Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften

TECHNISCHE UNIVERSITÄT
ILMENAU

9. Studienbrief zur Diskreten Mathematik

Im Stoff der kommenden zwei Wochen geht es um die Wiederlegung der EULER-Vermutung „in Gänze". Statt Mengen von Quadraten werden orthogonale Schemata zu betrachten sein, und mittels zweier Sätze werden wir imstande sein, neue Schemata aus bereits bekannten zu konstruieren. Im Stoff dieser Woche wird neben dem „kleinen Schemasatz" auch der Zusammenhang zwischen großen Mengen paarweise orthogonaler lateinischer Quadrate und der Existenz von projektiven Ebenen der selben Ordnung n behandelt werden.

Ilmenau, den 15. Juni 2020 · Matthias Kriesell

(Fortsetzung Kapitel 2:

Wir betrachten nun wieder allgemein ein orthogonales (n,k)-Schema über K, etwa $A \in K^{X\times Y}$. Eine Partition $\mathfrak{C}$ von X in n viele n-elementige Mengen heißt *Auflösung* von A, falls für jedes $W \in \mathfrak{C}$ und jedes $y \in Y$ die Einschränkung

$$A|(W\times\{y\}) : W\times\{y\} \to K$$

von A auf $W\times\{y\}$ bijektiv ist. Also: In der y-ten Spalte, eingeschränkt auf einen Teil W der Partition, tritt jedes Symbol aus K genau einmal auf. Hieraus folgt $|W| = |K| = n$ und $|\mathfrak{C}| = |X|/n = n$. Entsprechend heißt A *auflösbar*, wenn es eine Auflösung besitzt.

Betrachten wir die z-te Spalte eines eines orthogonalen $(n,k+1)$-Schemas $A \in K^{X\times Y}$. Durch Streichung dieser Spalte erhält man offenbar ein orthogonales (n,k)-Schema

$$A^- := A|(X \times (Y \setminus \{z\})).$$

Aus der gestrichenen Spalte kann man eine Auflösung von A^- gewinnen, nämlich $\{X_c : c \in K\}$ mit

$$X_c := \{x \in X : A(x,z) = c\},$$

denn für $y \in Y \setminus \{z\}$ und $b,c \in K$ kommt das Symbolpaar (b,c) an genau einer Stelle in der Superposition $A_{(y;z)}$ vor; somit tritt b genau einmal in $A|(X_c\times\{y\})$ auf.

Umgekehrt kann man aus einer Auflösung $\mathfrak{C}$ eines orthogonalen (n,k)-Schemas $A \in K^{X\times Y}$ ein $(n,k+1)$-Schema herstellen. Dazu seien $z \notin Y$ ein frischer Spaltenindex, $Y^+ := Y \cup \{z\}$, und die $|K|$ vielen Elemente aus $\mathfrak{C}$ auf irgendeine Weise mit K indiziert, das heißt

$$\mathfrak{C} = \{X_c : c \in K\}.$$

Wir definieren $A^+ \in K^{X\times Y^+}$ durch

$$A^+(x,y) := \begin{cases} A(x,y) & \text{für } y \in Y \\ c & \text{für } y = z \text{ und } x \in X_c \end{cases}$$

Für $y \neq y'$ aus Y ist $A^+_{(y;y')}$ ist gleich $A_{(y;y')}$ und darum bijektiv. Für $y \in Y$ ist $A^+_{(y;z)}$ surjektiv (und damit ebenfalls bijektiv): Ist nämlich (b,c) ein Symbolpaar, so kommt b in $A|(X_c \times \{y\})$ etwa an Stelle x vor, also $A(x,y) = b$ mit $x \in X_c$. Damit ist $A^+_{(y;z)}(x) = (b,c)$.

Wir fassen unsere Eingangsbetrachtungen in folgendem Satz zusammen.

Satz 2.1.

Für $k, n \geq 2$ sind äquivalent:

(i) $N(n) \geq k$,

(ii) es gibt ein orthogonales $(n, k+2)$-Schema,

(iii) es gibt ein auflösbares orthogonales $(n, k+1)$-Schema

Beweis. Ist oben erbracht. □

Es besteht der folgende fundamentale Zusammenhang zwischen orthogonalen lateinischen Quadraten und projektiven bzw. affinen Ebenen; letztere kamen bereits in den Übungen zur Sprache: Eine (endliche, kombinatorische) *affine Ebene der Ordnung* n ist ein

$$2\text{-}(n^2, n, 1)\text{-Design.}$$

Satz 2.2.

Sei $n \geq 2$. Dann sind äquivalent:

(i) $N(n) = n - 1$,

(ii) es gibt eine affine Ebene der Ordnung n,

(iii) es gibt eine projektive Ebene der Ordnung n.

Beweis. Die Äquivalenz von (ii) und (iii) ist in der 4. Übungsserie (7. Studienbrief) erbracht worden „(ii) → (iii)" ist dort Aufgabe 1, „(iii) → (ii)" Aufgabe 2.

Gelte nun (i). Wir zeigen (ii). Nach Satz 2.1 gibt es ein orthogonales $(n, n+1)$-Schema $A \in K^{X \times Y}$, wobei $|K| = b$, $|X| = n^2$ und $|Y| = n + 1$ gelten. $P := X$ wird die Punktmenge der künftigen affinen Ebene. Die Blöcke werden einzeln für $y \in Y$ und $c \in K$ definiert durch

$$B_{y,c} := \{x \in X : A(x, y) = c\},$$

woraus $|B_{y,c}| = n$ folgt, da ja unter allen n^2 verschiedenen Symbolpaaren in $A_{(x;y)}$ das Symbol c an genau n Stellen in der zweiten Komponente auftritt. Sei

$$\mathfrak{B} := \{B_{y,c} : y \in Y, c \in K\}.$$

Seien nun $x \neq x'$ aus X. Aus $x, x' \in B_{y,c} \cap B_{y',c'}$ folgt $(A(x, y), A(x, y')) = (c, c')$ und $(A(x', y), A(x', y')) = (c, c')$ und somit $y = y'$ (denn sonst träte (c, c') an zwei Stellen x, x' in $A_{(y,y')}$ auf). Daraus folgt auch $c = A(x, y) = A(x, y') =$

c'. Hieraus folgt, daß zu zwei verschiedenen Punkten $x \neq x'$ *höchstens* ein Paar $(y, c) \in Y \times K$ mit $x, x' \in B_{y,c}$ existiert. Insbesondere sind die ($n \geq 2$-elementigen) $B_{y,c}$ paarweise verschieden, also gilt

$$|\mathfrak{B}| = |Y||K| = (n+1)n.$$

Doppeltes Abzählen liefert

$$(n+1)n\binom{n}{2} = \sum_{B\in\mathfrak{B}} \sum_{\substack{x,x'\in B\\ x\neq x'}} 1 = \sum_{\substack{x,x'\in X\\ x\neq x'}} \sum_{\substack{B\in\mathfrak{B}\\ x,x'\in B}} 1 \leq \binom{|X|}{2}\cdot 1 = \binom{n^2}{2} = (n+1)n\binom{n}{2},$$

also Gleichheit überall: Zu $x \neq x'$ gibt es daher *genau* ein $B \in \mathfrak{B}$ mit $x, x' \in B$. Also ist $(P, \mathfrak{B})$ ein 2-$(n^2, n, 1)$-Design, das heißt eine affine Ebene der Ordnung n.

Gelte (iii), wir zeigen (i). Sei dazu $(P, \mathfrak{B})$ eine projektive Ebene der Ordnung n, also ein 2-$(n^2+n+1, n+1, 1)$-Design. Nach dem Lemma 1.9 (Blocklemma) folgen $|\mathfrak{B}| = |P|$ und $|\mathfrak{B}(x)| = n+1$ für jedes $x \in P$, und wegen Satz 1.7 (DE BRUIJN und ERDŐS) gibt es zu $x \neq x'$ aus P genau ein $B \in \mathfrak{B}$ mit $x, x' \in B$; dieses B bezeichnen wir mit $B(x, x')$.

Sei nun $Y \in \mathfrak{B}$ fest gewählt, $X := P \setminus Y$ und K eine beliebige n-elementige Symbolmenge. Zu jedem $y \in Y$ wählen wir eine Bijektion

$$\varphi_y : \mathfrak{B}(y) \setminus \{Y\} \to K$$

und definieren eine $X \times Y$-Matrix A über K durch

$$A(x, y) := \varphi_y(B(x, y)).$$

Wir wollen zeigen, daß A ein orthogonales $(n, n+1)$-Schema ist. Natürlich ist $|K| = n$ und $|Y| = n+1$. Sind nun $y \neq z$ aus Y und $(c, d) \in K \times K$ ein beliebiges Symbolpaar, so existieren

$$B \in \mathfrak{B}(y) \setminus \{Y\} \text{ mit } \varphi_y(B) = c \text{ und } C \in \mathfrak{B}(z) \setminus \{Y\} \text{ mit } \varphi_z(B) = d.$$

Sei x der Punkt in $B \cap C$ (natürlich ist $B \neq C$). Dann ist

$$B = B(x, y) \text{ und } C = B(x, z), \text{ also } (A(x, y), A(x, z)) = (c, d).$$

Das Symbolpaar (c, d) tritt somit einmal (und daher auch: genau einmal) in $A_{(y;z)}$ auf. □

Der folgende „Kleine Schemasatz", Satz 2.3, konstruiert ein größeres Schema aus zwei schon konstruierten kleineren und kann als Prototyp einer ganzen Reihe solcher Theoreme angesehen werden, die es schließlich ermöglichten EULERs Vermutung „in Gänze" zu wiederlegen, das heißt zwei orthogonale lateinische Quadrate der Ordnung n für *alle* $n \geq 2$ außer für $n = 2$ und $n = 6$

zu konstruieren. Zu einem Schemasatz gehört stets eine Folgerung über das Verhalten von $N(\cdot)$ (in diesem Fall die Folgerung 2.4). Allen Sätzen ist zudem gemein, daß die Beweise Routineaufgaben sind und eine ähnliche „Größenordnung" wie die Konstruktionsbeschreibung selbst haben. Die Schwierigkeit liegt im Entdecken dieser Konstruktionen und im Zusammenbau des Ganzen.

Satz 2.3. (Kleiner Schemasatz)

Sei $B \in M^{X \times Y}$ ein orthogonales (m, k)-Schema und $C \in T^{X' \times Y}$ ein orthogonales (t, k)-Schema. Dann wird durch

$$A((x, x'), y) := (B(x, y), C(x', y)) \text{ für } (x, x') \in X \times X' \text{ und } y \in Y$$

ein orthogonales (mt, k)-Schema $A \in (M \times T)^{(X \times X') \times Y}$ definiert.

Beweis. Wegen $|M| = m$ und $|T| = t$ folgt $|M \times T| = |M||T| = mt$, außerdem ist $|Y| = k$ und $|X \times X'| = |X||X'| = m^2t^2 = (mt)^2$. Es genügt also zu zeigen, daß die Superposition zweier Spalten von A jedes Symbolpaar einmal (und damit: genau einmal) enthält. Seien dazu $y \neq z$ aus Y zwei Spaltenindices und $(c, d) \in (M \times T) \times (M \times T)$ ein Symbolpaar, etwa $c = (p, q)$ und $d = (r, s)$. Dann gibt es ein $x \in X$ mit $(B(x, y), B(x, z)) = (p, r)$ und ein $x' \in X'$ mit $(C(x', y), C(x', z)) = (q, s)$, weil B bzw. C ein orthogonales Schema ist. Also ist

$$\begin{aligned}(A((x, x'), y), A((x, x'), z)) &= ((B(x, y), C(x', y)), (B(x, z), C(x', z))) \\ &= ((p, q), (r, s)) \\ &= (c, d).\end{aligned}$$

□

Folgerung 2.4.

Für $m, t \geq 2$ gilt $N(mt) \geq \min\{N(m), N(t)\}$.

Beweis. Sei $k := \min\{N(m), N(t)\}$. Dann gibt es wegen Satz 2.1 ein orthogonales $(m, k+2)$-Schema B und ein orthogonales $(t, k+2)$-Schema C. Mit der Konstruktion aus Satz 2.3 kann man daraus ein orthogonales $(mt, k + 2)$-Schema gewinnen. Wegen Satz 2.1. kommt $N(mt) \geq k$. □

Läßt man sich auf die Konvention

$$N(1) = +\infty$$

ein, was ja nicht zuletzt auch deswegen stimmig ist, weil je zwei lateinische Quadrate der Ordnung 1 schon orthogonal sind, und erweitert die durch $\leq$ geordnete Menge $\mathbb{N}$ um $+\infty$, größer als alle Elemente aus $\mathbb{N}$, so sind Aussagen wie die aus Folgerung 2.4 auch für $m, t \geq 1$ formal richtig. Im folgenden werden wir das ohne weiteren Kommentar verwenden.

Übungen (5)

Abgabe bis Freitag den 26. Juni 2020.

Die Aufgabe 5 soll mit dem Stoff des 10. Studienbriefes bearbeitet werden.

1. Man konstruiere explizit ein orthogonales $(5, 6)$-Schema.
2. Seien $n_1, \ldots, n_\ell \geq 1$. Man zeige: $N(n_1 \cdot \cdots \cdot n_\ell) \geq \min\{N(n_1), \ldots, N(n_\ell)\}$.
3. Man zeige, daß es zu jedem $n \geq 2$ ein k gibt derart, daß ein orthogonales (n, k)-Schema ohne Auflösung existiert.
4. Man beweise, daß die im Kapitel 2 konstruierte 196×4-Matrix ein orthogonales $(14, 4)$-Schema ist.
5. Analysieren Sie, für welche $n \in \{2, 3, \ldots, 30\}$ die Schemasätze und die sonstigen Betrachtungen im zweiten Kapitel zu besseren unteren Schranken von $N(n)$ als 2 führen.
6. Man gebe unendlich viele n an derart, daß $N(n) < n - 1$ ist.