Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften

TECHNISCHE UNIVERSITÄT
ILMENAU

8. Studienbrief zur Diskreten Mathematik

Aus Ihren Reihen (MK) kam der Hinweis auf einen Fehler im 6. Studienbrief, Vielen Dank dafür:

In Satz 1.11 (i) ist die Teilvoraussetzung $n \equiv 1 \bmod 2$ falsch. Richtig lautet sie $n \equiv 1 \bmod 4$. Zu Beginn des Beweis steht sie noch einmal falsch (copy-paste). Der Satz lautet daher richtig:

Satz 1.11 (BRUCK & RYSER 1949)

Existiere eine projektive Ebene der Ordnung $n \geq 2$. Dann gilt:

(i) Ist $n \equiv 1 \bmod 4$ oder $n \equiv 2 \bmod 4$, so hat jeder Primfaktor $p \equiv 3 \bmod 4$ gerade Vielfachheit in der Primfaktorzerlegung von n, und:

(ii) $n \not\equiv 6 \bmod 8$.

Gegenstand dieser Woche ist ein Gegenbeispiel zur EULER-Vermutung, nämlich die Konstruktion zweier orthogonaler lateinischer Quadrate der Ordnung 10. Diese werden nicht direkt konstruiert, sondern in Form eines sogenannten *orthogonalen Schemas* angegeben. Der Vorteil ist, daß man das Schema leichter („kompakter") beschreiben und recht systematisch analyisieren kann. Wer Freude am Programmieren hat, kann versuchen, daraus die beiden Quadrate zu gewinnen! — Eine ganz ähnliche Konstruktion liefert zwei orthogonale lateinische Quadrate der Ordnung 14.

Wie klingen Quadrate? Aus zwei orthogonalen lateinischen Quadraten der Ordnung 12 leitete der französische Dirigent und Komponist PIERRE BOULEZ seine „Structure Ia" für zwei Klaviere ab, ein Hauptwerk des sogenannten „total serialism". Wie das klingt, kann man sich im Netz anhören — unglaublicherweise eingespielt von zwei wirklichen Pianisten.

Ilmenau, den 8. Juni 2020 · Matthias Kriesell

(Fortsetzung Kapitel 2:

Für eine $X \times Y$-Matrix A über K und $y, z \in Y$ ist die *Superposition der x-ten und y-ten Spalte* definiert durch

$$A_{(y;z)} : X \to K \times K,\ A_{(y;z)}(x) := (A(x,y), A(x,z) \text{ für } x \in X.$$

Wir nennen A ein *orthogonales (n,k)-Schema über A*, falls $|K| = n \geq 1$ und $|Y| = k \geq 2$ gilt und die Superposition je zweier Spalten von A bijektiv ist. Für ein solches Schema gilt natürlich $|X| = |K|^2 = n^2$. Informell bedeutet die Bedingung an die Superpositionen, daß jedes Symbolpaar $(c,d) \in K \times K$ in jedem „Spaltenpaar" genau einmal auftritt.

Orthogonale Schemata sind eine recht kompakte Möglichkeit, Mengen von paarweise orthogonalen lateinischen Quadraten zu codieren. Wir betrachten abermals die beiden eingangs genannten orthogonalen Quasigruppen

$$Q := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \text{ und } Q' := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

und bauen uns daraus ein orthogonales $(3,4)$-Schema. In die ersten beiden Spalten kommen die Koordinatenpaare (x,y) (zeilenweise), und in die letzten beiden Spalten die Einträge $Q(x,y)$ und $Q'(x,y)$ an den entsprechenden Stellen in den Quadraten. So entsteht

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 2 \\ 1 & 3 & 3 & 3 \\ 2 & 1 & 2 & 3 \\ 2 & 2 & 3 & 1 \\ 2 & 3 & 1 & 2 \\ 3 & 1 & 3 & 2 \\ 3 & 2 & 1 & 3 \\ 3 & 3 & 2 & 1 \end{pmatrix}.$$

Man kann sich die zwei letzten Spalten auch als „Linearisierung" der Quadrate Q und Q' denken. Seien die Spalten kanonische mit $1,2,3,4$ indiziert. $A_{(1;2)}$ ist natürlich bijektiv, und die Bijektivität von $A_{1;3}$ und $A_{2;3}$ besagt, daß Q ein lateinisches Quadrat ist. Analog besagt die Bijektivität von $A_{1;4}$ und $A_{2;4}$, daß Q' ein lateinisches Quadrat ist. Die Bijektivität von $A_{3;4}$ schließlich bedeutet, daß Q und Q' orthogonal sind!

Ganz allgemein kann man aus paarweise orthogonalen Quasigruppen $Q_1, \ldots, Q_k$ über $K = \mathbb{N}_n$ ein orthogonales $(n, k+2)$-Schema A gewinnen, indem man $X := K \times K$ und $Y = \{1, \ldots, k+2\}$ setzt und

$$A((x,y),i) := \begin{cases} x & \text{für } i = 1, \\ y & \text{für } i = 2 \text{ und} \\ Q_{i-2}(x,y) & \text{für } i \geq 3, \end{cases}$$

für $(x, y) \in X$ und $i \in Y$ definiert.

Interessanterweise läßt sich der Prozess auch umkehren. Ist $A : X \times \mathbb{N}_{k+2} \to K$ ein orthogonales $(n, k+2)$-Schema über K, so werden durch

$$Q_i(A(x,1), A(x,2)) := A(x, i+2)$$

für $x \in X$ und $i \in \{1, \ldots, k\}$ paarweise orthogonale Quasigruppen $Q_1, \ldots, Q_k$ über K definiert. Daß dies tatsächlich eine vollständige, unzweideutige Definition ist, liegt natürlich daran, daß die Superposition von 1-ter und 2-ter Spalte bijektiv ist. („Durchläuft x die Menge X, so nimmt $(A(x,1), A(x,2))$ jeden Wert aus $K \times K$ genau einmal an.") Q_i ist ein lateinisches Quadrat, weil $Q_{(1;i-2)}$ und $Q_{(2;i-2)}$ bijektiv sind, und Q_i, Q_j sind orthogonal für $i \neq j$, weil $Q_{(i-2;j-2)}$ bijektiv ist.

Folglich gibt es zu $n \geq 2$ genau dann k paarweise orthogonale lateinische Quadrate der Ordnung n, wenn es ein orthogonales $(n, k+2)$-Schema gibt. Gegenüber der Anschaulichkeit der ersten Aussage steht meist die leichtere Verifizierbarkeit der zweiten. Zudem kann man Zeilen, Spalten und Symbole einzelner Spalten eines orthogonalen Schemas beliebig permutieren um neue orthogonale Schemata zu gewinnen.

*

Wir wollen nun ein orthogonales $(10, 4)$-Schema angeben. Das sieht schwierig aus, ist es doch erstens eine 100×4-Matrix und wiederlegt es zweitens die Vermutung von EULER. Die Symbolmenge sei dabei

$$K = \mathbb{Z}_7 \cup \{\alpha, \beta, \gamma\},$$

wobei wir uns die Elemente aus $\mathbb{Z}_7$ wie üblich als $0, \ldots, 6$ denken und damit rechnen. α, β, γ sind schlicht neue Symbole. Wir betrachten folgende Bausteine

$$B := \left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ \hline \alpha & 0 & 1 & 6 \\ 0 & \alpha & 6 & 1 \\ 1 & 6 & \alpha & 0 \\ 6 & 1 & 0 & \alpha \\ \hline \beta & 0 & 2 & 5 \\ 0 & \beta & 5 & 2 \\ 2 & 5 & \beta & 0 \\ 5 & 2 & 0 & \beta \\ \hline \gamma & 0 & 3 & 4 \\ 0 & \gamma & 4 & 3 \\ 3 & 4 & \gamma & 0 \\ 4 & 3 & 0 & \gamma \end{array}\right) \quad \text{und} \quad C = \left(\begin{array}{cccc} \alpha & \alpha & \alpha & \alpha \\ \alpha & \beta & \beta & \beta \\ \alpha & \gamma & \gamma & \gamma \\ \hline \beta & \alpha & \beta & \gamma \\ \beta & \beta & \gamma & \alpha \\ \beta & \gamma & \alpha & \beta \\ \hline \gamma & \alpha & \gamma & \beta \\ \gamma & \beta & \alpha & \gamma \\ \gamma & \gamma & \beta & \alpha \end{array}\right).$$

Die horizontalen Linien dienen der Orientierung. Die Matrix C ist ein alter Bekannter: Sie kann aus Umbenennung von $1, 2, 3$ in α, β, γ aus dem orthogonalen $(3, 4)$-Schema oben gewonnen werden. Die Matrix B wird nach folgendem

Gesetz versiebenfacht: Für $c \in \mathbb{Z}_7$ sei $B + c$ definiert durch

$$(B + c)(x, y) := \begin{cases} B(x, y) + c & \text{für } B(x, y) \in \mathbb{Z}_7 \text{ und} \\ B(x, y) & \text{für } B(x, y) \in \{\alpha, \beta, \gamma\}. \end{cases}$$

Also: $B + c$ entsteht aus B eintragsweise, indem nach Möglichkeit c addiert wird, nur die „neuen Symbole" bleiben wie sie sind. Die 100×4-Matrix

$$A := \begin{pmatrix} B + 0 \\ B + 1 \\ \vdots \\ B + 6 \\ C \end{pmatrix}$$

erweist sich als orthogonales $(10, 4)$-Schema. Hierzu muß man verifizieren, daß für $i \neq j$ aus $\{1, 2, 3, 4\}$ jedes der 100 Symbolpaare (c, d) aus $K \times K$ wenigstens einmal (und damit genau einmal) von $A_{(i;j)}$ angenommen wird.

Sind c, d beide aus $\{\alpha, \beta, \gamma\}$, so geschieht dies in den letzten neun Zeilen von $A_{(i;j)}$, weil ja C ein orthogonales $(3, 4)$-Schema über $\{\alpha, \beta, \gamma\}$ ist.

Ist c aus $\{\alpha, \beta, \gamma\}$ und d nicht, so gibt es in B genau eine Zeile x mit $B(x, i) = \alpha$. Der Eintrag $h := B(x, j)$ ist dann aus $\mathbb{Z}_7$ nach Konstruktion, und wenn wir Glück haben, ist es $h = d$. Wenn nicht, dann ist $(B + (d - h))(x, j) = h + d - h$ (und $(B+(d-h))(x, i)$ unverändert gleich c), also kommt das Symbolpaar (c, d) in einer Zeile der i-ten und j-ten Spalte von $B+(d-h)$ und damit in einer Zeile von $A_{(i;j)}$ vor.

Sind schließlich c, d beide aus $\mathbb{Z}_7$, so benutzen wir die folgende Eigenschaft von D: In den sieben Zeilen von $B_{(i;j)}$, in denen beide Einträge aus $\mathbb{Z}_7$ stammen, nimmt die Differenz $B_{(i;j)} - B_{(i;j)}$ jeden Wert aus $\mathbb{Z}_7$ (genau einmal) an. Es gibt also eine Zeile x in B mit $B(x, i) - B(x, j) = c - d$. Sei nun $h := B(x, i)$. Dann gilt $(B+(c-h))(x, i) = h+c-h = c$ und $(B+(c-h))(x, j) = B(x, j)+(c-h) = B(x, i) - (c - d) + (c - h) = d$. Also kommt das Symbolpaar (c, d) in einer Zeile der i-ten und j-ten Spalte von $B + (c - h)$ und damit in einer Zeile von $A_{(i;j)}$ vor.

Also ist A wirklich ein orthogonales $(10, 4)$-Schema, und daraus kann man zwei orthogonale lateinische Quadrate der Ordnung 10 herstellen. Folglich gilt

$$N(10) \geq 2,$$

die Vermutung von EULER ist damit wiederlegt. Ein ähnliches Argument mit

$\mathbb{Z}_{11}$ anstelle von $\mathbb{Z}_7$ und der Matrix

$$B' := \left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 4 & 6 \\ 6 & 0 & 1 & 4 \\ 4 & 6 & 0 & 1 \\ 1 & 4 & 6 & 0 \\ \hline \alpha & 0 & 4 & 1 \\ 1 & \alpha & 0 & 4 \\ 4 & 1 & \alpha & 0 \\ 0 & 4 & 1 & \alpha \\ \hline \beta & 0 & 6 & 2 \\ 2 & \beta & 0 & 6 \\ 6 & 2 & \beta & 0 \\ 0 & 6 & 2 & \beta \\ \hline \gamma & 0 & 9 & 8 \\ 8 & \gamma & 0 & 9 \\ 9 & 8 & \gamma & 0 \\ 0 & 9 & 8 & \gamma \end{array}\right)$$

anstelle von B liefert das orthogonale $(14, 4)$-Schema

$$A' := \begin{pmatrix} B' + 0 \\ B' + 1 \\ \vdots \\ B' + 10 \\ C \end{pmatrix}.$$

Dabei ist C unverändert wie oben. A' ist eine 196×4-Matrix.