13 Lateinische Quadrate

Def: Ein *lateinisches Quadrat der Ordnung n* ist eine $(n \times n)$-Tabelle mit Einträgen aus $\{0, \dots, n-1\}$, so dass jede Zahl in jeder Zeile und Spalte genau einmal vorkommt.

Bsp

0	1	2
1	2	0
2	0	1

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

Bem:
- Wir können die Symbole permutieren
- Wir können Zeilen und Spalten permutieren

$\Rightarrow$ LQ, die sich nur durch solche Operationen unterscheiden, heißen *äquivalent*.

Bsp: Verknüpfungstabelle von $(\mathbb{Z}_4, +)$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Def: $(Q, \circ)$ ist *Quasigruppe*: Q endlich und $\circ : Q \times Q \to Q$, so dass für $a, b \in Q$ die Gleichungen $a \circ x = b$ und $y \circ a = b$ eindeutige Lösungen haben (nicht notwendig gleich)

→ o kann über Tabelle gegeben werden

→ Tabelle ist LQ

Bsp

o	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

können partiell gefüllte LQ vervollständigt werden?

Satz: $(n \times n)$ - Tabelle
erste k Zeilen korrekt befüllt
Dann: können eine Zeile ergänzen

Satz von Hall!

$S_j := \{ i \mid i \text{ kommt noch nicht in Spalte } j \text{ vor} \}$

→ $|S_j| = n-k$

→ jedes i kommt in $n-k$ der S_j vor

Bipartiter Graph: $A, B = \{0, \dots, n-1\}$

$E = \{ (j, i) \mid i \in S_j \}$

$R \subseteq A$, dann: $N(R) = \bigcup_{j \in R} S_j$

und $|N(R)| \geq |R| \cdot \frac{n-k}{n-k} = |R|$ ∎

→ können wir auch auffüllen, wenn beliebige k Felder (korrekt) gefüllt sind?

1	2	
		3

$\Rightarrow k \geq n$ geht nicht

Satz (Evans, Smetaniuk)
Für $k \leq n-1$ ist Vervollständigung möglich.

[ohne Beweis]

→ wie viele LQ gibt es?

n	1	2	3	4	5	6	7	8
#	1	1	1	2	2	22	564	1676267

Def T_1, T_2 LQ der Ordnung n
T_1 und T_2 heißen orthogonal
$\Rightarrow$ zu jedem $(p_1, p_2) \in \{0, \dots, n-1\}^2$
gibt es eindeutige $0 \leq i, j \leq n-1$
mit $T_k(i,j) = p_k$ $k = 1, 2$.

Bsp

0	1	2
1	2	0
2	0	1

0	1	2
2	0	1
1	2	0

Satz: $T_1, \dots, T_k$ LQ der Ordnung n paarweise orthogonal. Dann $k \le n-1$

Durch Permutation der Einträge können wir annehmen, dass in jeder T_j die erste Zeile $0\ 1\ 2 \dots n-1$ ist.

Dann: Eintrag an $(2,1)$ muss für alle T_j verschieden sein!

da auch $\neq 1$

$\Rightarrow k \le n-1$ ∎

Def: $L(n) := \max(k \mid$ es gibt k paarw. orth. LQ der Ord. $n)$

→ ist $L(n) = n-1$?

$n = q^m$ Primzahlpotenz

Dann gibt $(\mathbb{Z}_n, \circ_j)$, $a \circ_j b := ja + b$

$n-1$ orthogonale LQ der Ordnung n.

0 1 2 3 4	0 1 2 3 4	0 1 2 3 4	0 1 2 3 4
1 2 3 ...	2 3 4 0 1	3 4 0 1 2	4 0 1 2 3
2	4 0 1 2 3	1 ...	3 4 ...
3	1 ...	4	2 ..
4	3 ..	2	1 ..

Satz $\Gamma = S \cdot t$. Dann $D(\Gamma) \ge \min(D(S), D(t))$

ohne Beweis

Kasc $r = p_1^{a_1} \cdots p_k^{a_k}$, dann

$$N(r) \geq \min\left(p_i^{a_i} - 1 \mid 1 \leq i \leq k\right)$$

und $N(r) \geq 2$ für $r \neq 2 \pmod 4$ ☐

Die ersten r, die keine Bernpotenz sind, sind

$$r = 6, 10, 12, 14$$

wissen: $N(6) = 1$, $N(r) \geq 3 \; \forall r \neq 2, 6$ (Bose et al)

$N(12) \geq 5$

→ noch ist nicht bekannt!

→ Quasigruppen und Steiner-Tripel-Systeme

Def Quasigruppe Q heißt

- kommutativ : $a \circ b = b \circ a$
- idempotent : $a \circ a = a$

Für $n = 2m+1$: $(\mathbb{Z}_n, +)$ und umbenennen, so dass Diagonale passt:

	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Für $n = 2m$ gibt es keine solchen Quasigruppen:

[jede Zahl kommt n mal auf, n gerade

also gleich oft in/unter Diag, einmal auf Diag]

können Steiner-Tripel-Systeme über Quasigruppen konstruiert:

$v = 6u+3$:

Q kommutativ, idempotente QG, $u = 2u+1$

$P = Q \times \mathbb{Z}_3$

$B_1 = \{ \{(i,0),(i,1),(i,2)\} \mid i \in Q \}$

$B_2 = \{ \{(i,k),(j,k),(i \circ j,k)\} \mid i \neq j, i,j \in Q, k \in \mathbb{Z}_3 \}$

$\rightarrow$ gleiche die Konstruktion des VL

Def Q mit Ordnung $2u$ ist halbidempotent

$\Leftrightarrow$ $a \circ a = (a+u) \circ (a+u) = a$, $0 \leq a < u$

konstruiere aus $(\mathbb{Z}_{2u}, +)$ durch Umbenennung, so dass Diagonale stimmt.

$\rightarrow v = 6u+1$:

Q' kommutativ, halbidempotent, Ordnung $u = 2u$

$Q := Q' \cup \{\omega\}$ für ein Symbol ω

$P = Q \times \mathbb{Z}_3$

$B_1 = \{ \{(i,0),(i,1),(i,3)\} \mid 0 \leq i < u \}$

$B_2 = \{ \{(i,k),(j,k),(i \circ j, k+1)\} \mid i \neq j \in Q, k \in \mathbb{Z}_3 \}$

$B_3 = \{ \{\omega,(i,k),(i+u,k-1)\} \mid 0 \leq i < u, k \in \mathbb{Z}_3 \}$

damit: Beweis analog zu $v = 6u+3$.