JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

TNF

Technisch-Naturwissenschaftliche
Fakultät

Wechselbeziehungen in der Existenz von orthogonalen lateinischen Quadraten, affinen und projektiven Ebenen und (0,m,s)-Netzen

BAKKALAUREATSARBEIT

im Bachelorstudium

Technische Mathematik

Eingereicht von:
Florian Puchhammer

Angefertigt am:
Institut für Finanzmathematik

Beurteilung:
A.Univ.-Prof. Mag. Dr.Friedrich Pillichshammer

Linz, Dezember, 2010

Inhaltsverzeichnis

Zusammenfassung

$(0, m, s)$-nets are most commonly known for their usage in approximating integrals of higher dimensions. The existence of these is in very close relation to that of other combinatorical constructs such as orthogonal latin squares, as well as affine and projective planes. Throughout this document the reader is provided basic properties of these objects. Additionally, the before-mentioned relations between them are clearly lined out and illustrated by (partly comprehensive) examples. So, the main emphasis of this document is clearly on presenting astonishing interdependent existence-theorems concerning orthogonal latin squares, affine and projective planes and $(0, m, s)$- nets and also on providing methods on how to construct one out of another.

1 Einleitung

Vor allem im Bereich der Finanzmathematik steht man oftmals vor dem Problem, eine Funktion über den s-dimensionalen Einheitswürfel zu integrieren. Bekanntlich ist dies jedoch meist entweder äußerst mühsam oder vielfach mit konventionellen Methoden (d.h. über die Stammfunktion) nicht möglich. In vielen Fällen eignet sich hierbei die Verwendung der sog. *Quasi-Monte Carlo Methode*, also eine Approximation des Integrals der Form

$$\int_{[0,1]^s} f(x)\,\mathrm{d}x \approx \frac{1}{N}\sum_{n=0}^{N-1} f(x_n),$$

wobei $x_0, \ldots, x_{N-1} \in [0,1)^s$ fest gewählte Punkte sind.

Für die Punktmenge $\mathcal{P} = \{x_0, \ldots x_{N-1}\}$ lässt sich der dabei verursachte absolute Fehler mit Hilfe der sog. *Koksma-Hlawka Ungleichung*[1] wie folgt abschätzen

$$\left|\int_{[0,1]^s} f(x)\,\mathrm{d}x - \frac{1}{N}\sum_{n=0}^{N-1} f(x_n)\right| \leq D_N^*(\mathcal{P})V(f).$$

Bei der Größe $V(f)$ handelt es sich um die *Variation* im Sinne von *Hardy* und *Krause*, welche nur von der Funktion f abhängt. Der einzige beeinflussbare Parameter in dieser Ungleichung ist die *Sterndiskrepanz* D_N^*, welche sich nach der Verteilung der Punkte in $[0,1)^s$ richtet. Allgemein gilt nach Roth (1954)

$$D_N^*(\mathcal{P}) \geq c\,\frac{(\log N)^{\frac{s-1}{2}}}{N},$$

wobei $c = c(s) > 0$ eine lediglich von der Dimension s abhängige Konstante beschreibt. Es wird allerdings vermutet, dass sich der Exponent in dieser Ungleichung auf $s-1$ vergrößern lässt.

$(0, m, s)$-Netze stehen nun für eine spezielle Wahl der Punktmenge $\mathcal{P}$, welche die wünschenswerte Eigenschaft besitzen, dass

$$D_N^*(\mathcal{P}) = \mathcal{O}\left(\frac{(\log N)^{s-1}}{N}\right).$$

Die Motivation hinter dieser Arbeit ist jedoch nicht, das Zusammenspiel von $(0, m, s)$-Netzen und der Quasi-Monte Carlo Methode zu analysieren.

[1] Details zu den Aussagen in der Einleitung bezügl. der Sterndiskrepanz können in [2] nachgeschlagen werden.

Vielmehr sollen dem Leser sowohl hinreichende als auch notwendige Bedingungen für die Existenz dieser Netze präsentiert werden. Überraschend ist allerdings, dass viele dieser Aussagen ihren Ursprung in gänzlich anderen Gebieten finden, auch wenn dies auf den ersten Blick keineswegs offensichtlich ist.

Das Kernstück dieses Dokuments bilden zweifelsohne die *lateinischen Quadrate*. Das sind $n \times n$-Matrizen, in denen jedes Symbol genau einmal pro Zeile und Spalte vorkommt. Genauer gesagt, sind spezielle Familien dieser, die *paarweise orthogonalen* lateinischen Quadrate von Signifikanz geprägt. Es soll weiters nicht nur auf bewiesene Tatsachen, sondern auch auf bekannte Vermutungen und - falls vorhanden - deren Widerlegung eingegangen werden.

Anschließend werden spezielle geometrische Konstrukte, nämlich *endliche affine* und *projektive Ebenen* untersucht. Dabei sieht sich der Leser hauptsächlich mit Anzahlaussagen bezüglich Geraden und Punkte konfrontiert. Mit Hilfe derer lassen sich Zusammenhänge im Sinne der Existenz von diesen Ebenen untereinander sowie mit paarweise orthogonalen lateinischen Quadraten beschreiben. Gleichzeitig werden auch die Vorgehensweisen erklärt, wie man eines aus dem anderen konstruieren kann und ein anderer Blickwinkel auf die ungelösten Probleme bezüglich lateinischer Quadrate geboten.

Schlussendlich wird das zuvor gesammelte Wissen dazu verwendet, die Existenz von den oben kurz beschriebenen $(0, m, s)$-*Netzen* auf die Existenz von affinen und projektiven Ebenen bzw. gleichbedeutent von speziellen Familien von lateinischen Quadraten zurück zu führen. Außerdem werden noch weitere, darauf beruhende Kriterien zur Existenz vorgestellt. Erneut werden Konstruktionsmethoden angegeben, die es ermöglichen, ein solches Netz zu erzeugen. Auch eine kurze Studie des allgemeineren Falles - nämlich (t, m, s) -Netze - soll nicht ausgelassen werden.

In dieser Arbeit wird dem Leser also eine verblüffende Reise durch hauptsächlich kombinatorische Konstrukte geboten, im Zuge welcher auch auf immer noch offene Probleme eingegangen wird und faszinierende Zusammenhänge aufgezeigt, analysiert und anhand einiger Beispiele anschaulich demonstriert werden.

2 Lateinische Quadrate

2.1 Was sind lateinische Quadrate?

Der Name *lateinisches Quadrat*[2] geht auf den berühmten Mathematiker Leonard Euler zurück. Dieser beschäftigte sich mit quadratischen $n \times n$ Matrizen, deren Einträge er auf spezielle Art und Weise festlegte. Er wählte dabei n verschiedene lateinische Buchstaben und füllte die Matrix derart mit ihnen, dass in keiner Zeile und in keiner Spalte einer dieser Buchstaben mehrmals auftrat. Diesem Konzept liegt auch die erste Definition zugrunde.

Definition 2.1 (Lateinisches Quadrat)**.** Ein *Lateinisches Quadrat der Ordnung* n ist eine $n \times n$ Matrix, welche exakt n verschiedene Symbole enthält. Dabei kommt jedes Symbol genau einmal in jeder Zeile und in jeder Spalte vor.

Diese n verschiedenen Symbole werden, falls nicht anders angegeben, in diesem Dokument immer mit $0, 1, \ldots, n-1$ bezeichnet.

Beispiel 2.2. Ein Beispiel für ein lateinisches Quadrat der Ordnung 3 ist die Matrix

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}.$$

Es ist leicht ersichtlich, dass jedes der 3 verschiedenen Symbole $0, 1, 2$ in jeder Zeile und in jeder Spalte genau einmal auftritt.

Die erste Frage, die sich nun sofort aufdrängt, ist, existiert überhaupt ein lateinisches Quadrat für jede beliebige Ordnung $n \in \mathbb{N}$? Die Antwort darauf fällt überraschen einfach:

Satz 2.3. *Für alle $n \in \mathbb{N}$ existiert ein lateinisches Quadrat der Ordnung n.*

Beweis. (Aus [5].)
Sei $n \in \mathbb{N}$ fix gewählt. Man betrachte die Verknüpfungstabelle der endlichen Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Angenommen, in einer Zeile tritt ein Wert zweimal auf.

$\downarrow + \rightarrow$	$\ldots$	x	$\ldots$	y	$\ldots$
$\vdots$		$\vdots$		$\vdots$	
c	$\ldots$	$c+x$	$\ldots$	$c+y$	$\ldots$
$\vdots$		$\vdots$		$\vdots$	

[2]Wegen des englischen Namens “Latin Square” wird “Lateinisches Quadrat” in der Literatur oftmals mit “LS” abgekürzt.

Dies ist gleichbedeutend mit $c + x \equiv c + y \bmod n$, woraus sofort $x \equiv y \bmod n$ folgt. Das heißt, $c + x$ und $c + y$ stehen an der selben Position in der Verknüpfungstabelle und jedes Symbol kommt somit höchstens einmal in jeder Zeile vor. Da es genau n Spalten gibt, folgt die Behauptung. Auf die selbe Art lässt sich dieses Resultat auch für die Spalten zeigen.

Überträgt man nun die Einträge der Verknüpfungstabelle in eine $n \times n$ Matrix, so erfüllt diese alle in Definition 2.1 angegebenen Eigenschaften und ist somit ein lateinisches Quadrat. □

Zum Beweis dieses Satzes müssen noch zwei Bemerkungen angebracht werden:

Bemerkung 2.4.

- Allgemeiner kann man für obigen Beweis natürlich anstatt $(\mathbb{Z}/n\mathbb{Z}, +)$ jede beliebige n-elementige Gruppe heranziehen.
- Es ist zwar jede Verknüpfungstabelle einer endlichen Gruppe ein lateinisches Quadrat, jedoch ist nicht jedes lateinische Quadrat die Verknüpfungstabelle einer endlichen Gruppe, was in Beispiel 2.5 demonstriert wird.

Beispiel 2.5. Die Einträge in der unten stehenden Tabelle bilden zweifelsohne ein lateinisches Quadrat ...

$\downarrow \circ \rightarrow$	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

... jedoch existiert hier kein rechtsneutrales Element.

Nachdem die Existenz eines lateinischen Quadrates für jede natürliche Ordnung n gesichert ist, wird nun untersucht, wie viele verschiedene es davon gibt.

Eine schlechte Nachricht geht der genaueren Untersuchung jedoch noch voran, nämlich, dass dieses Problem bis dato ungelöst ist. Es herrscht aber zumindest Glück im Unglück: Man kann das genannte Problem verkleinern. Zuerst sind dafür noch einige Definitionen nötig.

Definition 2.6. Mit L_n wird die Anzahl aller möglichen verschiedenen lateinischen Quadrate der Ordnung n bezeichnet.

Definition 2.7 (Reduziertes lateinisches Quadrat)**.** Ein *reduziertes lateinisches Quadrat* (RLS) der Ordnung n ist ein lateinisches Quadrat, dessen erste Zeile und erste Spalte in Standardordnung vorliegen, d.h. sie haben die Form $(0, 1, 2, ..., n-1)$.

Zum Beispiel ist $\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$ ein RLS, im Gegensatz zu $\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$.

Definition 2.8. l_n bezeichnet die Anzahl aller möglichen verschiedenen RLS, die zur Ordnung n existieren.

Bemerkung 2.9. Im Beweis zu Satz 2.3 wurde sogar gezeigt, dass es zu jeder Ordnung n mindestens ein RLS gibt.

Natürlich lässt sich l_n für kleine n leichter berrechnen als L_n. Damit man sich diese Eigenschaft zu Nutze machen kann, muss im folgenden Satz 2.10 noch ein Zusammenhang zwischen diesen beiden Größen hergestellt werden.

Satz 2.10. $\forall n \geq 2$: $\quad L_n = n!(n-1)!l_n$

Beweis. (Aus [5].)
Man betrachte ein beliebiges lateinisches Quadrat der Ordnung n.

- Permutiert man seine Spalten, können daraus wieder $n!$ verschiedene lateinische Quadrate der Ordnung n erzeugt werden.
- Vertauscht man zusätzlich die letzten $n-1$ Zeilen erhält man $(n-1)!$ verschiedene lateinische Quadrate, welche sich darüber hinaus von den Spalten-Permutierten unterscheiden.

Nimmt man nun ein beliebiges RLS der Ordnung n, können daraus nach obiger Anleitung $n!(n-1)!$ verschiedene lateinische Quadrate erzeugt werden und wegen der angewandten Permutationen ist nur dieses eine Quadrat ein RLS. Damit folgt die Ungleichung

$$L_n \geq n!(n-1)!l_n. \tag{1}$$

Andererseits kann man mit Hilfe von Permutationen immer ein RLS aus einem lateinischen Quadrat bilden. Damit gilt also

$$L_n \leq n!(n-1)!l_n. \tag{2}$$

Aus den Ungleichungen (1) und (2) folgt sofort das gewünschte Resultat. □

$$
\begin{array}{ccc}
\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix} \\
\downarrow & & \\
\begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix} \\
\downarrow & & \\
\begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 1 \\ 2 & 1 & 0 \end{pmatrix} \\
\downarrow & & \\
\begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} \\
\downarrow & & \\
\begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix} \\
\downarrow & & \\
\begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}
\end{array}
$$

Abbildung 1: Konstruktion von lateinischen Quadraten aus einem RLS.

Beispiel 2.11. Für $n = 3$ findet man genau ein RLS, also sollte man mit der Konstruktion im Beweis zu Satz 2.10 genau $3! \cdot 2! \cdot 1 = 12$ verschiedene lateinische Quadrate erhalten. Dies wird in Abb. 1 dargestellt.

Eine wichtige Frage bleibt nun noch offen: Wie berechnet man l_n? Dieses Problem ist jedoch noch ungelöst. Bis heute kennt man die Werte bis $n = 11$. In der nachstehenden Tabelle werden die Werte von l_n für $2 \leq n \leq 7$ aufgelistet (vgl. [5]).

n	2	3	4	5	6	7
l_n	1	1	4	65	9.408	16.942.080

Tabelle 1: Werte für l_n.

2.2 Orthogonale lateinische Quadrate

Angenommen man hat zwei lateinische Quadrate der gleichen Ordnung. Dann können diese überlagert werden, sodass daraus eine neue $n \times n$ Matrix entsteht *(Überlagerungsmatrix)*, deren Einträge geordnete Paare sind. Das folgende Beispiel soll dies anschaulich demonstrieren:

Beispiel 2.12.

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \text{ überlagert mit } \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix} \text{ ergibt } \begin{pmatrix} 00 & 11 & 22 \\ 12 & 20 & 01 \\ 21 & 02 & 10 \end{pmatrix}.$$

Mathematisch lässt sich die Überlagerung wie folgt beschreiben:

Definition 2.13 (Überlagerungsmatrix)**.** Seien A und B zwei lateinische Quadrate, beide von der Ordnung n mit den Einträgen a_{ij} bzw. b_{ij}. Die *Überlagerungsmatrix* C von A und B ist jene $n \times n$ Matrix, welche aus den Einträgen $c_{kl} = (a_{kl}, b_{kl})$ für alle $1 \leq k, l \leq n$ besteht.

In Beispiel 2.12 ist eines bereits auffällig. Es kommt nämlich jedes der 9 möglichen Tupel genau einmal in der Überlagerungsmatrix vor. Diese Eigenschaft soll das zentrale Thema dieses Abschnittes sein. Zuvor werden jedoch noch einige Begriffe rund um die *Orthogonalität* benötigt:

Definition 2.14.

(i) Zwei lateinische Quadrate der Ordnung n heißen genau dann *orthogonal*, wenn ihre Überlagerungsmatrix jedes der n^2 möglichen Tupel genau einmal enthält.

(ii) Die lateinischen Quadrate $L_1, L_2, \ldots, L_t$ $(t \geq 2)$ nennt man genau dann *paarweise orthogonal*, wenn für alle $1 \leq i < j \leq t$ gilt, dass L_i und L_j orthogonal sind.

Der Begriff *paarweise orthogonale lateinische Quadrate* wird mit *MOLS*[3] abgekürzt.

(iii) Mit $N(n)$ wird die maximale Anzahl paarweiser orthogonaler lateinischer Quadrate, die zur Ordnung n existieren können, bezeichnet.

Achtung! $N(n)$ sagt nichts über die Anzahl verschiedener MOLS, die man konstruieren kann, aus, sondern nur darüber, wie viele lateinische Quadrate der Ordnung n maximal paarweise orthogonal sein können!

Naheliegender Weise wird nun die Größe $N(n)$ näher untersucht. Dabei steht an erster Stelle eine obere Schranke.

Satz 2.15. $\forall n \geq 2 : \qquad N(n) \leq n - 1$

Beweis. (Aus [5].)
Seien L_1 und L_2 zwei orthogonale lateinische Quadrate der Ordnung n. Wenn man nun die Symbole in L_1 derart umbenennt, dass diese Neuzuordnung bijektiv ist, dann ändert dies natürlich nichts an der Orthogonalität zwischen L_1 und L_2.

Damit kann angenommen werden, dass in jeder Menge von MOLS die erste Zeile eines jeden lateinischen Quadrates in Standardordnung vorliegt (d.h. $0, 1, 2, \ldots, n-1$).

Nun betrachtet man den Eintrag in der zweiten Zeile, erste Spalte von jedem lateinischen Quadrat in einer Menge von $N(n)$ MOLS.

$$\begin{pmatrix} 0 & 1 & 2 & \ldots & n-1 \\ \sqcup & \ldots & & & \end{pmatrix}$$

[3] mutually orthogonal latin squares

An dieser Position kann in keinem der $N(n)$ lateinischen Quadrate eine 0 stehen, da es sich sonst nicht um ein solches handeln würde.

Weiters stehen in der Überlagerungsmatrix von zwei beliebigen Quadraten dieser Menge alle Tupel der Form $(i, i), 1 \leq i \leq n-1$, bereits in der ersten Zeile. Daher müssen alle diese paarweise orthogonalen lateinischen Quadrate an der untersuchten Position verschiedene Symbole aufweisen, sonst wären sie nicht orthogonal.

Da (nach Ausschluss der 0) nur noch $n-1$ Symbole zur Auswahl stehen, kann man maximal $n-1$ zueinander orthogonale lateinische Quadrate finden, also $N(n) \leq n-1$. □

Diese Schranke wirkt äußerst schwach, betrachtet man doch nur die erste, nicht besetzte Stelle im Quadrat. Umso mehr verblüfft es, dass für bestimmte n - nämlich für Primzahlenpotenzen - Gleichheit herrscht, wie später in Satz 2.17 bewiesen werden wird.

Auch wenn der Leser zu diesem Zeitpunkt eventuell noch (berechtigte) Zweifel an dieser Tatsache hat, wird eine Menge von MOLS, die die Ungleichung aus Satz 2.15 vollständig "ausnützt" schon jetzt mit einem eigenen Namen versehen.

Definition 2.16 (Vollständigkeit)**.** Eine Menge von $t \geq 2$ MOLS der Ordnung n heißt genau dann *vollständig*, falls $t = n-1$ gilt.

Wie oben bereits kurz erwähnt, gibt es für bestimmte Ordnungen eine solche vollständige Menge.

Satz 2.17 (Bose 1938)**.** *Sei q eine Primzahlpotenz. Dann gilt*

$$N(q) = q - 1.$$

Beweis. (Aus [5].)
Für diesen Beweis benötigt man den endlichen Körper $\mathbb{F}_q$, wobei q eine Primzahlpotenz ist. Sei weiters $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\} =: \{a_1, \ldots, a_{q-1}\}$.

- Man benenne die Spalten und Zeilen einer $q \times q$ Matrix mit den Elementen aus $\mathbb{F}_q$ derart, sodass jede Position in dieser Matrix eindeutig identifizierbar ist.

  Die Reihenfolge der Auflistung ist hierbei egal. D.h. man kann der ersten Zeile zB die Nummer 2 und der ersten Spalte die Nummer 0 zuordnen. Dann würde die erste Position in der Matrix, die normalerweise mit $(1, 1)$ identifiziert wird, mit $(2, 0)$ angesprochen.

- Nun wird zu jedem $1 \leq i \leq q-1$ ein lateinisches Quadrat L_i konstruiert:

  a. Definiere ein lineares Polynom $f_i(x, y) := a_i x + y$ mit $a_i \in \mathbb{F}_q^*$.

  b. Wähle für jede Position (k, l) in L_i (gemäß der oben gewählten Nummerierung) $f_i(k, l)$ als Eintrag.

- Damit wurde erreicht:

  i. Jedes Polynom f_i generiert ein lateinisches Quadrat. Denn, angenommen in der Spalte y kommt ein Symbol doppelt vor,

	$\dots$	y	$\dots$
$\vdots$		$\vdots$	
x	$\dots$	$f_i(x,y)$	$\dots$
$\vdots$		$\vdots$	
x'	$\dots$	$f_i(x',y)$	$\dots$
$\vdots$		$\vdots$	

  dann folgt

  $$f_i(x, y) = f_i(x', y) \iff a_i x + y = a_i x' + y \iff x = x'.$$

  Also kommt jedes Symbol maximal einmal pro Spalte vor. Da es genau q Zeilen gibt, folgt, dass jedes Symbol genau einmal in jeder Spalte auftritt. Das selbe Argument funktoniert natürlich auch für die Zeilen.

  ii. Je zwei so generierte lateinische Quadrate sind verschieden. Nimmt man nämlich an, es existieren $1 \leq i < j \leq q-1$, sodass die durch f_i und f_j erzeugten Quadrate gleich sind, dann muss für ein $x \neq 0$ folgendes gelten

  $$f_i(x, y) = f_j(x, y) \iff a_i x + y = a_j x + y \iff a_i = a_j.$$

  Dies steht im Widerspruch zu $i < j$.

  iii. Die erzeugten lateinischen Quadrate sind MOLS, also je zwei verschiedene sind orthogonal.

  Seien $1 \leq i < j \leq q-1$ und $(b_1, b_2) \in \mathbb{F}_q \times \mathbb{F}_q$. Es soll gezeigt werden, dass das Paar (b_1, b_2) genau einmal in der Überlagerungsmatrix von L_i und L_j vorkommt. Oder äquivalent dazu: Das lineare Gleichungssystem

  $$\begin{aligned} a_i x + y &= b_1 \\ a_j x + y &= b_2 \end{aligned}$$

besitzt eine eindeutige Lösung.
Nun ist aber für $i \neq j$ $\det \begin{vmatrix} a_i & 1 \\ a_j & 1 \end{vmatrix} = a_i - a_j \neq 0$ und somit das System eindeutig lösbar.

Zusammenfassend wurde also bewiesen, dass $q-1$ verschiedene und paarweise orthogonale lateinische Quadrate der Ordnung q konstruiert werden können und somit folgt mit Satz 2.15, dass $N(q) = q - 1$. □

Dank diesem konstruktiven Beweis ist es für Primzahlenpotenzen q sogar möglich, einen Algorithmus abzuleiten, wie man diese $q - 1$ MOLS konstruiert. Dieser soll nun gleich anhand eines Beispiels demonstriert werden.

Beispiel 2.18.

1. Es wird $q = 3$ angenommen, das heißt man erhält 2 MOLS.
2. Die Zeilen und Spalten werden beide mit $2, 0, 1$ durchnummeriert.
3. Nun kann man sich die nötigen linearen Polynome definieren.

$$\begin{aligned} f_1(x, y) &:= x + y \\ f_2(x, y) &:= 2x + y \end{aligned}$$

4. Schlussendlich berechnet man die beiden MOLS L_1 und L_2.

$$L_1 = \begin{pmatrix} f_1(2,2) & f_1(2,0) & f_1(2,1) \\ f_1(0,2) & f_1(0,0) & f_1(0,1) \\ f_1(1,2) & f_1(1,0) & f_1(1,1) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

$$L_2 = \begin{pmatrix} f_2(2,2) & f_2(2,0) & f_2(2,1) \\ f_2(0,2) & f_2(0,0) & f_2(0,1) \\ f_2(1,2) & f_2(1,0) & f_2(1,1) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

5. Anschließend kann man noch kontrollieren, ob L_1 und L_2 wirklich orthogonal zueinander sind, indem man ihre Überlagerungsmatrix

$$\begin{pmatrix} 10 & 21 & 02 \\ 22 & 00 & 11 \\ 01 & 12 & 20 \end{pmatrix}$$

betrachtet. Da jedes Tupel genau einmal vorkommt, handelt es sich tatsächlich um zwei orthogonale lateinische Quadrate.

Für Primzahlenpotenzen q ist die Suche nach $N(q)$ also beendet. Bei der Frage nach den Werten für andere $n \in \mathbb{N}$ muss man sich leider eingestehen, dass die meisten noch unbekannt sind.

Allerdings gibt es diesbezüglich eine Reihe von Vermutungen. Die wohl "bedeutendste" (sofern man bei Vermutungen von *bedeutend* sprechen kann) ist die Rückrichtung des vorherigen Satzes 2.17.

Vermutung 2.19 (Prime Power Conjecture)**.** *Für jedes natürliche $n \geq 2$ gilt*

$$N(n) = n - 1 \qquad \Longleftrightarrow \qquad n \text{ ist eine Primzahlpotenz.}$$

Dieses Problem erweist sich allerdings als äußerst hartnäckig und hat sich damit bereits einmal den Titel des *nächsten Fermat'schen Problems* eingehandelt.

Die Prime Power Conjecture ist natürlich nicht die einzige Vermutung die es bisher gab bzw. auch jetzt noch durch den Raum schwebt. Um die Entwicklung in der Erforschung von $N(n)$ besser erfassen zu können, werden im Folgenden die wichtigsten und bekanntesten Behauptungen behandelt. Der erste Mathematiker, der hierbei erwähnt werden soll, ist *Leonard Euler*.

Vermutung 2.20 (Euler 1782)**.** *Sei $n = 2(2k + 1)$ mit $k \geq 0$, dann ist $N(n) = 1$.*

Euler selbst konnte nicht einmal den Fall $n = 6$, also $k = 1$, beweisen. Tatsächlich wurde $N(6) = 1$ erst im Jahr 1900 (d.h. 118 Jahre später) gezeigt, was für den damaligen Stand der Technik eine beachtliche Leistung darstellt, hatte man doch keinen Computer zur Verfügung und ruft man sich in Erinnerung, dass nach Satz 2.10 und den Werten aus Tabelle 1 $L_6 \approx 8{\cdot}10^8$.

Mittlerweile hat man sich natürlich eingehend mit Euler's Vermutung beschäftigt und gelangte zu dem Resultat, dass sie genau für $k \in \{0, 1\}$ richtig ist. Für alle anderen Werte für k ist sie falsch. Diese Tatsache wurde allerdings erst viel später bekannt (siehe dazu Satz 2.22 auf Seite 13).

Nun wusste man also lediglich, dass die Vermutung 2.20 für $k \in \{0, 1\}$ stimmt. Nachdem Euler zu seiner Zeit als ein zuverlässiger Rechner galt und seine Vermutung schon für zwei Werte für k bewiesen war, getraute sich ein Mathematiker namens *MacNeish* diese sogar noch zu verallgemeinern.

Vermutung 2.21 (MacNeish 1922)**.** *Seien* $q_1 < q_2 < \ldots < q_r$ *Potenzen verschiedener Primzahlen und sei* $n = q_1 \cdots q_r$*. Dann gilt*

$$N(n) = q_1 - 1.$$

MacNeish's Vermutung stimmt natürlich für $n = 6$ und nach Satz 2.17 für einfache Primzahlenpotenzen. 1959 ereilte diese Behauptung allerdings das Schicksal der meisten Vermutungen, als *Parker* zeigte, dass

$$N(21) = N(3 \cdot 7) \geq 4.$$

Im selben Jahr wurde auch noch Eulers Vermutung widerlegt. Dies geschah durch *Bose* und *Shrikhande*, die beweisen konnten, dass

$$N(22) = N(2 \cdot (2 \cdot 5 + 1)) \geq 2.$$

Ein Jahr später gelang es diesen drei Herren *(Bose, Shrikhande* und *Parker)* dann noch ein allgemeines Resultat vorzuweisen, nämlich:

Satz 2.22 (Bose, Shrikhande, Parker 1960)**.**

$$\forall n \in \mathbb{N} \setminus \{2, 6\} : \qquad N(n) \geq 2$$

Bemerkung 2.23. Dieses Resultat garantiert also, dass für fast alle $n \in \mathbb{N}$ immer zumindest ein Paar MOLS existieren muss. Nebenbei bemerkt widerlegt Satz 2.22 ebenfalls Eulers Vermutung.

In der nachstehenden Tabelle 2 werden zusammenfassend die aus diesem Dokument bekannten Werte für $N(n)$ aufgelistet.

n	2	3	2^2	5	6	7	2^3	3^2
$N(n)$	1	2	3	4	1	6	7	8

Tabelle 2: Werte für $N(n)$.

Überraschend ist allerdings, dass an $N(10)$ immer noch geforscht wird. Bekannt ist allerdings:

Satz 2.24 (Lam, Thiel, Swiercz 1989)**.**

$$N(10) < 9$$

Interessant ist dabei, dass, obwohl dieses Problem mathematisch höchst anspruchsvoll im Vorfeld aufbereitet wurde, benötigte die Vollendung des Beweises noch immer über 2.000 Stunden Rechenzeit auf einem Cray-Supercomputer.

Mit einem weiteren Satz (entnommen aus [5]) lässt sich die obere Schranke aus Satz 2.24 sogar noch etwas weiter herabsetzen.

Satz 2.25.

$$n > 4 \quad \wedge \quad N(n) < n - 1 \qquad \Longrightarrow \qquad N(n) \leq n - 4$$

Korollar 2.26.

$$2 \leq N(10) \leq 6$$

Beweis. Folgt unmittelbar aus Satz 2.22 und aus Satz 2.25 zusammen mit Satz 2.24. □

2.2.1 Die Kronecker Produkt Konstruktion

Um eine weitere, bessere untere Schranke für $N(n)$ beweisen zu können, verwendete *MacNeish* eine spezielle Verknüpfung zweier lateinischer Quadrate, die sich sehr nahe an das *Kronecker Produkt* von zwei Matrizen anlehnt.

Seien also $H = (h_{ij})$ und $K = (k_{rs})$ zwei lateinische Quadrate der Ordnung n_1 bzw. n_2. Diese werden nun zu einer Matrix der Dimension $n_1 n_2 \times n_1 n_2$ zusammengesetzt, geschrieben $H \otimes K$. Dazu ersetzt man jedes h_{ij} in H mit einer $n_2 \times n_2$ Matrix mit den Einträgen $a_{rs} = (h_{ij}, k_{rs})$.

Zur Veranschaulichung dieser Konstruktionsmethode folgt ein kurzes Beispiel.

Beispiel 2.27.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} = \left(\begin{array}{ccc|ccc} 00 & 01 & 02 & 10 & 11 & 12 \\ 01 & 02 & 00 & 11 & 12 & 10 \\ 02 & 00 & 01 & 12 & 10 & 11 \\ \hline 10 & 11 & 12 & 00 & 01 & 02 \\ 11 & 12 & 10 & 01 & 02 & 00 \\ 12 & 10 & 11 & 02 & 00 & 01 \end{array}\right)$$

Eines fällt dem geübten Auge sofort auf. Ersetzt man nämlich in obigem Beispiel die Paare $00, 01, \ldots, 12$ mit den Ziffern $0, 1, \ldots, 5$ erhält man die Matrix

$$\begin{pmatrix} 00 & 01 & 02 & 10 & 11 & 12 \\ 01 & 02 & 00 & 11 & 12 & 10 \\ 02 & 00 & 01 & 12 & 10 & 11 \\ 10 & 11 & 12 & 00 & 01 & 02 \\ 11 & 12 & 10 & 01 & 02 & 00 \\ 12 & 10 & 11 & 02 & 00 & 01 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 0 & 4 & 5 & 3 \\ 2 & 0 & 1 & 5 & 3 & 4 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 5 & 3 & 1 & 2 & 0 \\ 5 & 3 & 4 & 2 & 0 & 1 \end{pmatrix},$$

welche zweifelsohne wieder ein lateinisches Quadrat ist. Diese Spur wird gleich weiter verfolgt und führt umgehend zu folgendem Lemma:

Lemma 2.28. *Seien H, K zwei lateinische Quadrate der Ordnung n_1 bzw. n_2. Dann ist $A = H \otimes K$ ein lateinisches Quadrat der Ordnung $n_1 n_2$.*

Beweis. Die Dimension der Matrix A ist nach der Konstruktionsmethode natürlich $n_1 n_2$.

Angenommen $H \otimes K$ ist kein lateinisches Quadrat, dann existiert ein Tupel (h, k), das in A mindestens zwei mal in der selben Spalte oder in der selben Zeile vorkommt. Nun ist aber H ein lateinisches Quadrat, welches die erste Komponente eines jeden Tupel in $H \otimes K$ bestimmt. Soll also (h, k) zweimal in A in der selben Spalte/Zeile auftreten, dann kann dies nur im selben $n_2 \times n_2$ Block mit den Einträgen $(h, .)$ geschehen.

Betrachtet man jetzt nur die zweite Komponente der Tupel in diesem Block, erhält man wieder K. Da aber weiterhin (h, k) zweimal im selben Block in der selben Zeile/Spalte vorkommt, bedeutet das, dass k in K in der selben Zeile/Spalte auftritt und somit kann K kein lateinisches Quadrat sein. Widerspruch!

Also kommt jedes Tupel höchstens einmal in jeder Zeile/Spalte vor und da es insgesamt $n_1 n_2$ Einträge pro Spalte/Zeile gibt, ist $H \otimes K$ ein lateinisches Quadrat. □

Damit sind die Möglichkeiten, die diese Konstruktionsmethode mit sich bringt, noch keineswegs ausgeschöpft. Man kann sogar noch eine Aussage, die die Orthogonalität betrifft, beweisen.

Lemma 2.29. *Seien H_1, H_2 zwei orthogonale lateinische Quadrate der Ordnung n_1, sowie K_1, K_2 zwei orthogonale lateinische Quadrate der Ordnung n_2. Dann ist $H_1 \otimes K_1$ orthogonal zu $H_2 \otimes K_2$.*

Beweis. Dass es sich bei den Matrizen $H_1 \otimes K_1$ und $H_2 \otimes K_2$ tatsächlich um lateinische Quadrate handelt, wurde bereits im vorherigen Lemma 2.28 gezeigt.

Angenommen die Aussage stimmt nicht, das heißt, ein Tupel der Form $\big((h_1,k_1),(h_2,k_2)\big)$ kommt in der Überlagerungsmatrix von $H_1 \otimes K_1$ und $H_2 \otimes K_2$ zumindest zwei mal an verschiedenen Positionen vor.

Dies hat zur Folge, dass in der Überlagerungsmatrix von H_1 und H_2 das Paar (h_1,h_2) ebenfalls zweimal vorkommt. Da es sich hierbei aber um zwei orthogonale lateinische Quadrate handelt, kann dies nur sein, falls die beiden Positionen ein und die selbe sind, also das Tupel eigentlich nur einmal auftritt.

Nach Voraussetzung befindet sich $\big((h_1,k_1),(h_2,k_2)\big)$ an zwei *verschiedenen* Stellen in der Überlagerungsmatrix von $H_1 \otimes K_1$ und $H_2 \otimes K_2$. Damit muss nun (k_1,k_2) an zwei verschiedenen Positionen in der Überlagerung von K_1 und K_2 stehen, im Widerspruch zu K_1 und K_2 sind orthogonal. Da insgesamt $(n_1 n_2)^2$ Einträge zu besetzen sind, folgt die Behauptung. □

Bemerkung 2.30. Für fast alle $n \in \mathbb{N}$ kann man sich nun auf diesem Weg MOLS konstruieren. Probleme machen weiterhin die Zahlen der Form $n = 2(2k+1)$ mit $k \in \mathbb{N}$, da $N(2) = 1$. Man findet also H_1 und H_2 aus obigen Satz nicht.

Mit Hilfe von diesen zwei Lemmata ist es nun möglich, eine weitere, vielfach bessere untere Schranke als jene aus Satz 2.22 beweisen.

Satz 2.31 (MacNeish 1922)**.** *Seien $q_1 < q_2 < \ldots < q_r$ Potenzen verschiedener Primzahlen und $n = q_1 \cdots q_r$. Dann gilt*

$$N(n) \geq q_1 - 1.$$

Beweis. (Aus [5].)
Für $q_1 = 2$ stimmt diese Aussage natürlich immer. Deshalb reicht es aus, nur den Fall $q_1 > 2$ zu betrachten. Wegen Satz 2.22 kann man dann schließen, dass $N(q_i) \geq 2$ für alle $1 \leq i \leq r$.

Nun nützt man den aus Satz 2.17 abgeleiteten Algorithmus um MOLS der Ordnung q_i zu erzeugen. Davon gibt es für jedes $1 \leq i \leq r$ wegen $N(q_i) = q_i - 1$ mindestens $q_1 - 1$ viele. Diese setzt man anschließend wie in Lemma 2.29 zu $q_1 - 1$ MOLS der Ordnung $q_1 \cdots q_r = n$ zusammen . □

Dieser Satz lädt schon wieder dazu ein, neue Vermutungen aufzustellen. Auf Seite 13 wurde festgestellt, dass die MacNeish Vermutung (Vermutung 2.21) $N(n) = q_1 - 1$ mit den dort angegebenen Bezeichnungen wegen $N(21) \geq 4$ falsch ist.

Nun gibt es Mathematiker, die sogar behaupten, dass diese Vermutung fast nie stimmt:

Vermutung 2.32 (Laywine, Mullen, Whittle 1995)**.** *Sei n keine Primzahlpotenz und $n \neq 6$. Seien weiters $q_1 < \ldots < q_r$ Potenzen verschiedener Primzahlen, sodass $n = q_1 \cdots q_r$. Dann gilt die MacNeish Vermutung nie. D.h.*

$$N(n) > q_1 - 1.$$

Bemerkung 2.33. Bis jetzt ist diese Vermutung für $n < 63$ bewiesen.

Ohne Beweis wird noch ein weiterer Satz angegeben, um das Kapitel der allgemeinen lateinischen Quadrate schlussendlich noch abzurunden.

Satz 2.34 (Bruck, Ryser 1949)**.** *Für unendlich viele $n \in \mathbb{N}$ gilt*

$$N(n) < n - 1.$$

2.3 Sudoku Squares

Sicherlich sind vielen Menschen heute Sudokus ein Begriff. In diesem Abschnitt wird hauptsächlich zwischen dem ungelösten Sudoku (*Sudoku Puzzle*) und dem gelösten Sudoku (*Sudoku Square*) unterschieden.

Ein *Sudoku Square* ist präziser formuliert eine spezielle Form eines lateinischen Quadrates und ein *Sudoku Puzzle* eine spezielle Form eines partiellen[4] lateinischen Quadrates. Von nun an steht q immer für eine beliebige Primzahlpotenz.

Definition 2.35 (Sudoku Square, Sudoku Puzzle)**.**

i. Ein *Sudoku Square* (SS) ist ein lateinisches Quadrat der Ordnung q^2, in dem jedes der q^2 disjunkten $q \times q$ Teilquadrate jedes Symbol genau einmal enthält.

ii. Ein *Sudoku Puzzle* (SP) ist ein partielles lateinisches Quadrat, das zu einem Sudoku Square erweitert werden kann.

[4] *Partiell* wird hier in dem Sinn verstanden, dass nicht alle Positionen im Quadrat belegt sind.

Ziel ist es jetzt, ein SS zu konstruieren. Hierzu sind jedoch noch einige Vorbereitungen notwendig.

Definition 2.36 (Zeilen-Spalten magisches Quadrat)**.** Ein *Zeilen-Spalten magisches Quadrat* der Ordnung n ist eine $n \times n$ Matrix, deren Zeilen- und Spaltensummen konstant gleich sind.

Solch ein Zeilen-Spalten magisches Quadrat kann auch auf ganz einfache Art und Weise aus zwei orthogonalen lateinischen Quadraten konstruiert werden:

Lemma 2.37. *Seien L_1 und L_2 zwei orthogonale lateinische Quadrate der Ordnung n mit Einträgen aus $\{0, \ldots, n-1\}$. Dann ist*

$$M = nL_1 + L_2$$

ein Zeilen-Spalten magisches Quadrat, welches aus den Zahlen $0, 1, \ldots, n^2-1$ besteht.

Beweis. Zuerst soll gezeigt werden, dass die Zeilen- bzw. Spaltensummen von M konstant gleich sind. Dazu betrachte man die Summe über die k-te Zeile von $nL_1 + L_2$ und erinnert sich daran, dass in den Zeilen von L_1 und L_2 jedes Symbol genau einmal vorkommt.

$$\sum_{i=1}^{n} \left(nl_{ki}^1 + l_{ki}^2\right) = n \sum_{i=0}^{n-1} i + \sum_{j=0}^{n-1} j = \frac{n^2(n-1)}{2} + \frac{n(n-1)}{2} = \frac{n(n-1)(n+1)}{2}$$

Dieser Ausdruck ist unabhängig von k und somit ist die Zeilensumme konstant gleich. Für die Spaltensummen geht man analog vor.

Als nächstes wird bewiesen, dass jede Zahl zwischen 0 und $n^2 - 1$ genau einmal in M vorkommt. Man nehme an, dass es zwei verschiedene Positionen (i, j) und (r, s) gibt, sodass

$$nl_{ij}^1 + l_{ij}^2 = nl_{rs}^1 + l_{rs}^2$$

gilt. Daraus folgt sofort

$$n \left|l_{ij}^1 - l_{rs}^1\right| = \left|l_{ij}^2 - l_{rs}^2\right|.$$

Ist nun $l_{ij}^1 = l_{rs}^1$, dann gilt auch $l_{ij}^2 = l_{rs}^2$ und somit können L_1 und L_2 nicht orthogonal sein.

Also ist nur noch der Fall $l_{ij}^1 \neq l_{rs}^1$ zu prüfen. Nun gilt die folgende Ungleichungskette:

$$n \leq n \left| l_{ij}^1 - l_{rs}^1 \right| = \left| l_{ij}^2 - l_{rs}^2 \right| \leq n - 1.$$

Das ist natürlich nicht möglich und somit kommt jede der Zahlen $0, \ldots, n^2-1$ genau einmal in M vor. □

Mit diesem Lemma sind nun alle Grundsteine dafür gelegt, ein SS zu konstruieren. Dieses wird darüber hinaus die zusätzliche Eigenschaft besitzen, dass die Summe über seine Zeilen/Spalten konstant gleich sein wird. Dazu geht man wie folgt vor:

1. Generiere zwei orthogonale lateinische Quadrate der Ordnung q (vgl. Beweis zu Satz 2.17).
2. Verwende diese, um ein Zeilen-Spalten magisches Quadrat M wie in Lemma 2.37 zu erzeugen.
3. Setze M in die linke obere Ecke.
4. Verschiebe die Zeilen von M um eins zyklisch nach unten und füge das so erhaltene Zeilen-Spalten magische Quadrat rechts an. Fahre so fort, bis insgesamt q Blöcke nebeneinander stehen.
5. Permutiere nach unten hin die Spalten auf analoge Weise.

Diese Vorgehensweise soll auch gleich wieder anhand eines Beispiels für $q = 3$ erprobt werden.

Beispiel 2.38.

1. Zwei orthogonale Quadrate wurden bereits im Beispiel 2.18 auf Seite 11 erzeugt.
$$\begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$
2. Nun kann das Spalten-Zeilen magische Quadrat mit der entsprechenden Formel berechnet werden.
$$3 \cdot \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 7 & 2 \\ 8 & 0 & 4 \\ 1 & 5 & 6 \end{pmatrix}$$

$$\begin{array}{ccccc}
\begin{pmatrix} 3 & 7 & 2 \\ 8 & 0 & 4 \\ 1 & 5 & 6 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 5 & 6 \\ 3 & 7 & 2 \\ 8 & 0 & 4 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 8 & 0 & 4 \\ 1 & 5 & 6 \\ 3 & 7 & 2 \end{pmatrix} \\
\downarrow & & \downarrow & & \downarrow \\
\begin{pmatrix} 2 & 3 & 7 \\ 4 & 8 & 0 \\ 6 & 1 & 5 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 6 & 1 & 5 \\ 2 & 3 & 7 \\ 4 & 8 & 0 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 4 & 8 & 0 \\ 6 & 1 & 5 \\ 2 & 3 & 7 \end{pmatrix} \\
\downarrow & & \downarrow & & \downarrow \\
\begin{pmatrix} 7 & 2 & 3 \\ 0 & 4 & 8 \\ 5 & 6 & 1 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 5 & 6 & 1 \\ 7 & 2 & 3 \\ 0 & 4 & 8 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 0 & 4 & 8 \\ 5 & 6 & 1 \\ 7 & 2 & 3 \end{pmatrix}
\end{array}$$

Abbildung 2: Konstruktion eines Sudoku Squares.

3. Die nächsten Schritte werden in Abb. 2 festgehalten.

Weiß man, wie man ein SS konstruiert, stellt es auch kein Problem mehr dar, ein SP zu erzeugen, muss man dafür doch nur Werte aus einem SS entfernen. Wie viele Zahlen man jedoch herausnehmen darf, damit die Erweiterung von einem SP zum SS eindeutig bleibt (d.h., dass das Sudoku eindeutig lösbar ist), ist in den meisten Fällen noch unbekannt.

Hierzu noch eine kurze Zusammenfassung, von dem, was darüber bekannt ist:

- Es existieren Sudoku Puzzles, in denen 77 von 81 Felder ausgefüllt sind und die nicht eindeutig zu einem SS erweiterbar sind.
- Es gibt aber auch solche, bei denen lediglich die Zahlen in 17 der 81 Felder bekannt sind, die eindeutig erweiterbar sind. Bei 16 befüllten Feldern ist man sich schon wieder nicht mehr sicher.

3 Affine und Projektive Ebenen

Um die Reichweite von lateinischen Quadraten besser zum Ausdruck zu bringen und nicht zuletzt, um einen Übergang zu $(0, m, s)$-Netzen zu schaffen, werden in diesem Abschnitt *affine* und *projektive Ebenen* behandelt. Der Zusammenhang mit lateinischen Quadraten ist zu Anfang wahrscheinlich wenig offensichtlich, es sei jedoch bereits jetzt schon verraten, dass sich mit Hilfe von MOLS eine sehr starke Existenzaussage treffen lässt.

3.1 Grundlegende Eigenschaften von affinen und projektiven Ebenen

Genauer genommen wird hier ausschließlich jener Fall behandelt, in dem diese Objekte endlich sind. Die Existenz solcher ist bis heute nur für Primzahlenpotenzen q gesichert. Deshalb werden endliche affine und projektive Ebenen normalerweise über einen endlichen Körper $\mathbb{F}_q$ definiert.

Über den ganzen Abschnitt fortwährend wird eine affine bzw. projektive Ebene der Ordnung $m \in \mathbb{N}$ mit der Dimension $n \geq 2$ mit $\mathrm{AG}(n, m)$ bzw. $\mathrm{PG}(n, m)$ abgekürzt. Für solche, die über einen endlichen Körper $\mathbb{F}_q$ - mit q einer Primzahlpotenz - definiert sind, wird auch die Kurzschreibweise $\mathrm{AG}(n, \mathbb{F}_q)$ bzw. $\mathrm{PG}(n, \mathbb{F}_q)$ verwendet. Nun sollen diese Konstrukte klar definiert werden.

Definition 3.1 (Projektive Ebene)**.** Eine *projektive Ebene* besteht aus einer Menge von *Punkten* $\mathcal{P}$, einer Menge von *Geraden* $\mathcal{G}$ und einer sog. *Inzidenzrelation* $\mathcal{I}$. Letztere beschreibt den Zusammenhang zwischen Punkten und Geraden, d.h. welche Punkte auf welchen Geraden liegen und sie soll folgende Eigenschaften besitzen:

(P1) Je zwei verschiedene Geraden schneiden sich in genau einem Punkt.

(P2) Je zwei verschiedene Punkte liegen auf genau einer Geraden.

(P3) Es existieren zumindest vier Punkte, von denen keine drei auf einer Geraden liegen.

Die Gerade g, welche durch zwei Punkte p_1, p_2 festgelegt ist, wird stets als $g = p_1 \vee p_2$ notiert. Für den Schnittpunkt p zweier Geraden g_1 und g_2 schreibt man $p = g_1 \wedge g_2$.

Bemerkung 3.2. In Definition 3.1 herrscht *Dualität* zwischen den Begriffen *Punkt* und *Gerade*. Das heißt, vertauscht man diese Begriffe, bleiben die ersten zwei Forderungen auf jeden Fall gültig und die dritte folgt aus diesen beiden. Damit genügt es z.B. Aussagen über Punkte für Geraden zu zeigen und umgekehrt.

Wegen (P3) weiß man nämlich, dass vier Punkte p_1, p_2, p_3, p_4 existieren, von denen keine drei auf einer Geraden liegen. Nun kann man als Konsequenz von (P2) die (eindeutigen) Geraden $p_1 \vee p_2,\ p_1 \vee p_3,\ p_2 \vee p_4,\ p_3 \vee p_4$ bilden. Von diesen vier Geraden verlaufen keine drei durch den selben Punkt.

Weiters lässt sich folgendes Resultat zeigen, welches notwendig ist, um den Begriff der *Ordnung* einzuführen.

Satz und Definition 3.3 (Ordnung einer projektiven Ebene)**.** *Sei* $\Pi = (\mathcal{P}, \mathcal{G}, \mathcal{I})$ *eine endliche projektive Ebene. Dann existiert ein* $m \in \mathbb{N}$*, sodass jeder Punkt genau auf* $m+1$ *Geraden liegt. Gleichzeitig liegen auch auf jeder Geraden genau* $m+1$ *Punkte. Darüber hinaus besitzt* Π *genau* $m^2 + m + 1$ *Punkte und auch gleich viele Geraden.*

Dieses m *nennt man Ordnung der projektiven Ebene* Π*.*

Beweis. (Aus [3].)
Zuerst soll gezeigt werden, dass auf jeder Geraden gleich viele Punkte liegen. Dafür betrachte man die zwei Geraden g und h in $\mathcal{G}$, wobei $g \neq h$. Die Existenz dieser ist durch (P3) gesichert. Weiters seien a, b, c, d paarweise verschiedene Punkte aus $\mathcal{P}$, sodass keine 3 von ihnen auf einer gemeinsamen Geraden liegen. Diese müssen - auch wegen (P3) - existieren.

Nun konstruiert man einen Punkt $q \in \mathcal{P}$, welcher weder auf g noch auf h liegt. Es ist entweder solch ein q bereits in $\{a, b, c, d\}$ enthalten, oder man kann annehmen, dass o.B.d.A. a und b auf g und c und d auf h liegen. Seien weiters

$$\bar{g} := a \vee c \qquad \text{und} \qquad \bar{h} := b \vee d. \tag{3}$$

Es folgt sofort, dass $\bar{g} \neq \bar{h}$, da ja keine 3 der Punkte a, b, c, d auf der selben Geraden liegen. Deshalb kann man ruhigen Gewissens $q = \bar{g} \wedge \bar{h}$ definieren.

Es liegt nun q nicht auf g, da sich ansonsten g und $\bar{g}$ wegen (3) bereits in zwei Punkten a und q schneiden würden, also $g = \bar{g}$. Damit liegt aber auch c auf g, im Widerspruch dazu, dass a, b, c nicht auf einer gemeinsamen

Geraden liegen können. Analog zeigt man, dass h nicht durch q verläuft.

Seien nun $[g] := \{p \in P \mid p \text{ liegt auf } g\}$ und $[h] := \{p \in P \mid p \text{ liegt auf } h\}$. Die Abbildung ϕ sei definiert durch

$$\begin{aligned} \phi : [g] &\longrightarrow [h] \\ u &\longmapsto (u \vee q) \wedge h. \end{aligned}$$

Diese Definition ist sicherlich sinnvoll, da $q \notin [g]$, $q \notin [h]$ und deshalb auch $u \vee q \neq h$ gilt. Offensichtlich ist ϕ bijektiv. Das bedeutet, dass $[g]$ und $[h]$ gleich viele Elemente besitzen. Also liegen auf jeder Geraden gleich viele Punkte. Dass durch jeden Punkt gleich viele Geraden verlaufen, ergibt sich aus der Dualität. Diese Anzahl wird mit $m + 1$ bezeichnet. Dass tatsächlich $m \in \mathbb{N}$ gilt, wird erst am Ende des Beweises ersichtlich.

Die Anzahl der Punkte (bzw. gleichzeitig auch der Geraden) in Π lässt sich wie folgt ermitteln. Seien g, h zwei verschiedene Geraden durch den fix gewählten Punkt $p \in \mathcal{P}$. Es gilt dann

$$[g] \setminus \{p\} \cap [h] \setminus \{p\} = \emptyset.$$

$\mathcal{P} \setminus \{p\}$ lässt sich nun als disjunkte Vereinigung von $m + 1$ Mengen mit der Mächtigkeit m wie folgt schreiben

$$\mathcal{P} \setminus \{p\} = \dot{\bigcup_{g \text{ verläuft durch } p}} [g] \setminus \{p\}.$$

Also gilt $|\mathcal{P}| - 1 = (m+1)m$. Da weiters wegen (P3) $|\mathcal{P}| \geq 4$ gilt, folgt, dass $m \geq 1$ und deshalb gilt auch $m \in \mathbb{N}$. □

Bemerkung 3.4. Im Anfangsteil des Beweises von Satz 3.3 wurde unter anderem auch gezeigt, dass zu zwei verschiedenen Geraden einer projektiven Ebene stets ein Punkt existiert, der auf keiner dieser Geraden liegt.

Ein Beispiel für eine projektive Ebene der Ordnung 2 ist die sogenannte *Fano-Ebene*. Diese wird in Abb. 3 dargestellt.

Definition 3.5 (Affine Ebene)**.** Eine *affine Ebene* besteht aus einer Menge von *Punkten* $\mathcal{P}$ und einer Menge von *Geraden* $\mathcal{G}$, sowie einer *Inzidenzrelation* $\mathcal{I}$, die folgenden Axiomen unterliegt:

(A1) Je zwei verschiedene Punkte liegen auf genau einer Geraden.

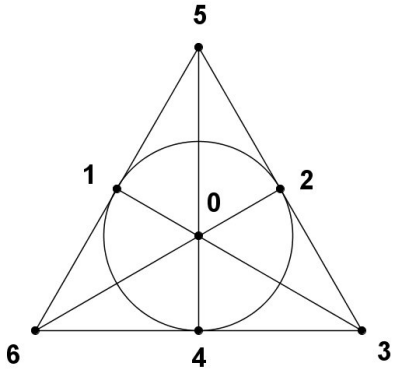

Abbildung 3: Projektive Ebene der Ordnung 2 (Fano-Ebene).

(A2) Zu jedem Punkt p, der nicht auf der Geraden g liegt, existiert eine eindeutige Gerade h, welche durch p verläuft und g nicht schneidet (*Parallelität*).

(A3) Es existieren zumindest drei verschiedene Punkte, die nicht alle auf einer Geraden liegen.

Dabei ist zu beachten, dass in (A2) der wesentliche Unterschied zwischen projektiven und affinen Ebenen liegt. Im projektiven Fall schneiden sich alle Geraden, hingegen es im affinen Fall parallele Geraden gibt.

Der Beweis des nächsten Satzes muss an dieser Stelle noch ausgelassen werden, da hierzu noch Resultate aus Abschnitt 3.2 benötigt werden. Dennoch ist es durchaus sinnvoll, bereits hier den Begriff der *Ordnung* einer affinen Ebene einzuführen.

Satz und Definition 3.6 (Ordnung einer affinen Ebene)**.** *Sei $\Sigma = (\mathcal{P}, \mathcal{G}, \mathcal{I})$ eine affine Ebene. Dann existiert ein $m \in \mathbb{N}$, sodass jede Gerade aus $\mathcal{G}$ genau durch m Punkte aus $\mathcal{P}$ verläuft. Weiters liegt jeder Punkt $p \in \mathcal{P}$ auf genau $m+1$ Geraden. Darüber hinaus gilt $|\mathcal{P}| = m^2$ und $|\mathcal{G}| = m^2 + m$.*

Dieses m nennt man Ordnung der affinen Ebene Σ.

Beweis. Der Beweis erfolgt erst auf Seite 26. □

Da nun bekannt ist, was man unter der Ordnung einer affinen Ebene versteht, ist es an der Zeit ein Beispiel für eine solche anzugeben. In Abb. 4 findet der Leser eine Möglichkeit, wie die affine Ebene $\mathrm{AG}(2,2)$ aussehen kann.

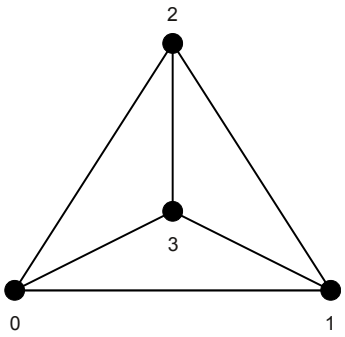

Abbildung 4: Affine Ebene der Ordnung 2, AG(2, 2).

3.2 Die Zusammenhänge zwischen affinen Ebenen, projektiven Ebenen und MOLS

Es ist prinzipiell möglich eine projektive Ebene aus einer affinen und umgekehrt zu konstruieren. Diese Tatsache wird im nächsten Satz festgehalten.

Satz 3.7. *Sei* $\Pi = (\mathcal{P}, \mathcal{G}, \mathcal{I})$ *eine endliche projektive Ebene und weiters sei* g_∞ *eine beliebige Gerade in* Π. *Dann ist durch*

$$\Sigma = (\mathcal{P} \setminus [g_\infty], \mathcal{G} \setminus \{g_\infty\}, \mathcal{I})$$

eine affine Ebene gegeben, wobei $[g] := \{p \in \mathcal{P} \mid p \text{ liegt auf } g\}$.

Umgekehrt lässt sich stets aus einer endlichen affinen Ebene Σ *durch Hinzunahme einer "unendliche Geraden", der sog. Ferngeraden* g_∞ *sowie deren Punkte eine projektive Ebene* Π *erzeugen.*

Beweis. (Aus [4].)
Sei nun also die endliche projektive Ebene $\Pi = (\mathcal{P}, \mathcal{G}, \mathcal{I})$ gegeben. Da zwei verschiedene Punkte p_1 und p_2 aus $\mathcal{P}$ stets eine eindeutige Gerade festlegen und die Gerade g_∞ mitsamt ihren Punkten aus Π entfernt wurde, wird diese Eigenschaft auf Σ übertragen.

Für den Beweis der Parallelität betrachte man eine beliebige Gerade g aus Σ. Sei weiters q der Schnittpunkt von g mit g_∞ in Π. Für jeden Punkt p aus Σ mit $p \notin [g]$ ist nun die Gerade $h = p \vee q$ die Parallele zu g durch p.

In Π existieren per Definition zumindest vier Punkte $\{a, b, c, d\}$, von denen keine drei auf einer Geraden liegen. Somit können von diesen höchstens zwei auf g_∞ liegen. Schließlich folgt mit Bemerkung 3.4 die Existenz von drei Punkten in Σ, welche nicht durch eine Gerade verbunden sind.

Geht man nun von einer affinen Ebene Σ aus, lässt sich daraus auch eine projektive Ebene Π erzeugen. Hierzu teilt man die Geraden aus Σ in sog. *Parallelklassen* ein. Dabei werden alle zueinander parallelen Geraden in einer Klasse zusammengefasst. Sei $\mathcal{S}$ eine beliebige Parallelklasse. Jeder Geraden aus $\mathcal{S}$ wird nun ein neuer Punkt hinzugefügt, welcher noch nicht in Σ vorhanden ist. Anschließend werden diese Punkte zur Ferngeraden g_∞ zusammengefasst.

Dass nun zwei Punkte eine eindeutige Gerade definieren wird von allen ursprünglich vorhandenen Punktepaaren sowieso erfüllt. Zwei Punkte aus $[g_\infty]$ können wegen der Konstruktion ohnehin nur g_∞ selbst festlegen. Schließlich sind noch Paare der Form $\{p, q\}$ mit $p \in \mathcal{P}$ und $q \in [g_\infty]$ zu betrachten. Die Existenz der Verbindungsgeraden ist erneut durch die Konstruktion gesichert und die Eindeutigkeit dieser ist aufgrund der Tatsache gegeben, dass jede Parallelkasse einen verschiedenen neuen Punkt zugewiesen bekommen hat.

Weiters schneiden sich zwei Geraden verschiedener Parallelklassen in genau einem Punkt, auch nachdem die neuen Punkte hinzugefügt wurden. Innerhalb solch einer Klasse ist der eindeutige Schnittpunkt durch den, für diese Klasse gewählten Punkt aus $[g_\infty]$ gegeben.

Schließlich kann man den drei Punkten aus Σ, welche nicht auf einer Geraden liegen einen vierten aus $[g_\infty]$ hinzufügen, sodass man eine projektive Ebene erhält. □

Jetzt ist man auch in der Lage Satz 3.6 zu beweisen:

Beweis. (Aus [4].)
Aus Satz 3.3 ist bekannt, dass jeder Punkt einer projektiven Ebene auf genau $m + 1$ Geraden liegt. Diese Eigenschaft geht beim Übergang auf eine affine Ebene wie in Satz 3.7 natürlich nicht verloren, da die Ferngerade mitsamt

ihrer Punkte entfernt wird.

Die Anzahl der Punkte auf jeder Geraden erhält man, indem man sich in Erinnerung ruft, dass diese im projektiven Fall mit $m + 1$ gegeben war. Mit Ausnahme der Ferngerade, die ohnehin entfernt wird, enthält jede Gerade genau einen Punkt auf g_∞. Also liegen genau m Punkte auf jeder Geraden.

Da man, wie bereits erwähnt, beim Übergang von einer projektiven zu einer affinen Ebene die Ferngerade sowie alle $m + 1$ Punkte auf ihr entfernt, gibt es in Σ genau m^2 Punkte und $m^2 + m$ Geraden. □

Wie zu Anfang dieses Kapitels schon kurz angemerkt wurde, kann man die Existenz einer projektiven Ebene und - wegen Satz 3.7 - auch die einer affinen Ebene für eine Primzahlenpotenzordnung q garantieren. Diese Tatsache soll nun im nächsten Abschnitt dargelegt werden.

3.2.1 Affine und projektive Ebenen über dem Körper $\mathbb{F}_q$

An erster Stelle stehen hierbei wieder einige Anzahlaussagen, welche die eigentliche Existenzaussage erleichtern sollen.

Lemma 3.8. *Sei q eine Primzahlpotenz und sei weiters $\mathbb{F}_q$ ein Körper mit q Elementen. Dann gilt*

i. Es existieren genau q^2 Punkte der Form $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$.

ii. Es existieren genau $q^2 + q$ Geraden.

iii. Auf jeder Geraden liegen genau q Punkte.

iv. Jeder Punkt liegt auf genau $q + 1$ Geraden.

Beweis. (Aus [1].)

i. Im Tupel (x, y) gibt es sowohl für x als auch für y genau q verschiedene Möglichkeiten und daher insgesamt genau q^2 verschiedene Punke.

ii. Hierfür betrachte man zuerst alle möglichen linearen Gleichungen der Form

$$y = mx + b \tag{4}$$

mit $m, b \in \mathbb{F}_q$. Für das Paar (m, b) gibt es hierbei wiederum insgesamt q^2 Möglichkeiten, also q^2 Geraden.

Nun gibt es noch Gleichungen der Form

$$x = k \tag{5}$$

für $k \in \mathbb{F}_q$. Nachdem man für dieses k nun q verschiedene Werte wählen kann erhält man insgesamt $q^2 + q$ verschiedene Geraden.

iii. Auf Geraden der Form (5) liegen ausschließlich Punkte der Form (k, r), $r \in \mathbb{F}_q$, also genau q verschiedene Punkte. Da auch Gleichungen der Art (4) jedem x-Wert einen eindeutigen y-Wert zuweisen, gibt es in diesem Fall genau q Punkte auf der Geraden.

iv. Dazu betrachte man den beliebigen Punkt (s, t). Dieser liegt mit Sicherheit auf der Geraden $x = s$. Alle anderen Geraden durch diesen Punkt sind vom Typ (4), also $y = mx + b$. Fixiert man nun ein m existiert dazu genau ein $b = t - ms$, sodass $t = ms + b$ gilt. Damit gibt es also genau q weitere Geraden, welche durch den Punkt (s, t) gehen.

□

Nun ist es endlich an der Zeit sich Gedanken zu machen, wie man solche Ebenen konstruieren kann. Der nächste Satz demonstriert, wie man von einem endlichen Körper ausgehend eine affine Ebene erzeugt.

Satz 3.9. *Sei $\mathbb{F}_q$ ein endlicher Körper. Weiters seien $\mathcal{P} = \{(x, y) \mid x, y \in \mathbb{F}_q\}$ und $\mathcal{G}$ so, dass*

$$g \in \mathcal{G} \Longleftrightarrow g = \{(x, y) \in \mathcal{P} \mid ax + by + c = 0\}$$

für bestimmte $a, b, c \in \mathbb{F}_q$ mit a, b nicht beide gleich 0. Dann bilden $\mathcal{P}$ und $\mathcal{G}$ zusammen mit der natürlichen Inzidenzrelation eine affine Ebene $AG(2, \mathbb{F}_q)$.

Beweis. (Aus [1].)

(A1) Es soll gezeigt werden, dass zwei verschiedene Punkte $s = (s_1, s_2)$ und $t = (t_1, t_2)$ eine Gerade auf eindeutige Weise bestimmen. Dazu betrachte man

$$(y - s_2)(t_1 - s_1) = (x - s_1)(t_2 - s_2) \tag{6}$$

bzw. äquivalent dazu

$$(t_1 - s_1)y + (s_2 - t_2)x + \big(s_1(t_2 - s_2) - s_2(t_1 - s_1)\big) = 0. \tag{7}$$

Da $s \neq t$ können in Gleichung (7) die Koeffizienten von x und y nicht beide gleichzeitig 0 sein. Deshalb beschreibt sie tatsächlich eine Gerade. Aus (6) ist sofort ersichtlich, dass sowohl s als auch t auf dieser Geraden liegen. Damit ist die Existenz gesichert.

Sei nun g eine beliebige Gerade durch s und t. Aus vorherigem Lemma 3.8 folgt, dass noch $q-2$ weitere verschiedene Punkte $p_1, \ldots, p_{q-2}$ auf g liegen, durch die wiederum jeweils $q+1$ verschiedene Geraden verlaufen. Damit hat man insgesamt bereits

$$\underbrace{(q+1)}_{\text{Geraden durch } s} + \underbrace{(q+1)}_{\text{Geraden durch } t} + (q-2)(q+1) = q^2+q$$

verschiedene Geraden. Hätte man nun eine weitere Gerade g' durch s und t, dann würde diese zweimal gezählt werden und somit wäre die Anzahl der Geraden höchstens q^2+q-1, im Widerspruch zu Lemma 3.8.

(A2) Sei nun p ein Punkt, welcher nicht auf der Gerade g liegt. Gesucht wird jetzt eine Gerade h, die durch p läuft, dabei aber g nicht schneidet.

Die q Punkte, die auf g liegen, werden mit $p_1, \ldots, p_q$ bezeichnet. Für jedes $1 \leq i \leq q$ gibt es nun genau eine Gerade, welche sowohl durch p als auch p_i verläuft. Aus Lemma 3.8 ist jedoch bekannt, dass es insgesamt $q+1$ verschiedene Geraden durch p gibt. Daher existiert genau eine Gerade h, die nicht mit g inzidiert.

(A3) Für den Beweis der Gültigkeit des letzten Axioms betrachtet man die Punkte $(0,0), (0,1), (1,0)$, sowie $(1,1)$. Eine Gerade durch 3 dieser Punkte würde zumindest $(0,0)$ und $(0,1)$ oder $(1,0)$ und $(1,1)$ enthalten. Das erste Paar hat aber als bestimmende Gleichung $x = 0$ und das zweite $x = 1$. Deshalb können keine drei dieser Punkte auf der selben Geraden liegen.

□

Als direkte Konsequenz des Satzes 3.9 und Satz 3.7 erhält man folgendes Korollar.

Korollar 3.10. *$PG(2, \mathbb{F}_q)$ und $AG(2, \mathbb{F}_q)$ existieren beide, falls q eine Primzahlpotenz ist.*

Schlussendlich wurden alle Hilfsmittel vorgestellt, mit denen man den Sprung von der affinen Ebene $\mathrm{AG}(2, \mathbb{F}_q)$ zur projektiven Ebene $\mathrm{PG}(2, \mathbb{F}_q)$ und zurück wagen kann. Aufgrund von Satz 3.7 kann man dazu wie folgt vorgehen:

1. Man benenne alle Punkte (x, y) in $\mathrm{AG}(2, \mathbb{F}_q)$ in $(x, y, 1)$ um.
2. Für die Geraden verwende man die Gleichung $ax + by + cz = 0$, wobei $(a, b) \neq (0, 0)$.
3. Definiere die sog. *Ferngerade* $g_\infty = \{(1, 0, 0)\} \cup \{(x, 1, 0) \mid x \in \mathbb{F}_q\}$.
4. $\mathcal{P}'$ sei nun die Vereinigung von $\mathcal{P}$ mit den Punkten auf g_∞.
5. Man setze schließlich $\mathcal{G}' = \mathcal{G} \cup \{g_\infty\}$.
6. $(\mathcal{P}', \mathcal{G}', \mathcal{I}')$ ist nun die projektive Ebene $\mathrm{PG}(2, \mathbb{F}_q)$.

Diese Konstruktionsmethoden sollen nun gleich anhand eines Beispiels erprobt werden.

Beispiel 3.11. Es wird der Fall $q = 2$ betrachtet. Da $\mathbb{F}_2$ aus zwei Elementen besteht, erhält man 4 verschiedene Punkte und 6 verschiedene Geraden. Die Inzidenzrelation ist in Tabelle 3 dargestellt.

Gerade	Gleichung	Punkte
g_1	$x + y = 0$	$(0, 0), (1, 1)$
g_2	$x + y - 1 = 0$	$(0, 1), (1, 0)$
g_3	$x = 0$	$(0, 0), (0, 1)$
g_4	$y = 0$	$(0, 0), (1, 0)$
g_5	$x - 1 = 0$	$(1, 0), (1, 1)$
g_6	$y - 1 = 0$	$(0, 1), (1, 1)$

Tabelle 3: Inzidenzrelation für $\mathrm{AG}(2, \mathbb{F}_2)$.

Wie oben beschrieben, werden der affinen Ebene nun bei allen Punkten eine dritte Koordinate 1, die zusätzlichen Punkte $(0, 1, 0), (1, 0, 0), (1, 1, 0)$, sowie die Ferngerade g_∞ hinzugefügt und die Gleichungen in die Form $ax+by+cz = 0$ übergeführt. Dies wird in Tabelle 4 festgehalten.

3.2.2 Der Hauptsatz über affine Ebenen und MOLS

Satz 3.7 bestätigte bereits einen engen Zusammenhang zwischen affinen und projektiven Ebenen. Wie zu Anfang dieses Kapitels erwähnt wurde, gibt es auch zwischen affinen Ebenen (und somit gleichzeitig mit projektiven) und vollständigen Kollektionen von MOLS eine $1 : 1$ Relation. Dieses bedeutende Resultat wird in Satz 3.12 festgehalten.

Gerade	Gleichung	Punkte
g_1	$x+y=0$	$(0,0,1),(1,1,0),(1,1,1)$
g_2	$x+y+z=0$	$(0,1,1),(1,0,1),(1,1,1)$
g_3	$x=0$	$(0,0,1),(0,1,0),(0,1,1)$
g_4	$y=0$	$(0,0,1),(1,0,0),(1,0,1)$
g_5	$x+z=0$	$(0,1,0),(1,0,1),(1,1,1)$
g_6	$y+z=0$	$(0,1,1),(1,0,0),(1,1,1)$
g_∞	$z=0$	$(0,1,0),(1,0,0),(1,1,0)$

Tabelle 4: Inzidenzrelation für $\mathrm{PG}(2,\mathbb{F}_2)$.

Satz 3.12 (Bose 1938)**.** *Es existieren genau dann $n-1$ MOLS der Ordnung n, wenn es eine affine Ebene der Ordnung n gibt.*

Beweis. (Aus [8].)
Angenommen es existiert eine affine Ebene der Ordnung n. Aus dieser sollen nun $n-1$ MOLS $L_0,\dots L_{n-2}$ der Ordnung n erzeugt werden. Zu diesem Zweck teilt man die n^2+n Geraden in $n+1$ Parallelklassen $P_0,\dots,P_n$ ein.

Natürlich schneiden sich zwei Geraden aus verschiedenen Parallelklassen in genau einem Punkt. Die Geraden aus P_i werden von nun an mit $g_{i,j}$ bezeichnet, wobei $0\le i\le n$ und $0\le j\le n-1$.

Die lateinischen Quadrate werden nach folgender Formel erzeugt:

$$L_x(i,j)=k \qquad \Longleftrightarrow \qquad g_{n-1,i}\wedge g_{n,j}\in[g_{x,k}]. \tag{8}$$

wobei $0\le x\le n-2$ sowie $0\le i,j\le n-1$ und $L_x(i,j)$ den Eintrag an der Position (i,j) im Quadrat L_x bezeichnet.

Diese so konstruierten Quadrate L_x sind in der Tat lateinische, denn angenommen ein Symbol k sowie eine Zeile i sind gegeben. Dann soll man einen eindeutigen Spaltenindex j finden, sodass $L_x(i,j)=k$. Da sich Geraden aus verschiedenen Parallelklassen in einem eindeutigen Punkt schneiden, gibt es genau ein $y=g_{n-1,i}\wedge g_{x,k}$. Dann existiert auch ein eindeutiges j, sodass $y\in[g_{n,j}]$, da ja P_n eine Parallelklasse ist, und somit gilt $L_x(i,j)=k$.

Nun seien ein Symbol k und eine Spalte j vorgegeben. Aus dem selben Argument wie im obigen Absatz existiert genau ein $y=g_{n,j}\wedge g_{x,k}$ und weiters genau ein i mit $y\in[g_{n-1,i}]$, was wieder $L_x(i,j)=k$ zur Folge hat. Damit wurde gezeigt, dass es sich bei $L_0,\dots,L_{n-2}$ tatsächlich um lateinische Quadrate handelt.

Im nächsten Schritt soll bewiesen werden, dass je zwei dieser $n-1$ Quadrate orthogonal sind. Dafür nimmt man $x \neq y$ an und betrachtet L_x und L_y. Seien l und k zwei beliebige Symbole. Zu diesen soll nun eine eindeutige Position (i, j) gesucht werden, sodass folgendes gilt

$$L_x(i,j) = k$$
$$L_y(i,j) = l.$$

Wegen der Konstruktion nach (8) ist dies äquivalent zu

$$g_{n-1,i} \wedge g_{n,j} \in [g_{x,k}]$$
$$g_{n-1,i} \wedge g_{n,j} \in [g_{y,l}].$$

Da $g_{x,k}$ und $g_{y,l}$ verschiedenen Parallelklassen entstammen, schneiden sie sich in einem einzigen Punkt z. Da P_{n-1} bzw. P_n Parallelklassen sind, existiert ein eindeutiges i bzw. j, sodass $z \in [g_{n-1,i}]$ bzw. $z \in [g_{n,j}]$. Damit wurde die gewünschte Position (i, j) gefunden und zwar auf eindeutige Weise. Also sind L_x und L_y orthogonal, falls $x \neq y$.

Andererseits, nimmt man an, es existieren $n-1$ MOLS $L_0, \ldots, L_{n-2}$ der Ordnung n, dann lässt sich daraus eine affine Ebene der Ordnung n konstruieren. Die Punktmenge $\mathcal{P}$ ist hierbei $\{0, \ldots, n-1\} \times \{0, \ldots, n-1\}$. Die Geraden werden dem nachstehenden Prinzip entsprechend gebildet. Seien dafür $0 \leq x \leq n-2$ und $0 \leq k \leq n-1$.

$$g_{x,k} = \{(i,j) \mid L_x(i,j) = k\} \tag{9}$$
$$g_{n-1,k} = \{(k,j) \mid 0 \leq j \leq n-1\} \tag{10}$$
$$g_{n,k} = \{(i,k) \mid 0 \leq i \leq n-1\} \tag{11}$$

Die letzten beiden Typen lassen sich dabei als Geraden, die über die kanonischen Spalten- bzw. Zeilen-Quadrate definiert sind, auffassen.

Nun setzt man $\mathcal{G} = \{g_{x,k} \mid 0 \leq x \leq n, 0 \leq k \leq n-1\}$. Klarer Weise existieren n^2 verschiedene Punkte in $\mathcal{P}$. Weiters liegen auch genau n Punkte auf jeder Geraden und die Anzahl aller konstruierten $g_{i,j}$ beträgt natürlich n^2+n.

Man fixiere nun die beiden Punkte $(i_1, j_1) \neq (i_2, j_2)$. Falls $i_1 = i_2$, dann liegt dieses Punktepaar auf g_{n-1,i_1} und sonst auf keiner Geraden. Ist $j_1 = j_2$, dann findet man das Paar nur auf g_{n,j_1}. Also kann $i_1 \neq i_2$ und $j_1 \neq j_2$ angenommen werden.

Seien $(x_1, k_1) \neq (x_2, k_2)$ so, dass (i_1, j_1) und (i_2, j_2) beide auf den Geraden g_{x_1,k_1} und g_{x_2,k_2} liegen. Das heißt

$$\begin{aligned} L_{x_1}(i_1, j_1) &= k_1 \\ L_{x_1}(i_2, j_2) &= k_1 \\ L_{x_2}(i_1, j_1) &= k_2 \\ L_{x_2}(i_2, j_2) &= k_2. \end{aligned}$$

Damit sieht man sofort, dass, sollte $x_1 = x_2$ sein, dann wäre $k_1 = k_2$ und damit die Tupel nicht verschieden. Deshalb wird $x_1 \neq x_2$ vorausgesetzt. Nun enthält aber die Überlagerungsmatrix von L_{x_1} und L_{x_2} das Paar (k_1, k_2) an den verschiedenen Positionen (i_1, j_1) und (i_2, j_2) und diese beiden lateinischen Quadrate sind somit nicht orthogonal. Das ist ein Widerspruch.

Somit ist garantiert, dass jedes Paar von Punkten höchstens einmal gemeinsam auf einer Geraden liegt. Die Anzahl der verschiedenen Geraden beträgt genau $n^2 + n$ und die Anzahl aller möglichen Punktepaare $\binom{n^2}{2}$. Dabei gilt für $n \geq 2$ stets

$$\binom{n^2}{2} = \frac{1}{2}n^2(n^2 - 1) \geq n^2 + n.$$

Also liegt jedes Paar von Punkten genau einmal gemeinsam auf einer Geraden, welche sie somit eindeutig bestimmen.

Nun soll geprüft werden, ob es eine eindeutige Parallele zu einer beliebigen Geraden durch einen nicht inzidenten Punkt gibt. Dafür betrachte man zu allererst eine Gerade $g_{n,k}$ und den Punkt (i, j) mit $j \neq k$. Offenbar kann sich $g_{n,j}$ nicht mit $g_{n,k}$ schneiden, sie inzidiert jedoch mit $g_{n-1,i}$ im Punkt (i, k).

Liegt (i, j) auf der Geraden $g_{x,l}$ ist dies gleichbedeutend mit $L_x(i, j) = k$. Da aber L_x ein lateinisches Quadrat ist, folgt, dass es auch einen Punkt (r, k) gibt mit $L_x(r, k) = l$, welcher klarerweise auch auf $g_{n,k}$ liegt. Also ist $g_{n,j}$ die einzige Parallele zu $g_{n,k}$ durch den Punkt (i, j). Diese Vorgehensweise lässt sich auch für die Parallelität einer Geraden $g_{n-1,k}$ anwenden.

Sei nun (i, j) ein beliebiger Punkt, welcher nicht auf $g_{x,k}$, $0 \leq x \leq n - 2$, liegt, also $L_x(i, j) = l \neq k$. Das heißt, (i, j) kommt auf $g_{x,l}$ vor. Auf $g_{n,j}$ liegen alle Punkte der Form (r, j), $0 \leq r \leq n-1$. Da L_x ein lateinisches Quadrat ist,

muss k in jeder Spalte, insbesondere in der Spalte j genau einmal vorkommen. Somit schneiden sich die beiden Geraden. Ähnliches gilt natürlich auch für $g_{n-1,i}$. Nimmt man nun an, dass es ein $y \neq x$, $0 \leq y \leq n-2$ gibt, sodass für passendes l $(i,j) \in [g_{y,l}]$ zutrifft, dann muss aufgrund der Orthogonalität das Tupel (k,l) genau einmal in der Überlagerungsmatrix von L_x und L_y vorkommen. Somit hat man auch zwischen $g_{x,k}$ und $g_{y,l}$ einen Schnittpunkt gefunden und es folgt, dass $g_{x,l}$ die eindeutige Parallele ist.

Das letzte zu überprüfende Axiom (A3) verlangt die Existenz von 4 Punkten, von denen keine 3 auf einer Geraden liegen. Zu diesem Zweck betrachtet man die Punkte $(0,0),(0,1),(1,0),(1,1)$. Auf einer Geraden vom Typ $g_{x,k}$, $0 \leq x \leq n-2$ können keine drei liegen, da sonst in einer Zeile eines der lateinischen Quadrate ein Symbol doppelt vorkommen würde. Da in der ersten bzw. zweiten Position der Punkte auch immer nur zwei Werte gleich sind, können keine drei dieser Punkte auf $g_{n-1,k}$ bzw. $g_{n,k}$ liegen.

Also wurde auch gezeigt, dass sich aus $n-1$ MOLS der Ordnung n eine affine Ebene der Ordnung n konstruieren lässt und dies beendet den Beweis. □

Im nächsten Beispiel sollen die Methoden aus diesem Beweis demonstriert werden. Als erstes werden aus einer affinen Ebene der Ordnung $n = 3$ zwei MOLS derselben Ordnung generiert und anschließend aus diesen wieder eine affine Ebene gewonnen.

Beispiel 3.13. Die Punktmenge $\mathcal{P}$ und die Menge der Geraden $\mathcal{G}$ seien wie folgt gegeben

$$\begin{aligned}\mathcal{P} &= \{00,01,02,10,11,12,20,21,22\}\\ \mathcal{G} &= \{\{00,01,02\},\{10,11,12\},\{20,21,22\},\{00,10,20\},\{01,11,21\},\\ &\quad \{02,12,22\},\{00,11,22\},\{01,12,20\},\{02,10,21\},\{00,12,21\},\\ &\quad \{01,10,22\},\{02,11,20\}\}.\end{aligned}$$

Anschließend kann man die Geraden in ihre Parallelklassen einteilen und entsprechend bennenen. $g_{x,l}$ bezeichnet demnach die l-te Gerade in der Klasse x.

$$\begin{array}{llll} g_{0,0} = \{00,01,02\} & g_{1,0} = \{00,10,20\} & g_{2,0} = \{00,11,22\} & g_{3,0} = \{00,12,21\}\\ g_{0,1} = \{10,11,12\} & g_{1,1} = \{01,11,21\} & g_{2,1} = \{01,12,20\} & g_{3,1} = \{01,10,22\}\\ g_{0,2} = \{20,21,22\} & g_{1,2} = \{02,12,22\} & g_{2,2} = \{02,10,21\} & g_{3,2} = \{02,11,20\}\end{array}$$

Verwendet man die Terminologie aus obigem Beweis, kann man beispielsweise $(i, j) = (1, 2)$ setzen. Dann erhält man für $n = 3$

$$g_{n-1,1} \wedge g_{n,2} = g_{2,1} \wedge g_{3,2} = (2, 0).$$

In der Klasse 0 bzw. 1 kommt $(2, 0)$ auf der Geraden mit der Nummer 2 bzw. 0 vor. Also ist $L_0(1, 2) = 2$ und $L_1(1, 2) = 0$. Führt man dies fort, erhält man die beiden MOLS

$$L_0 = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix} \qquad \text{und} \qquad L_1 = \begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}.$$

Nun soll dieser Prozess rückgängig gemacht werden. Die Punktmenge $\mathcal{P}$ ist natürlich die selbe wie oben. Die Geraden konstruiert man analog zum obigen Beweis für $0 \leq k \leq 2$ wie folgt

$$g_{x,k} = \begin{cases} \{(i, j) \mid L_x(i, j) = k\} & \text{für } 0 \leq x \leq 1 \\ \{(k, j) \mid 0 \leq j \leq 2\} & \text{für } x = 2 \\ \{(i, k) \mid 0 \leq i \leq 2\} & \text{für } x = 3 \end{cases}.$$

Somit bekommt man zum Beispiel die Gerade $g_{0,2}$ mittels

$$g_{0,2} = \{(i, j) \mid L_0(i, j) = 2\} = \{(0, 1), (1, 2), (2, 0)\}.$$

Nun kann man alle mit obiger Formel berechneten Geraden auflisten und erhält wiederum die oben angeführten Ausgangsgeraden bis auf Indexverschiebungen.

$$\begin{array}{llll} g_{0,0} = \{00, 11, 22\} & g_{1,0} = \{00, 12, 21\} & g_{2,0} = \{00, 01, 02\} & g_{3,0} = \{00, 10, 20\} \\ g_{0,1} = \{02, 10, 21\} & g_{1,1} = \{02, 11, 20\} & g_{2,1} = \{10, 11, 12\} & g_{3,1} = \{01, 11, 21\} \\ g_{0,2} = \{01, 12, 20\} & g_{1,2} = \{01, 10, 22\} & g_{2,2} = \{20, 21, 22\} & g_{3,2} = \{02, 12, 22\} \end{array}$$

Eine direkte Konsequenz von Satz 3.12 zusammen mit Korollar 3.10 ist folgendes:

Korollar 3.14. *Sei $n \geq 2$ eine natürliche Zahl. Dann sind folgende Aussagen äquivalent:*

i. Es existieren $n-1$ paarweise orthogonale lateinische Quadrate der Ordnung n.

ii. Es existiert eine affine Ebene der Ordnung n.

iii. Es existiert eine projektive Ebene der Ordnung n.

Satz 3.12 lässt wieder viel Raum für Vermutungen und offene Probleme. Erinnert man sich zurück an die *Prime Power Conjecture* (Vermutung 2.19 auf Seite 12) lässt sich diese nun auf die folgende Vermutung erweitern:

Vermutung 3.15 (Prime Power Conjecture für affine und projektive Ebenen)**.** *Folgende Aussagen sind äquivalent:*

i. n ist eine Primzahlenpotenz.

ii. Es existieren $n-1$ MOLS der Ordnung n.

iii. Es existiert eine affine Ebene der Ordnung n.

iv. Es existiert eine projektive Ebene der Ordnung n.

4 $(0, m, s)$-Netze und deren Existenz

In diesem Abschnitt wird kurz die Theorie der (t, m, s)-Netze erläutert, um anschließend näher auf den Spezialfall $(0, m, s)$-Netze eingehen zu können. Dabei soll wieder ein Zusammenhang zu orthogonalen lateinischen Quadraten hergestellt werden, welcher die Existenz von $(0, m, s)$-Netzen in bestimmten Fällen garantiert.

4.1 (t, m, s)-Netze

Um diese mathematischen Objekte studieren zu können, definiert man sich spezielle Teilintervalle des s-dimensionalen Einheitswürfels $I^s := [0, 1)^s$, die sogenannten *elementaren Intervalle*.

Definition 4.1 (Elementares Intervall)**.** Seien $b, s \in \mathbb{N}, b \geq 2$ sowie $d_i, a_i \in \mathbb{N}_0$, sodass $0 \leq a_i < b^{d_i}$ für alle $1 \leq i \leq s$. Ein *elementares Intervall in Basis b* ist ein Intervall der Form

$$E = \prod_{i=1}^{s} \left[\frac{a_i}{b^{d_i}}, \frac{a_i + 1}{b^{d_i}} \right).$$

Bemerkung 4.2. Die Länge eines Faktors in obigem Produkt ist genau b^{-d_i} und somit gilt für den Inhalt jedes elementaren Intervalls

$$\lambda(E) = b^{-(d_1 + \ldots + d_s)}.$$

Beispiel 4.3. Beispielsweise erhält man für $b = s = d_1 = d_2 = 2$ sowie $a_1 = 1$ und $a_2 = 0$ nach Definition 4.1 als elementares Intervall

$$E = \left[\frac{a_1}{b^{d_1}}, \frac{a_1 + 1}{b^{d_1}} \right) \times \left[\frac{a_2}{b^{d_2}}, \frac{a_2 + 1}{b^{d_2}} \right) = \left[\frac{1}{4}, \frac{1}{2} \right) \times \left[0, \frac{1}{4} \right)$$

mit dem Inhalt

$$\lambda(E) = b^{-(d_1 + d_2)} = 2^{-4} = \tfrac{1}{16}.$$

Oftmals ist man daran interessiert, wie viele Elemente einer Punktmenge $\mathcal{P} = \{x_0, \ldots, x_{N-1}\}$ in einer vorgegebenen Menge $J \subset \mathbb{R}^s, s \in \mathbb{N}$ auftreten. Dies wird durch die Größe

$$A(J, N) = A(J, N, \mathcal{P}) = \#\{n \mid 0 \leq n \leq N - 1 \quad \wedge \quad x_n \in J\}$$

beschrieben.

Definition 4.4 ((t, m, s)-Netz nach [6]. Siehe dazu auch [2] bzw. [7].)**.** Seien $b \geq 2$, m und s natürliche Zahlen. Weiters sei $t \in \mathbb{N}_0$ mit $0 \leq t \leq m$. Ein *(t, m, s)-Netz in Basis b* ist eine Punktmenge $\mathcal{P}$ bestehend aus b^m Punkten in I^s, sodass in jedem elementaren Intervall E in Basis b mit Volumen $\lambda(E) = b^{t-m}$ genau b^t Punkte aus $\mathcal{P}$ liegen, also $A(E, b^m) = b^t$.

Heuristisch betrachtet gibt der Parameter s die Dimension an, m legt die Anzahl der Punkte fest und t bestimmt die Feinheit bezüglich der Verteilung der Punkte.

Es soll noch angemerkt werden, dass sich (t, m, s)-Netze gut zum Annähern des Volumens eines elementaren Intervalls E eigenen, weil

$$\left| \frac{A(E, b^m)}{b^m} - \lambda(E) \right| = \left| \frac{b^t}{b^m} - b^{t-m} \right| = 0.$$

Da zu einem späteren Zeitpunkt in diesem Dokument speziellere Fälle von (t, m, s)-Netzen genauer untersucht werden sollen, werden diese kurz vorgestellt.

Bemerkung 4.5. Ein $(0, m, s)$-Netz in Basis b ist nach Definition 4.4 also eine Punktmenge mit b^m Elementen in I^s. Für diese soll gelten, dass in jedem elementaren Intervall in Basis b mit Volumen b^{-m} genau $b^0 = 1$ Punkt liegt.

Beispiel 4.6. Ein $(0, 2, 2)$-Netz in Basis $b = 2$ besteht also aus $b^m = 2^2 = 4$ Punkten in I^2. Dabei soll in jedem elementaren Intervall in Basis 2 mit $\lambda(E) = b^{-m} = 2^{-2} = 1/4$ genau ein Punkt liegen. Ein Beispiel hierfür ist in Abb. 5 gegeben.

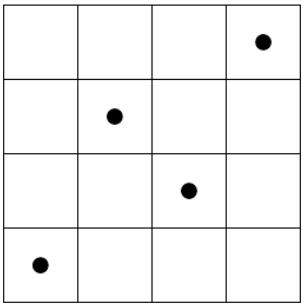

Abbildung 5: Beispiel eines $(0, 2, 2)$-Netzes.

Von nun an beschreibt die natürliche Zahl $b \geq 2$ eine beliebige Basis. Weiters seien $s \in \mathbb{N}$ die Dimension und m, t ganze Zahlen mit $0 \leq t \leq m$.

Im Folgenden werden nun einige Eigenschaften und Beziehungen zwischen diesen Netzen untereinander gezeigt.

Das erste Lemma hierzu besagt, dass eine Erhöhung der Feinheit eines (t, m, s)-Netzes $\mathcal{P}$ nichts an der Tatsache ändert, dass es sich weiterhin um ein solches Netz handelt.

Lemma 4.7. *Jedes (t, m, s)-Netz in Basis b ist auch ein (u, m, s)-Netz in Basis b für $t \leq u \leq m$.*

Beweis. (Aus [2] und [6].)
Sei E ein beliebiges elementares Intervall in I^s mit Volumen b^{u-m} in Basis b. Dieses kann man nun als disjunkte Vereinigung von elementaren Intervallen mit Volumen b^{t-m} in Basis b schreiben, also

$$E = \dot{\bigcup_{1 \leq n \leq b^{u-t}}} \prod_{i=1}^{s} \left[\frac{a_i^{(n)}}{b^{d_i^{(n)}}}, \frac{a_i^{(n)} + 1}{b^{d_i^{(n)}}} \right) \qquad \text{mit} \quad \sum_{i=1}^{s} d_i^{(n)} = m - t.$$

In jedem Intervall dieser Vereinigung liegen, da von einem (t, m, s)-Netz ausgegangen wurde, genau b^t Punkte, also insgesamt genau $b^{u-t} b^t = b^u$ Punkte in ganz E. Somit handelt es sich tatsächlich um ein (u, m, s)-Netz. □

Folgendes Lemma besagt, dass sich aus einem (t, m, s)-Netz in Basis b stets ein Netz in niedrigerer Dimension erzeugen lässt.

Lemma 4.8. *Sei $r \leq s$ eine natürliche Zahl und $i_1, \ldots, i_r$ eine beliebige Folge von r Elementen aus $\{1, \ldots, s\}$. Weiters sei $P : I^s \to I^r$ jene Projektion, die den Punkt $(\nu_1, \ldots, \nu_s)$ auf $(\nu_{i_1}, \ldots, \nu_{i_r})$ abbildet. Dann führt P jedes (t, m, s)-Netz in Basis b in ein (t, m, r)-Netz in Basis b über.*

Beweis. (Aus [2].)
O.B.d.A. betrachtet man nur jene Projektion, welche $(\nu_1, \ldots, \nu_s)$ in $(\nu_1, \ldots, \nu_r)$ überführt. Sei $\tilde{E}$ ein r-dimensionales, elementares Intervall in Basis b mit Volumen b^{t-m}. Betrachtet man nun $E = \tilde{E} \times [0, 1)^{s-r}$, dann sieht man sofort, dass $\lambda(E) = b^{t-m}$. Darum beinhaltet E genau b^t Punkte des (t, m, s)-Netzes.

An die letzten $s-r$ Koordinaten wurden jedoch keinerlei Einschränkungen gestellt und daher enthält $\tilde{E}$ genau b^t Punkte. Somit erhält man durch die Projektion P ein (t, m, r)-Netz in Basis b. □

Ausgehend von einem elementaren Intervall lässt sich auch der zweite Parameter m eines (t, m, s)-Netzes, also die Anzahl der Punkte variieren. Verwendet wird hierzu lediglich eine affine Transformation.

Lemma 4.9. *Seien $\mathcal{P}$ ein (t, m, s)-Netz und E ein elementares Intervall in Basis b mit $\lambda(E) = b^{-u}$, $0 \leq u \leq m - t$. Weiters sei $T : E \to I^s$ eine affine Transformation. Dann werden jene Punkte von $\mathcal{P}$, die in E liegen, von T in ein $(t, m - u, s)$-Netz in Basis b übergeführt.*

Beweis. (Aus [2] und [6].)
Erneut kann E als eine disjunkte Vereinigung von b^{m-t-u} elementarer Intervalle in Basis b geschrieben werden, wobei jedes dieser Intervalle den Inhalt b^{t-m} besitzt. Da $\mathcal{P}$ ein (t, m, s)-Netz ist, enthält E genau $b^{m-t-u}b^t = b^{m-u}$ Punkte aus P.

Wendet man nun T auf diese Punkte an, erhält man eine weitere Punktmenge $\mathcal{P}'$, welche aus b^{m-u} Elementen besteht. Sei jetzt E' ein beliebiges elementares Intervall in Basis b, sodass $\lambda(E') = b^{t-m+u}$. Betrachtet man einen Punkt $\mathbf{x} \in E$, dann gilt:

$$T(\mathbf{x}) \in E' \qquad \Longleftrightarrow \qquad \mathbf{x} \in T^{-1}(E')$$

Nun ist aber $T^{-1}(E')$ ein elementares Intervall in Basis b mit $\lambda(T^{-1}(E')) = b^{t-m}$. Da es sich bei $\mathcal{P}$ um ein (t, m, s)-Netz handelt, enthält $T^{-1}(E')$ genau b^t Punkte aus $\mathcal{P}$. Dies bedeutet wiederum, dass auch E' genau b^t Punkte aus $\mathcal{P}'$ enthält und somit ist $\mathcal{P}'$ ein $(t, m - u, s)$-Netz. □

Für spätere Zwecke ist das nachstehende Korollar noch von Bedeutung.

Korollar 4.10. *Falls ein $(0, m, s)$-Netz in Basis b existiert, dann gibt es auch ein $(0, 2, s)$-Netz in Basis b.*

Beweis. Ist ein unmittelbares Resultat von Lemma 4.9. □

Schließlich gibt es auch noch die Möglichkeit, die Basis b eines (t, m, s)-Netzes zu verändern, ohne die Netzeigenschaften wesentlich zu verändern.

Lemma 4.11. *Seien $t \in \mathbb{N}_0$, $t \leq m$ und $h \in \mathbb{N}$. Dann ist jedes (th, mh, s)-Netz in Basis b auch gleichzeitig ein (t, m, s)-Netz in Basis b^h.*

Beweis. (Aus [6].)
Per Definition besteht ein (th, mh, s)-Netz in Basis b aus genau b^{mh} Punkten. Dies ist aber auch genau die Anzahl von Punkten, die ein (t, m, s)-Netz in Basis b^h besitzen muss. Natürlich ist auch ein elementares Intervall E in Basis b^h mit $\lambda(E) = b^{ht-hm}$ ein elementares Intervall in Basis b mit dem Inhalt b^{ht-hm}. Also beinhaltet es genau b^{th} Punkte des (th, mh, s)-Netzes. □

4.2 Der Zusammenhang zwischen $(0, m, s)$-Netze und lateinischen Quadraten

Nun soll ein besonderes Augenmerk auf $(0, m, s)$-Netze gelegt werden. Das Studium dieser ist zuletzt nicht nur deswegen interessant, weil sie sich sehr gut für die sog. *Quasi-Monte Carlo Methode* eignen, sondern auch, da ihre Existenz wieder sehr stark mit der Existenz von paarweise orthogonalen lateinischen Quadraten und damit, wie aus Abschnitt 3.2 bereits bekannt ist, auch mit der Existenz von affinen und projektiven Ebenen verknüpft ist.

Bemerkung 4.12. Man beachte, dass im vorherigen Abschnitt stets $t \in \mathbb{N}_0$ gefordert wurde. Also gelten alle dort getroffenen Aussagen bezüglich (t, m, s)-Netze auch für $(0, m, s)$-Netze.

Da für ein weiteres Voranschreiten auch nicht notwendigerweise lateinische Quadrate vonnöten sind, werden zuerst noch einige, in ähnlicher Form bereits bekannte, Begriffe eingeführt.

Definition 4.13 (Quadrat)**.** Ein *Quadrat der Ordnung* n ist eine $n \times n$ Matrix. Weiters nennt man zwei Quadrate der gleichen Ordnung n *orthogonal*, falls jedes von ihnen genau n verschiedene Symbole enthält und zusätzlich in ihrer Überlagerungsmatrix jedes der n^2 möglichen Tupel genau einmal auftritt.

Darüber hinaus sind die Quadrate $E_1, \ldots, E_s$ der Ordnung n genau dann *paarweise orthogonal*, wenn für alle $1 \leq i < j \leq s$ gilt, dass E_i und E_j orthogonal sind.

Somit ist zum Beispiel die $n \times n$ Einheitsmatrix I_n ein Quadrat, sicherlich jedoch kein lateinisches. Auch gibt es nach obiger Definition für $n > 2$ kein Quadrat, welches zu I_n orthogonal ist, da diese nur 2 anstatt n verschiedene Einträge besitzt.

Die Signifikanz dieser Definition wird im nachstehenden Satz klar. Er stellt eine $1:1$ Beziehung zwischen paarweise orthogonalen Quadraten und $(0, 2, s)$-Netzen her.

Satz 4.14. *Seien $s, b \in \mathbb{N}$, beide größer als 1, dann existiert ein $(0, 2, s)$-Netz in Basis b genau dann, wenn es s paarweise orthogonale Quadrate der Ordnung b gibt.*

Beweis. (Aus [2] und [6].)
Angenommen, es existiert ein $(0, 2, s)$-Netz in Basis b mit $\mathcal{P} = \{P_1, \ldots, P_{b^2}\}$.

Nun lassen sich mithilfe der i-ten Koordinate des n-ten Punktes $P_n^{(i)}$ paarweise orthogonale Quadrate $E_i = (e_{hk}^{(i)})$ der Ordnung b erzeugen. Hierbei gilt natürlich $1 \leq i \leq s$ und $1 \leq n \leq b^2$, sowie $1 \leq k, h \leq b$. Die Einträge in den Quadraten werden wie üblich die Zahlen $0, \ldots, b-1$ sein.

Man definiere also

$$e_{hk}^{(i)} = \lfloor b P_{(h-1)b+k}^{(i)} \rfloor \qquad \text{für} \qquad 1 \leq h, k \leq b,\ 1 \leq i \leq s.$$

Will man nun zeigen, dass je zwei der $E_1, \ldots, E_s$ orthogonal sind, wählt man zuerst zwei Indizes $1 \leq i < j \leq s$ beliebig aber fix. Gelingt es nun zu beweisen, dass

$$\forall c, d \in \{0, \ldots, b-1\}\ \exists h, k: \quad (e_{hk}^{(i)}, e_{hk}^{(j)}) = (c, d)\,, \tag{12}$$

dann folgt sofort daraus, dass alle n^2 möglichen Tupel in der Überlagerung von E_i und E_j vorkommen und die beiden Quadrate orthogonal sind. Da i und j beliebig sind, erhält man dann die paarweise Orthogonalität.

Seien also $c, d \in \{0, \ldots, b-1\}$. Man betrachte nun das Intervall $J = \prod_{q=1}^{s} J_q$, wobei

$$J_q = \begin{cases} \left[\frac{c}{b}, \frac{c+1}{b}\right) & \text{für } q = i \\ \left[\frac{d}{b}, \frac{d+1}{b}\right) & \text{für } q = j \\ [0, 1) & \text{sonst} \end{cases}.$$

Da es sich bei J um ein elementares Intervall in Basis b mit dem Volumen b^{-2} handelt, enthält es genau einen Punkt P_n aus $\mathcal{P}$. Aus diesem n lassen sich die Indizes h, k wegen $1 \leq h, k \leq b$ eindeutig mit $n = (h-1)b + k$ bestimmen. Weiters gilt

$$P_{(h-1)b+k}^{(i)} \in J_i = \left[\frac{c}{b}, \frac{c+1}{b}\right) \quad \text{und} \quad P_{(h-1)b+k}^{(j)} \in J_j = \left[\frac{d}{b}, \frac{d+1}{b}\right).$$

Also ist

$$e_{hk}^{(i)} = \lfloor b P_{(h-1)b+k}^{(i)} \rfloor = c \quad \text{und} \quad e_{hk}^{(j)} = \lfloor b P_{(h-1)b+k}^{(j)} \rfloor = d.$$

Damit wurde Aussage (12) und folglich die paarweise Orthogonalität von $E_1, \ldots, E_s$ gezeigt.

Für die andere Richtung des Beweises nimmt man an, es existieren s paarweise orthogonale Quadrate $E_1, \ldots, E_s$ mit den Einträgen $e_{hk}^{(i)} \in \{0, \ldots, b-1\}$,

$1 \leq h, k \leq b$.

Sei nun ein i mit $1 \leq i \leq s$ fixiert. Aufgrund der Orthogonalität müssen zu jedem $v \in \{0, \ldots, b-1\}$ genau b Einträge in E_i gleich v sein. Somit existiert eine Abbildung ϕ_i von $C := \{1, \ldots, b\} \times \{1, \ldots, b\}$ nach $\{0, \ldots, b-1\}$ mit der Eigenschaft, dass die Einschränkung

$$\phi_i | \{(h,k) \in C | e_{hk}^{(i)} = v\}$$

bijektiv ist.

Schließlich kann man für $(h,k) \in C$ und $n = (h-1)b + k$ die Punkte $P_1, \ldots, P_{b^2}$ wie folgt komponentenweise definieren

$$P_n^{(i)} = P_{(h-1)b+k}^{(i)} = e_{hk}^{(i)} b^{-1} + \phi_i(h,k) b^{-2}.$$

Zu zeigen bleibt, dass diese Punkte ein $(0, 2, s)$-Netz in Basis b bilden.Trivialer Weise gilt

$$0 \leq e_{hk}^{(i)} b^{-1} + \phi_i(h,k) b^{-2} \leq (b-1)b^{-1} + (b-1)b^{-2} < 1$$

und damit ist P_n stets aus I^s.

Sei $J = \prod_{q=1}^{s} J_q$ ein elementares Intervall in Basis b mit Volumen b^{-2}. Dann ist $J_q \neq [0,1)$ für entweder genau einen oder genau zwei Werte für q.

Fall 1: Es wird angenommen, nur für den Index i gilt, dass $J_i \neq [0,1)$. Das bedeutet, dass die J_q von der Form

$$J_q = \begin{cases} \left[\frac{e}{b^2}, \frac{e+1}{b^2}\right) & \text{falls } q = i \\ [0,1) & \text{sonst} \end{cases}$$

mit $0 \leq e < b^2$ sind.

Damit gilt

$$P_n = P_{(h-1)b+k} \in J \qquad \Longleftrightarrow \qquad e_{hk}^{(i)} b + \phi_i(h,k) = e.$$

Schreibt man nun $e = vb + r$ mit $v, b \in \{0, \ldots, b-1\}$, dann lässt sich diese Beziehung umformulieren in

$$P_n \in J \qquad \Longleftrightarrow \qquad e_{hk}^{(i)} = v \ \wedge \ \phi_i(h,k) = r.$$

Diese Eigenschaft kann aber nach der Definition von ϕ_i genau ein Tupel $(h,k) \in C$ erfüllen. Daher enthält J genau einen Punkt P_n.

Fall 2: Für genau 2 Indizes $i < j$ aus $\{1, \ldots, s\}$ gilt, dass $J_q \neq [0, 1)$, also für bestimmte $c, d \in \{0, \ldots, b-1\}$

$$J_q = \begin{cases} \left[\frac{c}{b}, \frac{c+1}{b}\right) & \text{falls } q = i \\ \left[\frac{d}{b}, \frac{d+1}{b}\right) & \text{falls } q = j \\ [0, 1) & \text{sonst} \end{cases}.$$

Es gilt

$$P_n = P_{(h-1)b+k} \in J \qquad \Longleftrightarrow \qquad e_{hk}^{(i)} = c \ \wedge \ e_{hk}^{(j)} = d.$$

Da nun E_i und E_j orthogonal sind, ist das Tupel $(h, k) \in C$ eindeutig bestimmt. Also enthält J auch in diesem Fall genau einen Punkt P_n.

□

Beispiel 4.15. Geht man also von einem $(0, 2, 2)$-Netz in Basis $b = 2$ aus, dann sollte man daraus $s = 2$ orthogonale Quadrate konstruieren können. Die Punktmenge sei wie folgt gegeben

$$\mathcal{P} = \left\{ \left(0, \frac{1}{4}\right), \left(\frac{1}{4}, \frac{1}{2}\right), \left(\frac{1}{2}, 0\right), \left(\frac{3}{4}, \frac{3}{4}\right) \right\}.$$

Nun zerlegt man jedes $1 \leq n \leq b^2 = 4$ in $n = (h-1)b + k = 2(h-1) + k$ mit $1 \leq h, k \leq b = 2$ und setzt

$$e_{hk}^{(i)} = \lfloor b P_{(h-1)b+k}^{(i)} \rfloor = \lfloor 2 P_{2(h-1)+k}^{(i)} \rfloor.$$

Die auf diesem Wege gewonnenen Einträge lauten somit

$$\begin{aligned} e_{11}^{(1)} &= \lfloor 2P_1^{(1)} \rfloor = 0 & \qquad e_{11}^{(2)} &= \lfloor 2P_1^{(2)} \rfloor = 0 \\ e_{12}^{(1)} &= \lfloor 2P_2^{(1)} \rfloor = 0 & \qquad e_{12}^{(2)} &= \lfloor 2P_2^{(2)} \rfloor = 1 \\ e_{21}^{(1)} &= \lfloor 2P_3^{(1)} \rfloor = 1 & \qquad e_{21}^{(2)} &= \lfloor 2P_3^{(2)} \rfloor = 0 \\ e_{22}^{(1)} &= \lfloor 2P_4^{(1)} \rfloor = 1 & \qquad e_{22}^{(2)} &= \lfloor 2P_4^{(2)} \rfloor = 1 \end{aligned}$$

und diese ergeben wiederum die orthogonalen Quadrate

$$E_1 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \qquad \text{und} \qquad E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Dieser Prozess kann, wie aus dem Beweis von Satz 4.14 ersichtlich, auch wieder rückgängig gemacht werden. Dafür setzt man $C = \{1, \ldots, b\}^2 = \{(1,1), (1,2), (2,1), (2,2)\}$ und definiert für $i = 1, 2$ die Abbildungen

$$\phi_i : C \longrightarrow \{0, 1\}.$$

Diese sollen, jeweils auf die Mengen $\{(h,k) \in C | e_{h,k}^{(i)} = v\}$ für alle $v \in \{0,1\}$ eingeschränkt, bijektiv sein. Eine Wahl ist beispielsweise

$$\begin{aligned} \phi_1 : (1,1) &\mapsto 0 & \qquad \phi_2 : (1,1) &\mapsto 1 \\ (1,2) &\mapsto 1 & (1,2) &\mapsto 0 \\ (2,1) &\mapsto 0 & (2,1) &\mapsto 0 \\ (2,2) &\mapsto 1 & (2,2) &\mapsto 1. \end{aligned}$$

Zerlegt man nun n wieder wie oben und bedient sich der Zuweisung

$$P_n^{(i)} = P_{(h-1)b+k}^{(i)} = e_{hk}^{(i)} b^{-1} + \phi_i(h,k) b^{-2}$$

aus vorherigem Beweis so ergeben sich die folgenden Punkte

$$\begin{aligned} P_1^{(1)} &= e_{11}^{(1)} \frac{1}{2} + \phi_1(1,1)\frac{1}{4} = 0 & \qquad P_1^{(2)} &= e_{11}^{(2)} \frac{1}{2} + \phi_2(1,1)\frac{1}{4} = \frac{1}{4} \\ P_2^{(1)} &= e_{12}^{(1)} \frac{1}{2} + \phi_1(1,2)\frac{1}{4} = \frac{1}{4} & P_2^{(2)} &= e_{12}^{(2)} \frac{1}{2} + \phi_2(1,2)\frac{1}{4} = \frac{1}{2} \\ P_3^{(1)} &= e_{21}^{(1)} \frac{1}{2} + \phi_1(2,1)\frac{1}{4} = \frac{1}{2} & P_3^{(2)} &= e_{21}^{(2)} \frac{1}{2} + \phi_2(2,1)\frac{1}{4} = 0 \\ P_4^{(1)} &= e_{22}^{(1)} \frac{1}{2} + \phi_1(2,2)\frac{1}{4} = \frac{3}{4} & P_4^{(2)} &= e_{22}^{(2)} \frac{1}{2} + \phi_2(2,2)\frac{1}{4} = \frac{3}{4}, \end{aligned}$$

also $\mathcal{P} = \left\{ \left(0, \frac{1}{4}\right), \left(\frac{1}{4}, \frac{1}{2}\right), \left(\frac{1}{2}, 0\right), \left(\frac{3}{4}, \frac{3}{4}\right) \right\}$.

Es ist nun wünschenswert, könnte man die Aussage aus Satz 4.14 wieder mit lateinischen Quadraten bzw. gleichbedeutend damit mit affinen und projektiven Ebenen in Beziehung setzen. Dies wird durch das folgende Lemma ermöglicht.

Lemma 4.16. *Es existieren genau dann s paarweise orthogonale Quadrate der Ordnung n, wenn es $s-2$ MOLS der Ordnung n gibt.*

Beweis. (Aus [2] und [6].)
Seien $E_3, \ldots, E_s$ $s-2$ MOLS der Ordnung n. Definiert man $E_1 = (e_{hk}^{(1)})$ über $e_{hk}^{(1)} = h - 1$ und $E_2 = (e_{hk}^{(2)})$ über $e_{hk}^{(2)} = k - 1$, also

$$E_1 = \begin{pmatrix} 0 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 1 \\ \vdots & \vdots & & \vdots \\ b-1 & b-1 & \ldots & b-1 \end{pmatrix} \quad \text{und} \quad E_2 = \begin{pmatrix} 0 & 1 & \ldots & b-1 \\ 0 & 1 & \ldots & b-1 \\ \vdots & \vdots & & \vdots \\ 0 & 1 & \ldots & b-1 \end{pmatrix}, \quad (13)$$

dann sind natürlich E_1 und E_2 orthogonal. Vergleicht man nun E_1 bzw. E_2 mit einem weiteren E_j, $j > 2$, dann sind diese wegen der Tatsache, dass es sich bei E_j um ein lateinisches Quadrat handelt, ebenfalls orthogonal.

Andererseits nehme man an, es existieren die paarweise orthogonalen Quadrate $E_1, \ldots, E_s$ der Ordnung n und betrachte die Abbildung

$$\begin{aligned} \eta : \{0, \ldots, n-1\}^2 &\longrightarrow \{0, \ldots, n-1\}^2 \\ (h, k) &\longmapsto (e_{hk}^{(1)}, e_{hk}^{(2)}). \end{aligned}$$

Da E_1 und E_2 orthogonal sind, ist η bijektiv und deshalb invertierbar mit $\phi = \eta^{-1}$. Setzt man nun für alle $1 \leq i \leq s$

$$L_i = (l_{hk}^{(i)}) \qquad \text{mit} \qquad l_{hk}^{(i)} = e_{\phi(hk)}^{(i)},$$

dann folgt unmittelbar, dass $L_1, \ldots, L_s$ paarweise orthogonal sind, da sie aus $E_3, \ldots, E_s$ entstehen, indem man ihre Elemente identisch permutiert.

Es bleibt also zu zeigen, dass es sich bei $L_3, \ldots, L_s$ um lateinische Quadrate handelt. Es gilt $l_{hk}^{(1)} = e_{\phi(hk)}^{(1)} = h$ und $l_{hk}^{(2)} = e_{\phi(hk)}^{(2)} = k$. Also sind L_1 und L_2 wie E_1 und E_2 in (13) gegeben. Da nun jedes L_j, $j > 2$, orthogonal zu L_1 und L_2 sein muss, folgt, dass L_j ein lateinisches Quadrat ist. □

Korollar 4.17. *Es gelten folgende Aussagen:*

i. Es existiert genau dann ein $(0, 2, s)$-Netz in Basis b, wenn es $s - 2$ MOLS der Ordnung b gibt.

ii. Es existiert genau dann eine projektive sowie eine affine Ebene der Ordnung b, wenn es ein $(0, 2, b + 1)$-Netz in Basis b gibt.

Beweis. Folgt aus Satz 3.12 und aus Lemma 4.16 zusammen mit Satz 4.14. □

Korollar 4.17 bestätigt einen sehr starken Zusammenhang zwischen der Existenz von MOLS und derer von $(0, 2, s)$-Netzen. Es ist daher wenig überraschend, dass sich sogar noch weitere Existenzaussagen für den allgemeineren Fall der $(0, m, s)$-Netze treffen lassen.

Mit Korollar 4.10 auf Seite 40 ist der Sprung von $(0, m, s)$-Netze auf $(0, 2, s)$-Netze bereits geglückt. Nun lässt sich mit der Theorie von MOLS zeigen, dass die Dimension s eine gewisse, von der Basis b abhängige Schranke, nicht überschreiten darf, soll es ein $(0, m, s)$-Netz geben. An dieser Stelle wird noch einmal in Erinnerung gerufen, dass die Größe $N(n)$ die maximale Anzahl von MOLS bezeichnet, die zur Ordnung n existieren können.

Satz 4.18. *Sei $m \geq 2$. Ein $(0, m, s)$-Netz in Basis b kann nur existieren, falls $s \leq N(b) + 2$.*

Beweis. (Aus [6].)
Angenommen es existiert ein $(0, m, s)$-Netz in Basis b mit $m \geq 2$. Nach Korollar 4.10 gibt es also auch ein $(0, 2, s)$-Netz in Basis b. Aus Korollar 4.17 folgt die Existenz von $s - 2$ MOLS der Ordnung b. Das bedeutet also

$$s - 2 \leq N(b).$$

□

Korollar 4.19. *Für $m \geq 2$ kann ein $(0, m, s)$-Netz in Basis b nur existiern, falls $s \leq b + 1$.*

Beweis. (Aus [6].)
Aus Satz 2.15 ist bekannt, dass $N(b) \leq b - 1$. Somit folgt aus Satz 4.18

$$s \leq N(b) + 2 \leq b + 1.$$

□

Diese Resultate zeigen zum Beispiel auf, dass für $b = 6$ und $m \geq 2$ kein $(0, m, s)$-Netz für $s > 3$ existieren kann, da, wie in Abschnitt 2.2 erwähnt, $N(6) = 1$.

Bemerkung 4.20. Die obere Schranke aus Satz 4.18 kann im Allgemeinen nicht verbessert werden. Es kann nämlich gezeigt werden, dass für eine Primzahlpotenz q ein $(0, m, q + 1)$-Netz in Basis q existiert[5] und es gilt

$$s = q + 1 \leq N(q) + 2 = q + 1$$

nach Satz 2.17.

Zusammenfassend hat der Leser nun erfahren, dass es zwischen der Existenz von $(0, m, s)$-Netzen, MOLS, affinen und projektiven Ebenen eine sehr enge, nämlich sogar eine $1 : 1$ Beziehung gibt. Mit den aus den Beweisen abgeleiteten Algorithmen lässt sich stets ein Objekt aus dem anderen erzeugen. Zusätzlich ist der Leser jetzt in der Lage, für Primzahlpotenzen solche sogar explizit zu konstruieren.

[5] Für Details siehe [2] bzw. [6].

Tabellenverzeichnis

Abbildungsverzeichnis

Literatur

[1] R. A. Brualdi: *Introductory Combinatorics.* Elsevier Science, 4th edition (1984)

[2] J. Dick, F. Pillichshammer: *Digital Nets and Sequences: Discrepancy Theory and Quasi-Monte Carlo Integration.* Cambridge University Press, Cambridge (2010)

[3] K. Jacobs: *Einführung in die Kombinatorik.* Walter de Gruyter, Berlin-New York, 1.Aufl. (1983)

[4] K. Jacobs: *Einführung in die Kombinatorik.* Walter de Gruyter, Berlin-New York, 2.Aufl. (2004)

[5] G. F. Mullen, C. Mummert: *Finite Fields and Applications.* American Mathematical Society (2007)

[6] H. Niederreiter: *Point Sets and Sequences with small Discrepancy.* Monatshefte für Mathematik 104(4) (1987)

[7] H. Niederreiter: *Random Number Generation and Quasi-Monte Carlo Methods.* No. 63 in CBMS-NSF Series in Applied Mathematics. SIAM, Philadelphia (1992)

[8] D. R. Stinson: *Combinatorial Designs: Constructions and Analysis.* Springer-Verlag New York (2004)