Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften

TECHNISCHE UNIVERSITÄT
**ILMENAU**

# 10. Studienbrief zur Diskreten Mathematik

In dieser Woche werden wir die Betrachtungen zu lateinischen Quadraten abschließen. Es wird uns (theoretisch) möglich sein, zu jedem $n \geq 1$, $n \neq 2$, $n \neq 6$ zwei orthogonale lateinische Quadrate zu konstruieren.

Die Teilkonstruktionen beruhen auf den Schemasätzen und können leicht in Linearzeit (von $n$) durchgeführt werden, wie man dort unmittelbar ablesen kann. Auf den ersten Blick erscheint es daher auch in der „Praxis" leicht, zwei orthogonale lateinische Quadrate anzugeben. Allerdings muß man zur Festlegung, was in den Rekursionsschritten eigentlich geschehen soll, eine Primfaktorzerlegung von $n$ (siehe Beweis von Satz 2.7) herstellen, und hierfür ist kein effizienter Algorithmus bekannt.[1] Wer Spaß an solchen Betrachtungen hat, mag anhand des Beweises von 2.7 darüber nachdenken, ob man dieses Problem umgehen kann, und ob im Beweisverlauf vielleicht noch weitere Fallstricke lauern, die eine Umsetzung in ein schnelles praktisches Verfahren verhindern.

Ilmenau, den 19. Juni 2020 · Matthias Kriesell

[1] Vor knapp 20 Jahren ist ein Polynomialzeitalgorithmus gefunden worden, der entscheiden kann, ob eine Zahl $n$ prim ist oder nicht — der sogenannten AKS-Primzahltest. Es ist jedoch kein Polynomialzeitalgorithmus bekannt, der einen nicht-trivialen Teiler von $n$ findet (falls $n$ nicht prim ist).

(Fortsetzung Kapitel 2:

Wir kommen nun zum „Großen Schemasatz" von RAY-CHAUDHURI. Obwohl er sich auch ohne Entlehnungen aus der Arithmetik formulieren läßt (also in der gleichen Weise „rein kombinatorisch" ist wie der kleine Schemasatz), ist die folgende Version leichter zu formulieren und zu beweisen. Statt $A \in K^{\mathbb{N}_p \times \mathbb{N}_q}$ schreiben wir $A \in K^{p \times q}$ und nennen $A$ eine $p \times q$-Matrix.

**Satz 2.5.** (Großer Schema Satz)

Seien $m, s, t, k \geq 1$ mit $s \leq t$ und $k \geq 2$ gegeben. Sei

$B \in \mathbb{N}_m^{m^2 \times k}$ ein orthogonales $(m, k)$-Schema,

$C \in \mathbb{N}_{m+1}^{(m+1)^2 \times k}$ ein orthogonales $(m+1, k)$-Schema mit $C((m+1)^2, j) = m+1$ für alle $j \in \mathbb{N}_k$,

$D \in \mathbb{N}_s^{s^2 \times k}$ ein orthogonales $(s, k)$-Schema und

$H \in \mathbb{N}_t^{t^2 \times k}$ ein orthogonales $(t, k)$-Schema mit Auflösung $\{P_i := \{j + (i-1)t : j \in \mathbb{N}_t\} : i \in \mathbb{N}_t\}$.

Sei $K := \mathbb{N}_s \dot{\cup} (\mathbb{N}_t \times \mathbb{N}_m)$ und

$$X := \underbrace{\mathbb{N}_{s^2}}_{=:X_1} \dot{\cup} \underbrace{(\mathbb{N}_{st} \times \mathbb{N}_{m^2+2m})}_{=:X_2} \dot{\cup} \underbrace{((\mathbb{N}_{t^2} \setminus \mathbb{N}_{st}) \times \mathbb{N}_{m^2})}_{=:X_3}$$

Wir definieren $A \in K^{X \times k}$ (das heißt: $A \in K^{X \times \mathbb{N}_k}$) durch

$$\begin{array}{rcl} A(x,j) & := & D(x,j) \\ & & \text{für } x \in X_1, j \in \mathbb{N}_k \\ A((x,y),j) & := & \left\{ \begin{array}{ll} ((H(x,j), C(y,j)) & \text{für } C(y,j) \leq m \\ \lceil x/t \rceil & \text{für } C(y,j) = m+1 \end{array} \right\} \\ & & \text{für } (x,y) \in X_2, j \in \mathbb{N}_k \\ A((x,y),j) & := & (H(x,j), B(y,j)) \\ & & \text{für } (x,y) \in X_3, j \in \mathbb{N}_k \end{array}$$

Dann ist $A$ ein orthogonales $(mt+s, k)$-Schema.

**Beweis.** Es ist $|K| = mt + s$. Weiterhin ist

$$|X| = |X_1| + |X_2| + |X_3| = s^2 + st(m^2+2m) + (t^2 - st)m^2 = s^2 + 2mst + t^2m^2 = (mt+s)^2,$$

so daß die Dimensionierung der Matrix $A$ der Behauptung nicht entgegensteht und nur der Nachweis erbracht werden muß, daß jedes Symbolpaar in der Superposition zweier Spalten einmal (und dann auch: genau einmal) auftritt.

Die Auflösung von $H$ besteht aus $t$ Blöcken von $t$ aufeinanderfolgen Indices. Daher gilt für $x \in \mathbb{N}_{t^2}$:

$$x \in P_c \longleftrightarrow \lceil x/t \rceil = c.$$

Seien nun $i < j$ aus $\mathbb{N}_k$ zwei Spaltenindices und $(c, c') \in K \times K$ ein Symbolpaar. Je nach Herkunft von $c, c'$ aus $\mathbb{N}_s$ oder $\mathbb{N}_t \times \mathbb{N}_m$ unterscheiden wir vier Fälle.

**1. Fall** $(c, c') \in \mathbb{N}_s \times \mathbb{N}_s$.

Weil $D$ ein orthogonales $(s, k)$-Schema ist, gibt es ein $x \in \mathbb{N}_{s^2} = X_1$ mit $(D(x, i), D(x, j)) = (c, c')$, also auch

$$(A(x, i), A(x, j)) = (c, c').$$

**2. Fall** $(c, c') \in \mathbb{N}_s \times (\mathbb{N}_t \times \mathbb{N}_m)$.

Sei etwa $c' = (c'_1, c'_2) \in \mathbb{N}_t \times \mathbb{N}_m$. Weil $\{P_1, \ldots, P_t\}$ Auflösung von $H$ ist und $c'_1$ im Symbolraum von $H$ liegt, gibt es ein $x \in P_c$ mit $H(x, j) = c'_1$, und natürlich gilt $\lceil x/t \rceil = c$. Wegen $c \leq s$ ist $P_c \subseteq \mathbb{N}_{st}$, also $x \in \mathbb{N}_{st}$. Weil $C$ orthogonales Schema ist gibt es ein $y \in \mathbb{N}_{(m+1)^2}$ mit $(C(y, i), C(y, j)) = (m + 1, c'_2)$, und wegen $c'_2 \leq m$ ist $y \neq (m + 1)^2$, also aus $\mathbb{N}_{m^2+2m}$. Somit ist $(x, y) \in X_2$, und es gilt nach Definition von $A$ in diesem Bereich

$$(A((x, y), i), A((x, y), j) = (\lceil x/t \rceil, ((H(x, j), C(y, j))) = (c, (c'_1, c'_2)) = (c, c').$$

**3. Fall** $(c, c') \in (\mathbb{N}_t \times \mathbb{N}_m) \times \mathbb{N}_s$

Dieser Fall kann analog zum 2. Fall behandelt werden. Man führe das übungshalber durch.

**4. Fall** $(c, c') \in (\mathbb{N}_t \times \mathbb{N}_m) \times (\mathbb{N}_t \times \mathbb{N}_m)$.

Seien etwa $c = (c_1, c_2)$ und $c' = (c_1, c_2)$ aus $\mathbb{N}_t \times \mathbb{N}_m$. Weil $H$ ein orthogonales Schema ist, gibt es ein $x \in \mathbb{N}_{t^2}$ mit $(H(x, i), H(x, j)) = (c_1, c'_1)$.

**1. Unterfall** $x \in \mathbb{N}_{t^2} \setminus \mathbb{N}_{st}$

Weil $B$ ein orthogonales Schema ist, gibt es ein $y \in \mathbb{N}_{m^2}$ mit $(B(y, i), B(y, j)) = (c_2, c'_2)$ Es ist $(x, y) \in X_3$, und in diesem Bereich gilt nach Definition von $A$

$$(A((x, y), i), A((x, y), j)) = (\underbrace{(H(x, i), B(y, i))}_{=(c_1, c_2)=c}, \underbrace{(H(x, j), B(y, j))}_{=(c'_1, c'_2)=c'}).$$

**2. Unterfall** $x \in \mathbb{N}_{st}$

Weil $C$ ein orthogonales Schema ist, gibt es ein $y \in \mathbb{N}_{(m+1)^2}$ mit $(C(y, i), C(y, j))$ $= (c_2, c'_2)$, und wegen $c_2 \leq m$ ist $y \neq (m + 1)^2$, also aus $\mathbb{N}_{m^2+2m}$. Demnach ist $(x, y) \in X_2$, und wegen $c_2, c'_2 \leq m$ gilt nach Definition von $A$

$$(A((x, y), i), A((x, y), j)) = (\underbrace{(H(x, i), C(y, i))}_{=(c_1, c_2)=c}, \underbrace{(H(x, j), C(y, j))}_{=(c'_1, c'_2)=c'}).$$

Eine raffinierte Konstruktion! □

Man beachte, daß die Zusatzbedingung an das Schema $C$ („letzte Zeile konstant $m+1$") durch Permutation der Symbole einzelner Spalten von $C$ stets hergestellt werden kann. Auch die „Blockgestalt" der Auflösung von $H$ kann durch Zeilentausch aus einer beliebigen Auflösung von $H$ hergestellt werden. Darauf baut auch der Beweis der Folgerung über das Verhalten von $N(\cdot)$ aus dem großen Schemasatz.

**Folgerung 2.6**

Für $m, s, t \geq 1$ mit $s \leq t$ gilt $N(mt+s) \geq \min\{N(m), N(m+1), N(s), N(t)-1\}$.

**Beweis.** Sei $k := \min\{N(m), N(m+1), N(s), N(t)-1\}$. Wegen Satz 2.1 gibt es ein orthogonales $(m, k+2)$-Schema $B$, ein orthogonales $(m+1, k+2)$-Schema $C$, ein orthogonales $(s, k+2)$-Schema $D$ und ein auflösbares orthogonales $(t, k+2)$-Schema $H$. Alle Voraussetzungen von Satz 2.5 an die dortigen Schemata können hergestellt werden, und die Konstruktion liefert ein orthogonales $(mt+s, k+2)$-Schema. Satz 2.1 impliziert dann $N(mt+s, k) \geq k$. □

Aus den bisherigen Betrachtungen folgt nun der besagte Satz von BOSE, SHRIKHANDE und PARKER.

**Satz 2.7.** (BOSE, SHRIKHANDE und PARKER)

Für $n \geq 2$, $n \neq 2$, $n \neq 6$ gilt $N(n) \geq 2$.

**Beweis.** Wir betrachten die Primfaktorzerlegung von $n$,

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_\ell^{\alpha_\ell}.$$

Da für alle Primzahlpotenzen $q$ es $q-1$ paarweise orthogonale lateinische Quadrate gibt (eingangs dieses Kapitels konstruiert), folgt mit der Folgerung aus dem kleinen Schemasatz, Folgerung 2.4:

$$N(n) \geq \min\{N(p_1^{\alpha_1}), \ldots, N(p_\ell^{\alpha_\ell})\} = \min\{p_1^{\alpha_1} - 1, \ldots, p_\ell^{\alpha_\ell} - 1\}.$$

Alle am Minimum beteiligten Terme sind wenigstens 2, es sei denn der Primfaktor 2 tritt mit nur einfacher Vielfachheit auf. Dies zeigt die Behauptung außer für den Fall $n \equiv 2 \bmod 4$.

Die beiden „Direktkonstruktionen" orthogonaler $(10, 4)$- und $(14, 4)$-Schemata zeigen $N(10) \geq 2$ und $N(14) \geq 2$. Für die nächsten vier Fälle $n \in \{18, 22, 26, 30\}$ helfen der große Schemasatz und spezielle Zerlegungen in $n = mt + s$, wie

folgt:

$$\begin{aligned} N(18 = 3 \cdot 5 + 3) &\geq \min\{N(3), N(4), N(3), N(5) - 1\} = 2, \\ N(22 = 3 \cdot 7 + 1) &\geq \min\{N(3), N(4), N(1), N(7) - 1\} = 2, \\ N(26 = 3 \cdot 7 + 5) &\geq \min\{N(3), N(4), N(5), N(7) - 1\} = 2, \\ N(30 = 3 \cdot 9 + 3) &\geq \min\{N(3), N(4), N(3), N(9) - 1\} = 2. \end{aligned}$$

Wir dürfen also $n \geq 34$ (und immer: $n \equiv 2 \bmod 4$) annehmen. Von den sechs ungeraden Zahlen

$$n-1, n-3, n-5, n-7, n-9, n-11$$

sind zwei durch 3, aber höchstens eine durch 9 teilbar. Das heißt, es gibt ein $s \in \{1, 3, 5, 7, 9, 11\}$ mit $3|(n-s)$ und $9 \not| (n-s)$. Also gilt $(n-s) = 3t$ für ein $t$ mit $3 \not| t$. Umstellen nach $n$ liefert

$$n = 3t + s.$$

Weil $n$ gerade ist und $s$ ungerade, muß $t$ ungerade sein. Wegen $s \leq 11$ und $n \geq 34$ muß $t > 1$ sein. Der kleinste Primteiler von $t$ ist daher 5, und so kommt mit den obigen Betrachtungen für $t$ anstelle von $n$

$$N(t) \geq 4.$$

Wäre $s > t$, so wäre $t \in \{9, 7, 5, 3, 1\}$, also $t \in \{7, 5\}$ nach Faktenlage, woraus $n = 3t + s \leq 3 \cdot 7 + 11 = 32$ folgt, ein Widerspruch. Also ist $s \leq t$, und Folgerung 2.6 liefert

$$N(n) = N(3t + s) \geq \min\{N(3), N(4), N(s), N(t) - 1\} = 2.$$

□