Seien λ^i und λ^j zwei Punkte der Geometrie, nimmt man $d-2$ weitere linear unabhängige Punkte hinzu, bestimmen die d Punkte eine Hyperebene. Diese $d-2$ Punkte können beliebig aus dem $(d-1)$-dimensionalen Untervektorraum $V/\langle \lambda^i, \lambda^j \rangle$ gewählt werden, also auf $\begin{bmatrix} d-1 \\ d-2 \end{bmatrix}_n = \begin{bmatrix} d-1 \\ 1 \end{bmatrix}_n = \frac{n^{d-1}-1}{n-1}$ Arten. Hieraus folgt, dass es $\frac{n^{d-1}-1}{n-1}$ verschiedene Hyperebenen gibt, die zwei bestimmte Punkte der Geometrie enthalten.

Behauptung: jede Hyperebene $H = \{i_0, \ldots, i_{r-1}\} \subset \mathbb{Z}_q$ ist eine (q, r, s)-Differenzenmenge.

Die Parameter q und r sind schon gezeigt. Sei $g \in \mathbb{Z}_q \setminus \{0\}$ ein nicht-neutrales Element, also ein Punkt λ^g, dann sind λ^g und λ^0 in genau $s = \frac{n^{d-1}-1}{n-1}$ verschiedenen Hyperebenen $E_0, \ldots, E_{s-1}$ enthalten. Diese s Hyperebenen werden durch die Kollineation aus H durch wiederholte Anwendung erzeugt und umgekehrt.

Es gibt also genau s Zahlen $j_0, \ldots, j_{s-1} \in \mathbb{Z}_q$, so dass $H = \varphi^{j_k}(E_k)$ für $k = 0, \ldots, s-1$. Da $g \in E_k$ und so $\varphi^{j_k}(\lambda^g) = \lambda^{g+j_k} \in H$, gibt es also ein eindeutiges Bild $\lambda^{g+j_k} =: \lambda^{i_{\sigma(k)}}$ von g in H zu jedem $k = 0, \ldots, s-1$. Damit gilt $i_{\sigma(k)} = g + j_k$, also $g = i_{\sigma(k)} - j_k$ für jede der s Hyperebenen E_k, $k = 0, \ldots, s-1$. Da $\lambda^0 \in E_k$ und so $\varphi^{j_k}(\lambda^0) = \lambda^{j_k} \in H$, ist auch $j_k \in H$ und damit ist g also auf genau s Arten als Differenz aus H darstellbar. □

Die Bedeutung von Differenzenmengen für die Design Theorie ist, dass sich aus diesen durch Entwicklung über der abelschen Gruppe leicht ein symmetrisches BIBD erzeugen lässt.

Satz 10. Ist $B \subset G$ eine (v, k, λ)-Differenzenmengen über einer endlichen abelschen Gruppe $(G, +)$, so gibt es ein

$$(v{=}|G|,\ b{=}v,\ r{=}k,\ k{=}|B|,\ \lambda)\text{-BIBD}$$

mit den Blöcken $\mathcal{B} = \{B + g \mid g \in G\}$.

Wir verzichten auf einen Beweis und entwickeln stattdessen folgendes Beispiel, das eine bereits bekannte Struktur neu erzeugt.

Beispiel 3. Sei $G = (\mathbb{Z}_7, +)$ und $B = \{1, 2, 4\}$, dann gibt es folgende Paare aus $(x, y) \in B \times B$:

$$\begin{array}{lll} 1-1=0 & 2-1=1 & 4-1=3 \\ 1-2=-1=6 & 2-2=0 & 4-2=2 \\ 1-4=-3=4 & 2-4=-2=5 & 4-4=0 \end{array}$$

Es kommt also jedes Element von $\mathbb{Z}_7$ außer der Null genau $\lambda = 1$ mal als Differenz vor. Damit ist B eine $(7, 3, 1)$-Differenzenmenge und lässt sich nach Satz 10 zu folgendem $(7, 7, 3, 3, 1)$-BIBD entwickeln:

$$\mathcal{B} = \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,0\},\{5,6,1\},\{6,0,2\},\{0,1,3\}\}$$

Dies ist die Fano-Ebene (Abbildung 1) als Block-Design entwickelt. Folgende Matrizen stellen die Geraden des Designs wie in (5) und (6) dar. In der zweiten quadratischen Matrix der Geraden durch 0, erkennt man die Zahlen von $1, \ldots, 6$ jeweils einmal aus der Differenzenmenge B entwickelt.

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \end{array} \qquad \begin{array}{ccc} 0 & 6 & 4 \\ 1 & 0 & 5 \\ 3 & 2 & 0 \end{array}$$

Beispiel 4. Als umfangreicheres Konstruktionsbeispiel betrachten wir $\mathrm{PG}(2, 3)$. Sei also $V = \mathrm{GF}(3)[X]/(f)$ mit dem irreduziblen Polynom $f = X^3 - X + 1$. Es gilt also $X^3 = X - 1 = X + 2$ in V. Ist λ eine beliebige Nullstelle von f, so kann man die Potenzen von λ durch das Polynom kürzen und erhält mit der Bijektion π folgende Tabelle von Zuordnungen von allen Potenzen zu deren Koordinaten von $\mathrm{GF}(n)^3 \setminus \{0\}$, von denen eine homogen ist.

$$\begin{array}{rcl} \lambda^0 = 1 & \overset{\pi}{\leftrightarrow} & (1,0,0) \equiv (2,0,0) \overset{\pi}{\leftrightarrow} 2 = \lambda^{13} \\ \lambda^1 = \lambda & \leftrightarrow & (0,1,0) \equiv (0,2,0) \leftrightarrow 2\lambda = \lambda^{14} \\ \lambda^2 = \lambda^2 & \leftrightarrow & (0,0,1) \equiv (0,0,2) \leftrightarrow 2\lambda^2 = \lambda^{15} \\ \lambda^3 = 2 + \lambda & \leftrightarrow & (2,1,0) \equiv (1,2,0) \leftrightarrow 1 + 2\lambda = \lambda^{16} \\ \lambda^4 = 2\lambda + \lambda^2 & \leftrightarrow & (0,2,1) \equiv (0,1,2) \leftrightarrow \lambda + 2\lambda^2 = \lambda^{17} \\ \lambda^5 = 2 + \lambda + 2\lambda^2 & \leftrightarrow & (2,1,2) \equiv (1,2,1) \leftrightarrow 1 + 2\lambda + \lambda^2 = \lambda^{18} \\ \lambda^6 = 1 + \lambda + \lambda^2 & \leftrightarrow & (1,1,1) \equiv (2,2,2) \leftrightarrow 2 + 2\lambda + 2\lambda^2 = \lambda^{19} \\ \lambda^7 = 2 + 2\lambda + \lambda^2 & \leftrightarrow & (2,2,1) \equiv (1,1,2) \leftrightarrow 1 + \lambda + 2\lambda^2 = \lambda^{20} \\ \lambda^8 = 2 + 2\lambda^2 & \leftrightarrow & (2,0,2) \equiv (1,0,1) \leftrightarrow 1 + \lambda^2 = \lambda^{21} \\ \lambda^9 = 1 + \lambda & \leftrightarrow & (1,1,0) \equiv (2,2,0) \leftrightarrow 2 + 2\lambda = \lambda^{22} \\ \lambda^{10} = \lambda + \lambda^2 & \leftrightarrow & (0,1,1) \equiv (0,2,2) \leftrightarrow 2\lambda + 2\lambda^2 = \lambda^{23} \\ \lambda^{11} = 2 + \lambda + \lambda^2 & \leftrightarrow & (2,1,1) \equiv (1,2,2) \leftrightarrow 1 + 2\lambda + 2\lambda^2 = \lambda^{24} \\ \lambda^{12} = 2 + \lambda^2 & \leftrightarrow & (2,0,1) \equiv (1,0,2) \leftrightarrow 1 + 2\lambda^2 = \lambda^{25} \end{array}$$

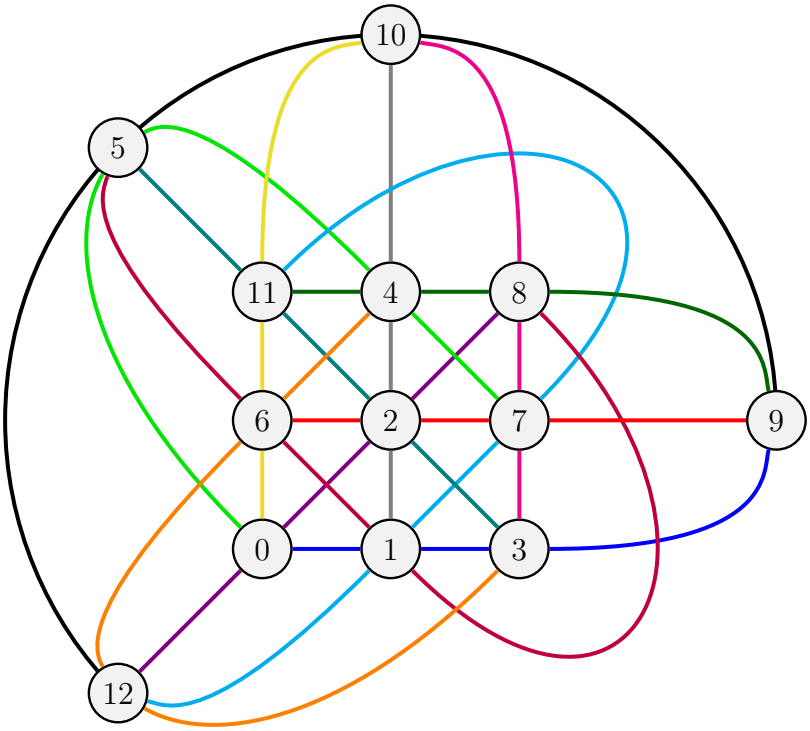


Abbildung 2: Zeichnung von PG(2, 3)

Verwendet man nun eine Differenzenmenge von $\mathbb{Z}_{13}$, beispielsweise $B = \{0, 1, 3, 9\}$, so kann man mit Satz 10 die Blöcke des Designs und äquivalent dazu die Geraden der projektiven Ebene erzeugen.

Alternativ dazu kann man eine beliebige Gerade konstruieren, die wegen $d = 2$ durch eine beliebige nicht-triviale lineare Hyperebenengleichung vollständig definiert ist. Beispielsweise ist die Lösungsmenge von $1x_0 + 0x_1 + 0x_2 = 0$ gerade $\{(0, 1, 0), (0, 0, 1), (0, 2, 1), (0, 1, 1)\}$, welche den Potenzen $\{\lambda^1, \lambda^2, \lambda^4, \lambda^{10}\}$ oder schlicht $\{1, 2, 4, 10\}$ entspricht.

Entwickelt man einen der Initialblöcke, so erhält man folgende Geraden- oder Blockmenge. In Abbildung 2 ist die durch die Potenzen von λ und folgenden Geraden erzeugte projektive Ebene graphisch dargestellt.

$$\mathcal{B} = \left\{ \begin{array}{ccccc} \{0,1,3,9\}, & \{1,2,4,10\}, & \{2,3,5,11\}, & \{3,4,6,12\}, & \{4,5,7,0\}, \\ \{5,6,8,1\}, & \{6,7,9,2\}, & \{7,8,10,3\}, & \{8,9,11,4\}, & \{9,10,12,5\}, \\ \{10,11,0,6\}, & \{11,12,1,7\}, & \{12,0,2,8\} & & \end{array} \right\}$$

Literatur

[ACDG06] Ian Anderson, Charles J. Colbourn, Jeffrey H. Dinitz und Terry S. Griggs. „Design Theory: Antiquity to 1950“. In: *Handbook of Combinatorial Designs*. Hrsg. von Charles J. Colbourn und Jeffrey H. Dinitz. 2nd Edition. Discrete Mathematics and Its Applications. Chapman & Hall/CRC, 2006. Kap. I.2, S. 11–22. ISBN: 0-8493-8948-8.

[Bal26] Walter W. Rouse Ball. „Kirkman's School-Girls Problem“. In: *Mathematical Recreations and Essays*. 10th Edition. MacMillan und Co., 1926. Kap. X, S. 193–223.

[BJL99] Thomas Beth, Dieter Jungnickel und Hanfried Lenz. *Design Theory, Volume 1*. 2nd Edition. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 1999. ISBN: 0-521-44432-2.

[Bos04] Siegfried Bosch. *Algebra*. Springer Berlin/Heidelberg, 2004. ISBN: 3-540-30488-4.

[BR04] Albrecht Beutelspacher und Ute Rosenbaum. *Projektive Geometrie: von den Grundlagen bis zu den Anwendungen*. 2. Auflage. Wiesbaden: Vieweg+Teuber Verlag, 2004. ISBN: 3-528-17241-X.

[Col06] Charles J. Colbourn. „Triple Systems“. In: *Handbook of Combinatorial Designs*. Hrsg. von Charles J. Colbourn und Jeffrey H. Dinitz. 2nd Edition. Discrete Mathematics and Its Applications. Chapman & Hall/CRC, 2006. Kap. II.2, S. 58–71. ISBN: 0-8493-8948-8.

[Hir79] James W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford mathematical monographs. Oxford: Clarendon Press, 1979. ISBN: 0-198-53526-0.

[Pol98] Burkard Polster. *A Geometrical Picture Book*. Universitext Series. Springer Berlin/Heidelberg, 1998. ISBN: 0-387-98437-2.

[Sin38] James Singer. „A Theorem in Finite Projective Geometry and Some Applications to Number Theory“. In: *Transactions of the American Mathematical Society* 43.3 (Mai 1938), S. 377–385. ISSN: 0002-9947.

[Sto06] Leo Storme. „Finite Geometry“. In: *Handbook of Combinatorial Designs*. Hrsg. von Charles J. Colbourn und Jeffrey H. Dinitz. 2nd Edition. Discrete Mathematics and Its Applications. Chapman & Hall/CRC, 2006. Kap. VII.2, S. 702–729. ISBN: 0-8493-8948-8.

[Swe08] Frank J. Swetz. *Legacy of the Luoshu: The 4,000 Year Search for the Meaning of the Magic Square of Order Three*. A.K. Peters, 2008. ISBN: 978-1568814278.

[VB06] Oswald Veblen und W. H. Bussey. „Finite Projective Geometries“. In: *Transactions of the American Mathematical Society* 7.2 (Apr. 1906), S. 241–259. ISSN: 0002-9947.

[VY10] Oswald Veblen und John Wesley Young. *Projective Geometry, Volume I*. Ginn And Company, 1910. ISBN: 978-1418167073.

[Wal07] Walter D. Wallis. *Introduction to Combinatorial Designs*. 2nd Edition. Chapman & Hall/CRC, 2007. ISBN: 978-1584888383.

A Konstruktion und Modelle von PG(3, 2)

In diesem Extrakapitel wird mit den in dieser Ausarbeitung entwickelten Methoden und Sätze die kleinste räumliche projektive Geometrie PG(3, 2) konstruiert und visualisiert.

Beispiel 5. Betrachte PG(3, 2) also $d = 3$, $n = 2$.

Aus Satz 2 erhält man für PG(3, 2) die folgenden Anzahl von Punkten $\mathcal{P}$, Geraden $\mathcal{L}$, Hyperebenen $\mathcal{H}$ und Punkte in einer beliebigen Geraden L:

$$|\mathcal{P}| = \begin{bmatrix}4\\1\end{bmatrix}_2 = 15 \qquad |\mathcal{L}| = \begin{bmatrix}4\\2\end{bmatrix}_2 = 35 \qquad |\mathcal{H}| = \begin{bmatrix}4\\3\end{bmatrix}_2 = 15 \qquad |L| = \begin{bmatrix}2\\1\end{bmatrix}_2 = 3$$

Sei $V := \mathrm{GF}(2)[X]/(f)$ mit dem irreduziblen Polynom $f = X^4 + X + 1$, also $X^4 = X + 1$, dann kann man die homogenen Koordinaten und Potenzen von λ folgendermaßen entwickeln:

$$\begin{array}{llll}
\lambda^0 = 1 & & & \overset{\pi}{\leftrightarrow} (1,0,0,0) \\
\lambda^1 = & \lambda & & \leftrightarrow (0,1,0,0) \\
\lambda^2 = & & \lambda^2 & \leftrightarrow (0,0,1,0) \\
\lambda^3 = & & & \lambda^3 \leftrightarrow (0,0,0,1) \\
\lambda^4 = 1 + \lambda & & & \leftrightarrow (1,1,0,0) \\
\lambda^5 = & \lambda + \lambda^2 & & \leftrightarrow (0,1,1,0) \\
\lambda^6 = & & \lambda^2 + \lambda^3 & \leftrightarrow (0,0,1,1) \\
\lambda^7 = 1 + \lambda & & + \lambda^3 & \leftrightarrow (1,1,0,1)
\end{array}
\qquad
\begin{array}{llll}
\lambda^8 = 1 & & + \lambda^2 & \overset{\pi}{\leftrightarrow} (1,0,1,0) \\
\lambda^9 = & \lambda & & + \lambda^3 \leftrightarrow (0,1,0,1) \\
\lambda^{10} = 1 + \lambda + \lambda^2 & & & \leftrightarrow (1,1,1,0) \\
\lambda^{11} = & \lambda + \lambda^2 & + \lambda^3 & \leftrightarrow (0,1,1,1) \\
\lambda^{12} = 1 + \lambda + \lambda^2 & & + \lambda^3 & \leftrightarrow (1,1,1,1) \\
\lambda^{13} = 1 & & + \lambda^2 + \lambda^3 & \leftrightarrow (1,0,1,1) \\
\lambda^{14} = 1 & & + \lambda^3 & \leftrightarrow (1,0,0,1)
\end{array}$$

Eine Gerade erhält man durch Auswahl zweier homogener Koordinaten und Hinzunahme ihrer einen Linearkombination.

$$\begin{array}{ll}
L_0 = \{(1,0,0,0),(0,1,0,0),(1,1,0,0)\} = \{\lambda^0,\lambda^1,\lambda^4\} & L_{18} = \{(0,0,0,1),(1,1,0,0),(1,1,0,1)\} = \{\lambda^3,\lambda^4,\lambda^7\} \\
L_1 = \{(1,0,0,0),(0,0,1,0),(1,0,1,0)\} = \{\lambda^0,\lambda^2,\lambda^8\} & L_{19} = \{(0,0,0,1),(0,1,1,0),(0,1,1,1)\} = \{\lambda^3,\lambda^5,\lambda^{11}\} \\
L_2 = \{(1,0,0,0),(0,0,0,1),(1,0,0,1)\} = \{\lambda^0,\lambda^3,\lambda^{14}\} & L_{20} = \{(0,0,0,1),(1,0,1,0),(1,0,1,1)\} = \{\lambda^3,\lambda^8,\lambda^{13}\} \\
L_3 = \{(1,0,0,0),(0,1,1,0),(1,1,1,0)\} = \{\lambda^0,\lambda^5,\lambda^{10}\} & L_{21} = \{(0,0,0,1),(1,1,1,0),(1,1,1,1)\} = \{\lambda^3,\lambda^{10},\lambda^{12}\} \\
L_4 = \{(1,0,0,0),(0,0,1,1),(1,0,1,1)\} = \{\lambda^0,\lambda^6,\lambda^{13}\} & L_{22} = \{(1,1,0,0),(0,1,1,0),(1,0,1,0)\} = \{\lambda^4,\lambda^5,\lambda^8\} \\
L_5 = \{(1,0,0,0),(1,1,0,1),(0,1,0,1)\} = \{\lambda^0,\lambda^7,\lambda^9\} & L_{23} = \{(1,1,0,0),(0,0,1,1),(1,1,1,1)\} = \{\lambda^4,\lambda^6,\lambda^{12}\} \\
L_6 = \{(1,0,0,0),(0,1,1,1),(1,1,1,1)\} = \{\lambda^0,\lambda^{11},\lambda^{12}\} & L_{24} = \{(1,1,0,0),(0,1,0,1),(1,0,0,1)\} = \{\lambda^4,\lambda^9,\lambda^{14}\} \\
L_7 = \{(0,1,0,0),(0,0,1,0),(0,1,1,0)\} = \{\lambda^1,\lambda^2,\lambda^5\} & L_{25} = \{(1,1,0,0),(0,1,1,1),(1,0,1,1)\} = \{\lambda^4,\lambda^{11},\lambda^{13}\} \\
L_8 = \{(0,1,0,0),(0,0,0,1),(0,1,0,1)\} = \{\lambda^1,\lambda^3,\lambda^9\} & L_{26} = \{(0,1,1,0),(0,0,1,1),(0,1,0,1)\} = \{\lambda^5,\lambda^6,\lambda^9\} \\
L_9 = \{(0,1,0,0),(0,0,1,1),(0,1,1,1)\} = \{\lambda^1,\lambda^6,\lambda^{11}\} & L_{27} = \{(0,1,1,0),(1,1,0,1),(1,0,1,1)\} = \{\lambda^5,\lambda^7,\lambda^{13}\} \\
L_{10} = \{(0,1,0,0),(1,1,0,1),(1,0,0,1)\} = \{\lambda^1,\lambda^7,\lambda^{14}\} & L_{28} = \{(0,1,1,0),(1,1,1,1),(1,0,0,1)\} = \{\lambda^5,\lambda^{12},\lambda^{14}\} \\
L_{11} = \{(0,1,0,0),(1,0,1,0),(1,1,1,0)\} = \{\lambda^1,\lambda^8,\lambda^{10}\} & L_{29} = \{(0,0,1,1),(1,1,0,1),(1,1,1,0)\} = \{\lambda^6,\lambda^7,\lambda^{10}\} \\
L_{12} = \{(0,1,0,0),(1,1,1,1),(1,0,1,1)\} = \{\lambda^1,\lambda^{12},\lambda^{13}\} & L_{30} = \{(0,0,1,1),(1,0,1,0),(1,0,0,1)\} = \{\lambda^6,\lambda^8,\lambda^{14}\} \\
L_{13} = \{(0,0,1,0),(0,0,0,1),(0,0,1,1)\} = \{\lambda^2,\lambda^3,\lambda^6\} & L_{31} = \{(1,1,0,1),(1,0,1,0),(0,1,1,1)\} = \{\lambda^7,\lambda^8,\lambda^{11}\} \\
L_{14} = \{(0,0,1,0),(1,1,0,0),(1,1,1,0)\} = \{\lambda^2,\lambda^4,\lambda^{10}\} & L_{32} = \{(1,0,1,0),(0,1,0,1),(1,1,1,1)\} = \{\lambda^8,\lambda^9,\lambda^{12}\} \\
L_{15} = \{(0,0,1,0),(1,1,0,1),(1,1,1,1)\} = \{\lambda^2,\lambda^7,\lambda^{12}\} & L_{33} = \{(0,1,0,1),(1,1,1,0),(1,0,1,1)\} = \{\lambda^9,\lambda^{10},\lambda^{13}\} \\
L_{16} = \{(0,0,1,0),(0,1,0,1),(0,1,1,1)\} = \{\lambda^2,\lambda^9,\lambda^{11}\} & L_{34} = \{(1,1,1,0),(0,1,1,1),(1,0,0,1)\} = \{\lambda^{10},\lambda^{11},\lambda^{14}\} \\
L_{17} = \{(0,0,1,0),(1,0,1,1),(1,0,0,1)\} = \{\lambda^2,\lambda^{13},\lambda^{14}\} &
\end{array}$$

Die 15 Hyperebenen können auf zwei Arten berechnet werden. Einmal können Sie als Lösungsmenge der 15 nicht-trivialen linearen Gleichungen bestimmt werden, wobei jede Hyperebene genau 7 Punkte und ebenso 7 Geraden enthält.

$H_0 = H_{(0,0,0,1)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 0x_0 + 0x_1 + 0x_2 + 1x_3 = 0\} = \langle L_0, L_1, L_3, L_7, L_{11}, L_{14}, L_{22}\rangle =$
$\{(1,0,0,0), (0,1,0,0), (0,0,1,0), (1,1,0,0), (0,1,1,0), (1,0,1,0), (1,1,1,0)\} = \{\lambda^0, \lambda^1, \lambda^2, \lambda^4, \lambda^5, \lambda^8, \lambda^{10}\}$

$H_1 = H_{(0,0,1,0)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 0x_0 + 0x_1 + 1x_2 + 0x_3 = 0\} = \langle L_0, L_2, L_5, L_8, L_{10}, L_{18}, L_{24}\rangle =$
$\{(1,0,0,0), (0,1,0,0), (0,0,0,1), (1,1,0,0), (1,1,0,1), (0,1,0,1), (1,0,0,1)\} = \{\lambda^0, \lambda^1, \lambda^3, \lambda^4, \lambda^7, \lambda^9, \lambda^{14}\}$

$H_2 = H_{(0,0,1,1)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 0x_0 + 0x_1 + 1x_2 + 1x_3 = 0\} = \langle L_0, L_4, L_6, L_9, L_{12}, L_{23}, L_{25}\rangle =$
$\{(1,0,0,0), (0,1,0,0), (1,1,0,0), (0,0,1,1), (0,1,1,1), (1,1,1,1), (1,0,1,1)\} = \{\lambda^0, \lambda^1, \lambda^4, \lambda^6, \lambda^{11}, \lambda^{12}, \lambda^{13}\}$

$H_3 = H_{(0,1,0,0)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 0x_0 + 1x_1 + 0x_2 + 0x_3 = 0\} = \langle L_1, L_2, L_4, L_{13}, L_{17}, L_{20}, L_{30}\rangle =$
$\{(1,0,0,0), (0,0,1,0), (0,0,0,1), (0,0,1,1), (1,0,1,0), (1,0,1,1), (1,0,0,1)\} = \{\lambda^0, \lambda^2, \lambda^3, \lambda^6, \lambda^8, \lambda^{13}, \lambda^{14}\}$

$H_4 = H_{(0,1,0,1)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 0x_0 + 1x_1 + 0x_2 + 1x_3 = 0\} = \langle L_1, L_5, L_6, L_{15}, L_{16}, L_{31}, L_{32}\rangle =$
$\{(1,0,0,0), (0,0,1,0), (1,1,0,1), (1,0,1,0), (0,1,0,1), (0,1,1,1), (1,1,1,1)\} = \{\lambda^0, \lambda^2, \lambda^7, \lambda^8, \lambda^9, \lambda^{11}, \lambda^{12}\}$

$H_5 = H_{(0,1,1,0)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 0x_0 + 1x_1 + 1x_2 + 0x_3 = 0\} = \langle L_2, L_3, L_6, L_{19}, L_{21}, L_{28}, L_{34}\rangle =$
$\{(1,0,0,0), (0,0,0,1), (0,1,1,0), (1,1,1,0), (0,1,1,1), (1,1,1,1), (1,0,0,1)\} = \{\lambda^0, \lambda^3, \lambda^5, \lambda^{10}, \lambda^{11}, \lambda^{12}, \lambda^{14}\}$

$H_6 = H_{(0,1,1,1)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 0x_0 + 1x_1 + 1x_2 + 1x_3 = 0\} = \langle L_3, L_4, L_5, L_{26}, L_{27}, L_{29}, L_{33}\rangle =$
$\{(1,0,0,0), (0,1,1,0), (0,0,1,1), (1,1,0,1), (0,1,0,1), (1,1,1,0), (1,0,1,1)\} = \{\lambda^0, \lambda^5, \lambda^6, \lambda^7, \lambda^9, \lambda^{10}, \lambda^{13}\}$

$H_7 = H_{(1,0,0,0)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 1x_0 + 0x_1 + 0x_2 + 0x_3 = 0\} = \langle L_7, L_8, L_9, L_{13}, L_{16}, L_{19}, L_{26}\rangle =$
$\{(0,1,0,0), (0,0,1,0), (0,0,0,1), (0,1,1,0), (0,0,1,1), (0,1,0,1), (0,1,1,1)\} = \{\lambda^1, \lambda^2, \lambda^3, \lambda^5, \lambda^6, \lambda^9, \lambda^{11}\}$

$H_8 = H_{(1,0,0,1)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 1x_0 + 0x_1 + 0x_2 + 1x_3 = 0\} = \langle L_7, L_{10}, L_{12}, L_{15}, L_{17}, L_{27}, L_{28}\rangle =$
$\{(0,1,0,0), (0,0,1,0), (0,1,1,0), (1,1,0,1), (1,1,1,1), (1,0,1,1), (1,0,0,1)\} = \{\lambda^1, \lambda^2, \lambda^5, \lambda^7, \lambda^{12}, \lambda^{13}, \lambda^{14}\}$

$H_9 = H_{(1,0,1,0)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 1x_0 + 0x_1 + 1x_2 + 0x_3 = 0\} = \langle L_8, L_{11}, L_{12}, L_{20}, L_{21}, L_{32}, L_{33}\rangle =$
$\{(0,1,0,0), (0,0,0,1), (1,0,1,0), (0,1,0,1), (1,1,1,0), (1,1,1,1), (1,0,1,1)\} = \{\lambda^1, \lambda^3, \lambda^8, \lambda^9, \lambda^{10}, \lambda^{12}, \lambda^{13}\}$

$H_{10} = H_{(1,0,1,1)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 1x_0 + 0x_1 + 1x_2 + 1x_3 = 0\} = \langle L_9, L_{10}, L_{11}, L_{29}, L_{30}, L_{31}, L_{34}\rangle =$
$\{(0,1,0,0), (0,0,1,1), (1,1,0,1), (1,0,1,0), (1,1,1,0), (0,1,1,1), (1,0,0,1)\} = \{\lambda^1, \lambda^6, \lambda^7, \lambda^8, \lambda^{10}, \lambda^{11}, \lambda^{14}\}$

$H_{11} = H_{(1,1,0,0)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 1x_0 + 1x_1 + 0x_2 + 0x_3 = 0\} = \langle L_{13}, L_{14}, L_{15}, L_{18}, L_{21}, L_{23}, L_{29}\rangle =$
$\{(0,0,1,0), (0,0,0,1), (1,1,0,0), (0,0,1,1), (1,1,0,1), (1,1,1,0), (1,1,1,1)\} = \{\lambda^2, \lambda^3, \lambda^4, \lambda^6, \lambda^7, \lambda^{10}, \lambda^{12}\}$

$H_{12} = H_{(1,1,0,1)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 1x_0 + 1x_1 + 0x_2 + 1x_3 = 0\} = \langle L_{14}, L_{16}, L_{17}, L_{24}, L_{25}, L_{33}, L_{34}\rangle =$
$\{(0,0,1,0), (1,1,0,0), (0,1,0,1), (1,1,1,0), (0,1,1,1), (1,0,1,1), (1,0,0,1)\} = \{\lambda^2, \lambda^4, \lambda^9, \lambda^{10}, \lambda^{11}, \lambda^{13}, \lambda^{14}\}$

$H_{13} = H_{(1,1,1,0)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 1x_0 + 1x_1 + 1x_2 + 0x_3 = 0\} = \langle L_{18}, L_{19}, L_{20}, L_{22}, L_{25}, L_{27}, L_{31}\rangle =$
$\{(0,0,0,1), (1,1,0,0), (0,1,1,0), (1,1,0,1), (1,0,1,0), (0,1,1,1), (1,0,1,1)\} = \{\lambda^3, \lambda^4, \lambda^5, \lambda^7, \lambda^8, \lambda^{11}, \lambda^{13}\}$

$H_{14} = H_{(1,1,1,1)} = \{(x_0, x_1, x_2, x_3) \in \mathcal{P} \mid 1x_0 + 1x_1 + 1x_2 + 1x_3 = 0\} = \langle L_{22}, L_{23}, L_{24}, L_{26}, L_{28}, L_{30}, L_{32}\rangle =$
$\{(1,1,0,0), (0,1,1,0), (0,0,1,1), (1,0,1,0), (0,1,0,1), (1,1,1,1), (1,0,0,1)\} = \{\lambda^4, \lambda^5, \lambda^6, \lambda^8, \lambda^9, \lambda^{12}, \lambda^{14}\}$

Einfacher erhält man die Hyperebenen durch Anwendung der Kollineation aus dem Satz von Singer. In folgender Matrix wurde analog zu (5) die Potenzen λ^i der Hyperebene H_0 durch Inkrementieren zu allen Hyperebenen von PG$(3, 2)$ entwickelt.

H_0	H_7	H_{11}	H_{13}	H_{14}	H_6	H_{10}	H_4	H_9	H_{12}	H_5	H_2	H_8	H_3	H_1
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	3	4	5	6	7	8	9	10	11	12	13	14	0
2	3	4	5	6	7	8	9	10	11	12	13	14	0	1
4	5	6	7	8	9	10	11	12	13	14	0	1	2	3
5	6	7	8	9	10	11	12	13	14	0	1	2	3	4
8	9	10	11	12	13	14	0	1	2	3	4	5	6	7
10	11	12	13	14	0	1	2	3	4	5	6	7	8	9

Betrachtet man nur die Hyperebenen, die den Punkt 0 enthalten, so ergibt sich folgende Matrix analog zu (6):

H_0	H_1	H_3	H_2	H_5	H_4	H_6
0	14	13	11	10	7	5
1	0	14	12	11	8	6
2	1	0	13	12	9	7
4	3	2	0	14	11	9
5	4	3	1	0	12	10
8	7	6	4	3	0	13
10	9	8	6	5	2	0

Jede Zahl außer Null ist in obiger Anordnung genau $3 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}_n$ mal enthalten, wie in Satz 9 gezeigt wurde. Jede der Hyperebenen ist also eine $(15, 7, 3)$-Differenzenmenge.

Räumliche Modelle

Für PG$(3, 2)$ gibt es eine faszinierende räumliche Modellierung (siehe [Pol98] für viele weitere schöne Illustrationen geometrischer Strukturen): verwendet man vier Punkte als die Ecken eines Tetraeders, so kann man durch geschickte Anordnung die projektive Geometrie als räumliche Variante der Fano-Ebene zeichnen.

Folgende zwei mit ePiX erstellte Diagramme ergeben zusammen ein Stereogramm, welches ohne Hilfsmittel durch spezielle Fokussierung der Augen (dem Kreuzblick oder Parallelblick) als dreidimensionale Struktur wahrgenommen werden kann.

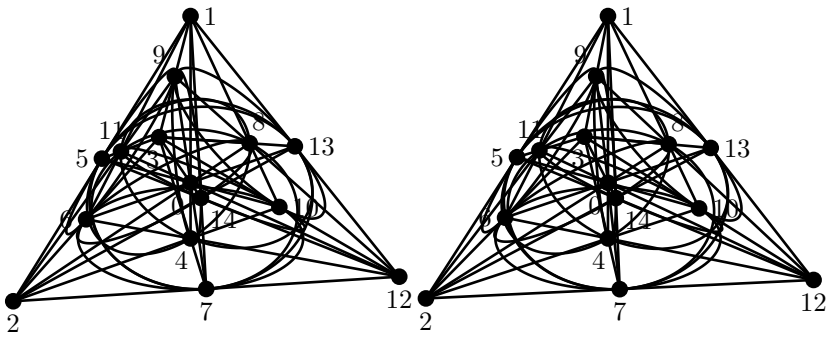


Abbildung 3: Stereogramm von PG$(3, 2)$

Obige vollständige Zeichnung von PG$(3, 2)$ ist durch die 35 verschiedenen Geraden sehr dicht und schwer zu durchschauen. Daher werden zur besseren Visualisierung der Struktur in folgenden vier Stereogrammen einzelne Geradenmengen getrennt illustriert.

Eine hilfreiche Technik zur richtigen Fokussierung der Augen ist diese erst zu entspannen, wodurch die wahrgenommenen Punkte sich verdoppeln und auseinander laufen. Bringt man nun durch weitere bewusste Entspannung zwei gleich-nummerierte Punkte aufeinander, so hat man den richtigen Fokus erreicht.

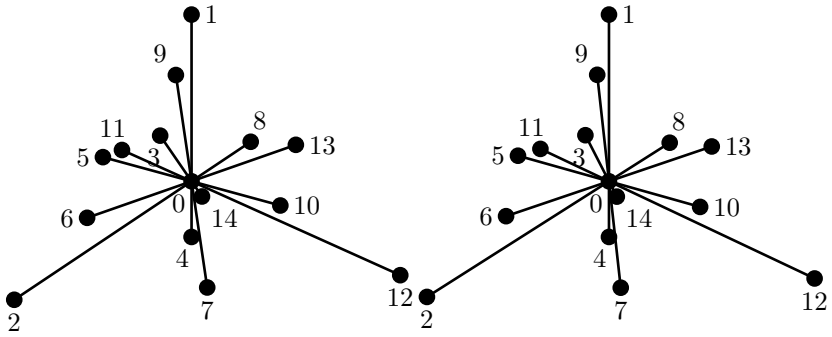


Abbildung 4: Stereogramm der Geraden durch 0 von PG(3, 2)

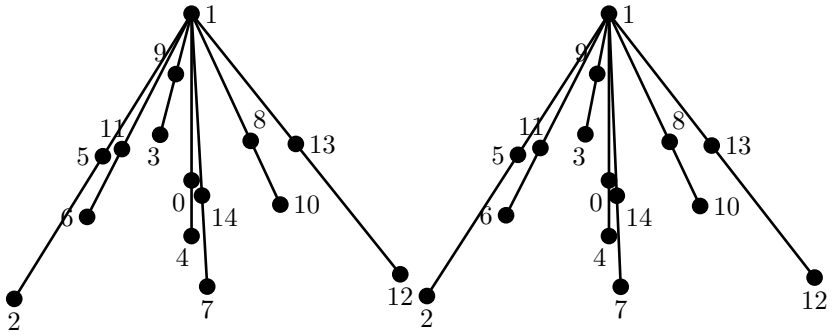


Abbildung 5: Stereogramm der Geraden durch 1 von PG(3, 2)

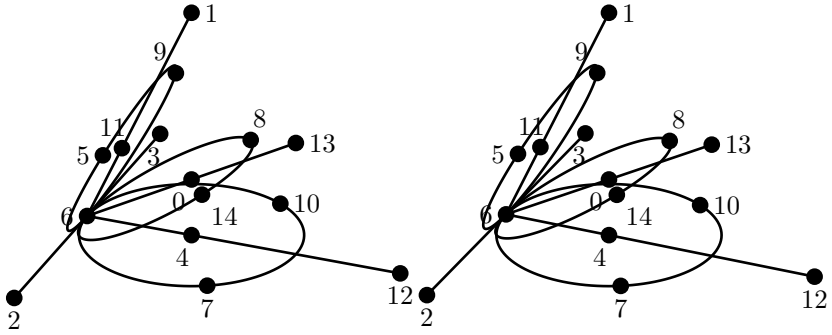


Abbildung 6: Stereogramm der Geraden durch 6 von PG(3, 2)

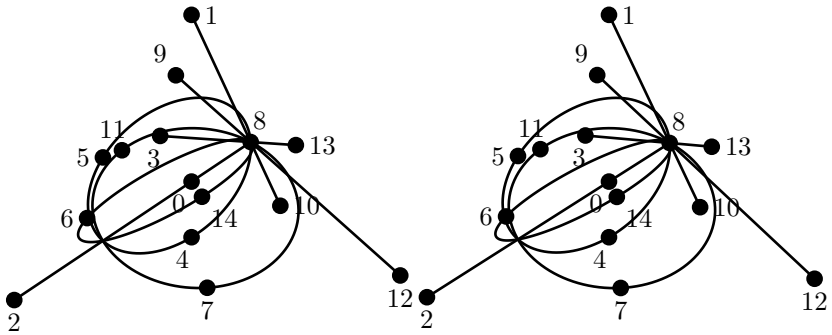


Abbildung 7: Stereogramm der Geraden durch 8 von PG(3, 2)

Die 15 Hyperebenen lassen sich in vier Kategorien einteilen. Zehn hiervon sind Einbettungen der Fano-Ebene in das Tetraeder: vier auf den Außenflächen (H_7, H_8, H_9, H_{11}) und sechs auf der Schnittfläche von Halbierungen (H_0, H_1, H_2, H_3, H_4, H_5).

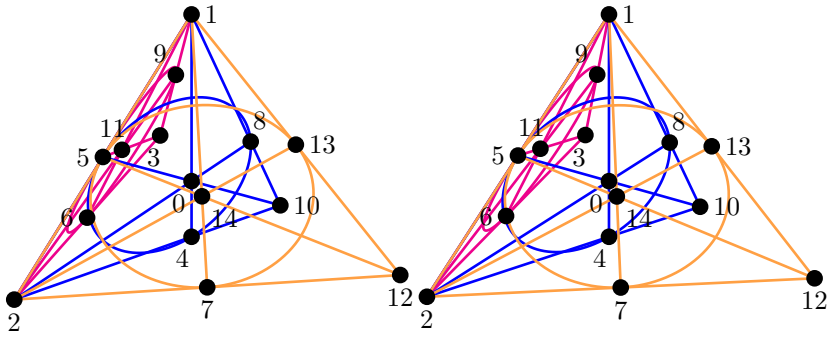


Abbildung 8: Stereogramm der Hyperebenen H_7, H_0 und H_8 von PG$(3, 2)$

Vier weitere Hyperebene enthalten je vier Kreise und einen Punkt des Tetraeders (H_{10}, H_{12}, H_{13}, H_{14})

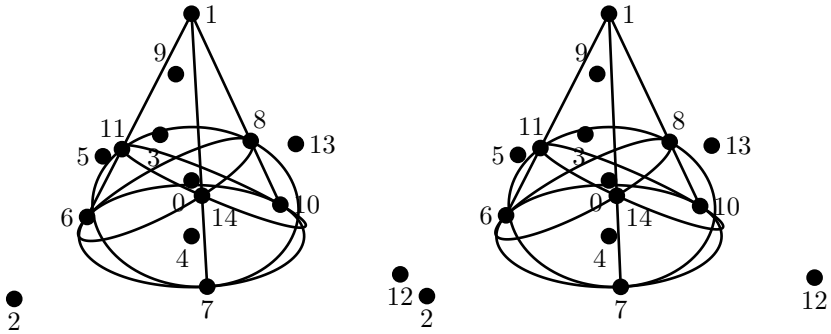


Abbildung 9: Stereogramm der Hyperebene H_{10} von PG$(3, 2)$

Und eine Hyperebene H_6 enthält den Mittelpunkt mit vier umliegenden Kreisen und Geraden zu den Punkten dieser Kreise.

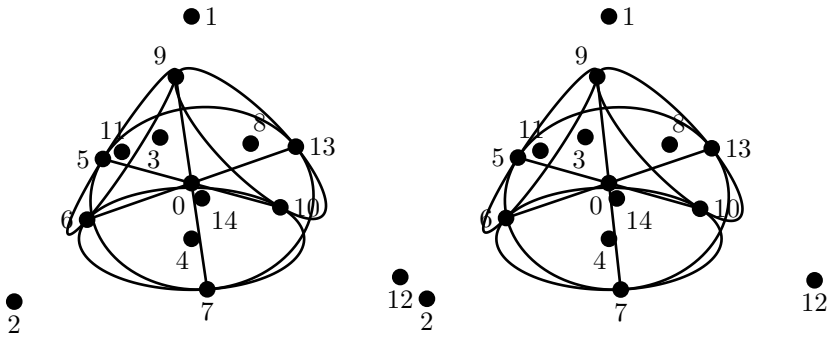


Abbildung 10: Stereogramm der Hyperebene H_6 von PG$(3, 2)$

Der Abschluss dieser Serie von Zeichnungen ist folgendes räumliches, animiertes Modell von PG(3, 2). Das Stereogramm kann mit dem Adobe PDF Reader bewegt dargestellt werden.

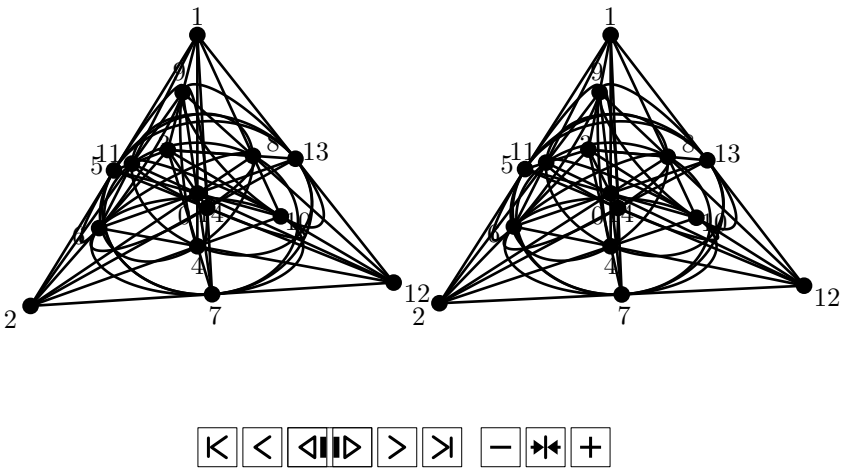


Abbildung 11: Animiertes Stereogramm von PG(3, 2).