Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften

TECHNISCHE UNIVERSITÄT
ILMENAU

5. Studienbrief zur Diskreten Mathematik

In dieser Woche wird der „Nichtexistenzsatz" von BRUCK, RYSER und CHOWLA behandelt. Obwohl ein primär ein Satz der Kombinatorik, beruht sein Beweis auf Konzepten und Resultaten der (linearen) Algebra und Zahlentheorie — unter anderem auf dem berühmten Vier-Quadrate-Satz von LAGRANGE, nach der sich jede natürliche Zahl als Summe vierer Quadratzahlen darstellen läßt. Einen Beweis findet der Interessierte im entsprechenden (englischen) Wikipedia-Artikel, aber auch in praktisch jedem Buch über Zahlentheorie.

Der Nichtexistenzsatz beginnt (mehr oder weniger) mit den Worten „Existiere ein 2-(v, k, λ)-Design", so daß man sich fragen könnte, warum er denn ein *Nicht*-Existenzsatz sei. Der springende Punkt ist hier, daß aus der Existenzvoraussetzung Aufschluß über die Parameter v, k, λ gewonnen wird (Aussagen (i) und (ii) des Satzes). Erfüllen nun umgekehrt gewisse v, k, λ diese Aussagen nicht, so kann ein entsprechendes Design nicht existieren. Daher.

Die ganz wesentliche Bedeutung dieses Satzes liegt im Spezialfall kombinatorischer projektiver Ebenen, den wir in den kommenden beiden Wochen zum Abschluß des Kapitels über Mengensysteme mit Symmetrieeigenschaften ansehen werden.

Das Lesepensum ist reichlich, unter Präsenzbedingungen hätte ich wohl (i), aber nicht (ii) des Satzes beweisen können. Vielleicht möchten Sie die Lektüre des Beweises von (ii) in die nächste Woche verschieben (in der entsprechend weniger Stoff vorkommt), doch wollte ich nicht „mitten im Beweis aufhören"...

Ilmenau, den 18. Mai 2020 · Matthias Kriesell

(Fortsetzung Kapitel 1: Mengensysteme mit Symmetrieeigenschaften)

Wir kommen nun zum „Nichtexistenzsatz" von BRUCK, RYSER und CHOWLA. Hierzu benötigen wir einige Zutaten aus Algebra und Zahlentheorie.

Zwei $n \times n$-Matrizen A, B über einem Körper K heißen bekanntlich *kongruent*, wenn es eine invertierbare $n \times n$-Matrix S mit $S^\top AS = B$ gibt. Wir schreiben dann $A \cong B$ und definieren so eine Äquivalenzrelation auf der Menge der $n \times n$-Matrizen über K. Für zwei $n \times n$-Matrizen A, B und zwei $m \times m$-Matrizen C, D gilt:

$$A \cong B \wedge C \cong D \longrightarrow \begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} \cong \begin{pmatrix} B & 0 \\ 0 & D \end{pmatrix},$$

denn sind S, T invertierbare Matrizen mit $S^\top AS = B$ und $T^\top CT = D$, so ist wegen $\det \left(\begin{smallmatrix} S & 0 \\ 0 & T \end{smallmatrix}\right) = \det S \cdot \det T \neq 0$ auch $\left(\begin{smallmatrix} S & 0 \\ 0 & T \end{smallmatrix}\right)$ invertierbar, und es gilt $\left(\begin{smallmatrix} S & 0 \\ 0 & T \end{smallmatrix}\right)^\top \left(\begin{smallmatrix} A & 0 \\ 0 & C \end{smallmatrix}\right) \left(\begin{smallmatrix} S & 0 \\ 0 & T \end{smallmatrix}\right) = \left(\begin{smallmatrix} S^\top & 0 \\ 0 & T^\top \end{smallmatrix}\right) \left(\begin{smallmatrix} A & 0 \\ 0 & C \end{smallmatrix}\right) \left(\begin{smallmatrix} S & 0 \\ 0 & T \end{smallmatrix}\right) = \left(\begin{smallmatrix} S^\top AS & 0 \\ 0 & T^\top CT \end{smallmatrix}\right) = \left(\begin{smallmatrix} B & 0 \\ 0 & D \end{smallmatrix}\right)$.

Der berühmte Vier-Quadrate-Satz von LAGRANGE besagt, daß jede natürliche Zahl die Summe vierer Quadratzahlen ist. Wir verwenden ihn hier ohne Beweis.

Sei m eine natürliche Zahl und seien a, b, c, d Zahlen mit $m = a^2 + b^2 + c^2 + d^2$. Wir betrachten nun die Matrix

$$S := \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}.$$

Offensichtlich ist das Produkt einer Spalte von S mit sich selbst gleich $a^2 + b^2 + c^2 + d^2$, während — nicht ganz so offensichtlich — das Produkt zweier verschiedener Spalten gleich 0 ist! Bezeichnen wir mit E_n die $n \times n$-Einheitsmatrix, so kommt folglich

$$S^\top E_4 S = S^\top S = (a^2 + b^2 + c^2 + d^2) \cdot E_4, \text{ also } E_4 \cong mE_4.$$

Wegen obiger Aussage zur Kongruenz von Blockdiagonalmatrizen folgt sofort

$$E_n \cong mE_n \text{ für alle } m, n \geq 0 \text{ mit } 4|n.$$

Die zweite Hilfsaussage ist von eher technischer Art:

Zu $S \in \mathbb{Q}^{n \times n}$ existiert ein $y \in \mathbb{Q}^n$ mit $(Sy)_j{}^2 = y_j{}^2$ für $j \in \mathbb{N}_{n-1}$ und $y_n \neq 0$.

Beweis der Hilfsaussage.

Induktion über n. Klar für $n = 1$. Sei nun $n > 1$ und $S \in \mathbb{Q}^{n \times n}$ gegeben. Wir setzen

$$\varepsilon := \begin{cases} +1 & \text{für } S(1,1) \neq 1 \\ -1 & \text{für } S(1,1) = 1. \end{cases}$$

und

$$T(i,j) := \frac{S(i,1)\cdot S(1,j)}{(\varepsilon - S(1,1))} + S(i,j) \text{ für } i,j \in \{2,\ldots,n\}.$$

Dies definiert eine $\{2,\ldots,n\}\times\{2,\ldots,n\}$-Matrix über $\mathbb{Q}$. Nach Induktionsvoraussetzung existiert dazu ein $y = (y_2,\ldots,y_n)$ mit

$$(Ty)_j{}^2 = {y_j}^2 \text{ für } j \in \{2,\ldots,n-1\} \text{ und } y_n \neq 0.$$

Wir ergänzen zu $y \in \mathbb{Q}^n$ durch

$$y_1 := \sum_{\ell=2}^{n} \frac{S(1,\ell)\cdot y_\ell}{\varepsilon - S(1,1)}$$

und rechnen nach:

$$\begin{aligned}
(Sy)_1 &= \sum_{\ell=1}^{n}(S(1,\ell)y_\ell \\
&= S(1,1)y_1 + \sum_{\ell=2}^{n} S(1,\ell)y_\ell \\
&= S(1,1)y_1 + (\varepsilon - S(1,1))y_1 \\
&= \varepsilon y_1, \\
(Sy)_i &= \sum_{\ell=1}^{n}(S(i,\ell)y_\ell \\
&= S(i,1)y_1 + \sum_{\ell=2}^{n}(S(i,\ell)y_\ell \\
&= \sum_{\ell=2}^{n}\big(\frac{S(i,1)\cdot S(1,\ell)}{\varepsilon - S(1,1)} + S(i,\ell)\big)y_\ell \\
&= (Ty)_i{}^2
\end{aligned}$$

für $i \in \{2,\ldots,n\}$. Also gilt $(Sy)_i{}^2 = {y_i}^2$ für alle $i \in \{1,\ldots,n\}$, was die Hilfsaussage beweist.

Satz 1.10. (Nichtexistenzsatz von BRUCK, RYSER, CHOWLA)

Seien $v \geq k \geq 2$ und $\lambda > 0$ Zahlen mit $\lambda(v-1) = k(k-1)$.

Existiere ein 2-(v,k,λ)-Design. Dann gilt:

(i) Ist v gerade, so ist $k-\lambda$ eine Quadratzahl.

(ii) Ist v ungerade, so besitzt die diophantische Gleichung

$$x^2 = (k-\lambda)^2 + (-1)^{(v-1)/2}\lambda z^2$$

eine nichttriviale Lösung $(x,y,z) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$.

Beweis. Sei $(P, \mathfrak{B})$ ein 2-(v, k, λ)-Design.

Wir definieren die $P \times \mathfrak{B}$-Matrix N über $\mathbb{Q}$ durch

$$N(x, B) := \left\{ \begin{array}{ll} 1 & \text{falls } x \in B \\ 0 & \text{falls } x \notin B \end{array} \right\}.$$

N heißt *Inzidenzmatrix* von $(P, \mathfrak{B})$. Nach dem Blocklemma und wegen $\lambda(v-1) = k(k-1)$ ist $|\mathfrak{B}| = \lambda\binom{v}{2}/\binom{k}{2} = v$, so daß N als eine quadratische $v \times v$-Matrix angesehen werden kann, wobei wir uns die Indexmengen P und $\mathfrak{B}$ jeweils mit einer festen linearen Ordnung versehen denken.

Das Blocklemma liefert mit $\lambda(v-1) = k(k-1)$ auch $|\mathfrak{B}(x)| = \lambda\binom{v-1}{1}/\binom{k-1}{1} = k$, das heißt: Jeder Punkt inzidiert mit genau k Blöcken. In jeder Zeile von N stehen folglich genau k Einsen (in jeder Spalte sowieso, wegen $|B| = k$ für alle $B \in \mathfrak{B}$). Für die x-te Zeile von N gilt daher $N(x, \cdot) \cdot N(x, \cdot)^\top = k$ und für verschiedene Zeilen, etwa die x-te und die y-te, $x \neq y$ aus P, kommt

$$N(x, \cdot) \cdot N(y, \cdot)^\top = \sum_{B \in \mathfrak{B}} N(x, B) N(y, B),$$

was offensichtlich die Anzahl der Blöcke, die x und y beide enthalten liefert. Diese Zahl ist natürlich gleich λ (siehe Definition Design), und so ist $NN^\top$ auf der Diagonalen k und überall sonst λ:

$$NN^\top = (k - \lambda)E_v + \lambda J_v,$$

wobei J_v die $v \times v$-Matrix konstant 1 ist. Die Determinante von $NN^\top$ gewinnt man zum Beispiel, indem man durch Subtraktion der ersten Spalte von allen anderen und Addition der $v-1$ letzten Zeilen zur ersten eine untere Dreiecksmatrix herstellt und deren Diagonaleinträge multipliziert:

$$\begin{aligned} \det NN^\top &= \det \begin{pmatrix} k & \lambda-k & \lambda-k & \dots & \lambda-k \\ \lambda & k-\lambda & 0 & \dots & 0 \\ \lambda & 0 & k-\lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \dots & k-\lambda \end{pmatrix} \\ &= \det \begin{pmatrix} k+(v-1)\lambda & 0 & 0 & \dots & 0 \\ \lambda & k-\lambda & 0 & \dots & 0 \\ \lambda & 0 & k-\lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \dots & k-\lambda \end{pmatrix} \\ &= (k+(v-1)\lambda)(k-\lambda)^{v-1} \\ &= k^2 \cdot (k-\lambda)^{v-1}. \end{aligned}$$

(Die letzte Gleichung beruht auf der Voraussetzung $\lambda(v-1) = k(k-1)$.) Wegen $\lambda(v-1) = k(k-1) \leq k(v-1)$ kommt $\lambda \leq k$ und im Fall $\lambda = k$ auch $v = k$ und damit $|\mathfrak{B}| \leq 1$ im Widerspruch zu $|\mathfrak{B}| = v \geq 2$. Also ist $\lambda < k$ und somit

$$(\det N)^2 = \det NN^\top = k^2(k-\lambda)^{v-1} > 0.$$

Insbesondere ist N invertiertierbar. Weil die Determinante einer ganzzahligen Matrix ganzzahlig ist, ist $(k-\lambda)^{v-1}$ eine Quadratzahl. Für ungerades v gilt Letzteres ja ohnehin — für gerades v aber nur dann, wenn schon $k-\lambda$ eine Quadratzahl ist! Hieraus folgt (i).

Sei jetzt v ungerade. Wegen $(N^\top)^\top E_v N^\top = NN^\top$ ist $E_v \cong NN^\top$, und wir unterscheiden die beiden Fälle $v \equiv 1 \bmod 4$ und $v \equiv 3 \bmod 4$.

Im Fall $v \equiv 1 \bmod 4$ haben wir die diophantische Gleichung

$$x^2 = (k-\lambda)y^2 + \lambda z^2$$

nichttrivial in ganzen Zahlen zu lösen, wobei es tatsächlich genügt, eine nicht-triviale *rationale* Lösung zu finden. Mit der Vorbemerkung ist

$$NN^\top \cong E_v \cong \begin{pmatrix} E_{v-1} & 0 \\ 0 & E_1 \end{pmatrix} \cong \begin{pmatrix} (k-\lambda)E_{v-1} & 0 \\ 0 & E_1 \end{pmatrix} =: B;$$

daher gibt es ein invertierbare $v \times v$-Matrix S über $\mathbb{Q}$ mit $S^\top(NN^\top)S = B$. Wir wählen $y \in \mathbb{Q}^v$ wie in der Hilfsaussage und erhalten mit $x := Sy$ zunächst

$$x^\top NN^\top x = y^\top S^\top NN^\top Sy = y^\top By,$$

und daraus

$$\begin{aligned} y^\top By &= (k-\lambda)(y_1^2 + \cdots + y_{v-1}^2) + y_v^2 \\ = x^\top NN^\top x &= (k-\lambda)(x_1^2 + \cdots + x_v^2) + \lambda(x_1 + \cdots + x_v)^2; \end{aligned}$$

zusammen mit $y_i^2 = x_i^2$ für $i \in \{1, \ldots, v-1\}$ folgt

$$y_v^2 = (k-\lambda)x_v^2 + \lambda(x_1 + \cdots + x_v)^2,$$

und wegen $y_v \neq 0$ ist ist $(y_v, x_v, x_1 + \cdots + x_v)$ eine nicht-triviale Lösung der obigen Gleichung.

Im Fall $v \equiv 3 \bmod 4$ haben wir eine nichttriviale rationale Lösung für

$$x^2 = (k-\lambda)y^2 - \lambda z^2$$

zu finden. Wegen der Vorbemerkung kommt

$$\begin{pmatrix} NN^\top & 0 \\ 0 & E_1 \end{pmatrix} \cong E_{v+1} \cong (k-\lambda)E_{v+1} =: B,$$

also gibt es eine invertierbare $v+1 \times v+1$-Matrix über $\mathbb{Q}$ mit

$$S^\top \begin{pmatrix} NN^\top & 0 \\ 0 & E_1 \end{pmatrix} S = B.$$

Wieder wählen wir $y \in \mathbb{Q}^{v+1}$ wie in der Hilfsaussage und erhalten, ähnlich wie im ersten Fall:

$$\begin{aligned} y^\top By &= (k-\lambda)(y_1^2 + \cdots + y_{v+1}^2) \\ = x^\top \begin{pmatrix} NN^\top & 0 \\ 0 & E_1 \end{pmatrix} x &= (k-\lambda)(x_1^2 + \cdots + x_v^2) + \lambda(x_1 + \cdots + x_v)^2 + x_{v+1}^2; \end{aligned}$$

zusammen mit $y_i^2 = x_i^2$ für $i \in \{1, \ldots, v\}$ folgt

$$x_{v+1}^2 = (k-\lambda)y_{v+1}^2 - \lambda(x_1 + \cdots + x_v)^2,$$

und wegen $y_{v+1} \neq 0$ ist $(x_{v+1}, y_{v+1}, x_1 + \cdots + x_v)$ eine nicht-triviale Lösung der obigen Gleichung, wie gewünscht. □

Übungen (3)

Abgabe bis Freitag den 29. Mai 2020.

1. Sei V der Vektorraum ${\mathbb{Z}_2}^4$, $P := V \setminus \{0\}$ und $\mathfrak{B} := \{\{x, y, z\} \in \mathfrak{P}_3(P) : x + y + z = 0\}$. Ist $(P, \mathfrak{B})$ ein t-(v, k, λ)-Design? Wenn ja, für welche Parameter (t möglichst groß)?

2. Konstruieren Sie ein 2-$(9, 3, 1)$-Design.

3. Sei $D = (P, \mathfrak{B})$ ein t-(v, k, λ)-Design und $X \subseteq P$ mit $|X| \leq t$. Zeigen Sie, daß die folgenden Inzidenzstrukturen jeweils t'-(v', k', λ')-Designs sind und bestimmen sie „die" Parameter (t' möglichst groß).

   (i) $D^c := (P, \{P \setminus B : B \in \mathfrak{B}\})$,

   (ii) $D - X := (P \setminus X, \{B \in \mathfrak{B} : B \cap X = \emptyset\})$,

   (iii) $D/X := (P \setminus X, \{B \setminus X : B \subseteq \mathfrak{B},\ X \subseteq B\})$.

   D^c ist das *Komplement* von D, $D - X$ das *Residualdesign* von D nach X und D/X das von D nach X *abgeleitete Design*.

4. Das *verallgemeinerte Schulmädchenproblem* besteht darin, v Schulmädchen an x Sonntagen so in $v/3$ Dreierreihen spazieren zu führen, daß jedes Mädchenpaar an genau einem Sonntag in einer Dreierreihe zusammentrifft. Zeigen Sie, daß hierfür keine Lösung existiert, wenn v ein Vielfaches von 6 ist.

5. Ein 2-(v, k, λ)-Design heißt *symmetrisch*, falls es genau v Blöcke besitzt. Gibt es zu jedem beliebigen v ein symmetrisches 2-$(v, k, 1)$-Design (für ein geeignetes gewähltes k)?

6. Sei N die Inzidenzmatrix (siehe Beweis zu Satz 1.10) eines symmetrischen 2-(v, k, λ)-Designs. Für einen gegebenen Block B und $j \in \{0, \ldots, k\}$ sei a_j die Anzahl Blöcke $B' \neq B$ mit $|B \cap B'| = j$. Zeigen Sie (z. Bsp. durch Abzählen geeigneter Objekte) die Identitäten

   (i) $\sum_{j=0}^{k} a_j = v - 1$,

   (ii) $\sum_{j=0}^{k} j a_j = k \cdot (k - 1)$ sowie

   (iii) $\sum_{j=0}^{k} \binom{j}{2} a_j = \binom{k}{2}(\lambda - 1)$.

   Folgern Sie daraus: $\sum_{j=0}^{k} (j - \lambda)^2 a_j = 0$, und leiten Sie daraus her, daß auch $N^\top$ Inzidenzmatrix eines symmetrischen Designs ist.