Codes & Lateinische Quadrate

von Ines Griesbach

NB: Für q prim wissen wir, dass $GF(q) = \mathbb{F}_q$ gilt. Im folgenden sei daher $GF(q) = \mathbb{F}_q = \{0, 1, \dots, q-1\}$, falls q prim ist.

Definition Ein lateinisches Quadrat der Ordnung q ist ein $q \times q$ Array mit Einträgen von q-verschiedenen Elementen aus dem $GF(q)$-Körper, sodass jede Zeile und jede Spalte jedes Element genau einmal enthält.

Beispiel: $\mathbb{F}_3 = \{0, 1, 2\}$:

$$\begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix} \quad , \quad \begin{matrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{matrix}$$

Theorem 10.2.: Für jede natürliche Zahl q existiert ein lateinisches Quadrat A der Ordnung q.

Beweis: OE sei $(a_{0,0}, a_{0,1}, \dots, a_{0,q-1}) = (0, 1, \dots, q-1)$ die erste Zeile. Setze $(a_{i,0}, a_{i,1}, \dots, a_{i,q-1}) = (a_{0,0} + i, a_{0,1} + i, \dots, a_{0,q-1} + i)$ für $i \in \{1, \dots, q-1\}$.

$\Rightarrow$

$$\begin{matrix} 0 & \cdots & q-1 \\ 1 & \cdots & 0 \\ \vdots & & \\ q-1 & 0 & \cdots \; q-2 \end{matrix}$$

Definition Seien A, B zwei lateinische Quadrate der Ordnung q. Seien a_{ij} (und b_{ij}) die Einträge der i-ten Zeile und j-ten Spalte von A (und B). Wenn die q^2 geordneten Tupel (a_{ij}, b_{ij}), $i, j = 0, \dots q-1$, alle verschieden sind, dann heißen A und B **paarweise orthogonale lateinische Quadrate** (engl: mutually orthogonal latin squares, kurz MOLS).

Beispiel:

$$A = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix} \quad B = \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix} \rightsquigarrow AB = \begin{matrix} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \\ (2,1) & (0,2) & (1,0) \end{matrix}$$

Beispiel: Für lateinische Quadrate der Ordnung 2 existiert kein Paar von paarweise orthogonalen lateinischen Quadraten.

Beweis: Für $q=2$ existieren nur zwei lateinische Quadrate:

$$A = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}, \quad B = \begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix} \rightsquigarrow AB = \begin{matrix} (0,1) & (1,0) \\ (1,0) & (0,1) \end{matrix} \Rightarrow \begin{matrix} ab_{11} = ab_{22} \\ ab_{12} = ab_{21} \end{matrix}$$

Optimale Fehler-erkennende und -korrigierende Codes der Länge 4

Erinnerung an die Hauptproblematik der Kodierungstheorie:

$$A_q(4,3) = \max\{M \mid \text{existiert } q\text{-närer } (4,M,3)\text{-Code}\}$$

Theorem 10.5: $A_q(4,3) \leq q^2$ für alle $q \in \mathbb{N}$

Beweis: Angenommen C sei ein solcher $(4,M,3)$-Code und $x = (x_1\ x_2\ x_3\ x_4)$ und $y = (y_1\ y_2\ y_3\ y_4)$ seien verschiedene Codewörter von C.

Es folgt: $(x_1\ x_2) \neq (y_1\ y_2)$, ansonsten wäre $d(C) < 3$ ↯

$\Rightarrow \hat{x} = (x_1\ x_2), \hat{y} = (y_1\ y_2) \in (\mathbb{F}_q)^2$

$\Rightarrow M \leq q^2$

Beispiel 10.6: Für $q=3$ wird die Obergrenze aus Theorem 10.5 erreicht, denn der Hamming Code $\text{Ham}(2,3)$ ist ein $(4,9,3)$-Code:

$$\begin{array}{cccc} 0&0&0&0\\ 0&1&1&2\\ 0&2&2&1\\ 1&0&1&1\\ 1&1&2&0\\ 1&2&0&2\\ 2&0&2&2\\ 2&1&0&1\\ 2&2&1&0 \end{array}$$

Bemerkung: Ist $q \geq 4$, dann ist die obere Schranke von Theorem 10.5 eine deutliche Verbesserung zu der „sphere-packing"-Schranke:

$$A_q(4,3) \leq q^4 (4q-3)^{-1} \quad \text{(Satz 2.16)}$$

Wir halten fest: Für Codewörter eines $(4, q^2, 3)$-Codes C sind die ersten beiden Einträge so, dass für $x, y \in C$ gilt: $(x_1, x_2) \neq (y_1, y_2)$

Damit definieren wir unseren Code C:

$$C = \{(i, j, a_{ij}, b_{ij}) \mid (i,j) \in (\mathbb{F}_q)^2\}$$

Theorem 10.7. Es existiert ein q-närer $(4, q^2, 3)$-Code genau dann, wenn ein Paar von paarweise orthogonalen lateinischen Quadraten existiert.

Beweis: Wir zeigen:

$C = \{(i, j, a_{ij}, b_{ij}) \mid (i,j) \in (\mathbb{F}_q)^2\}$ ist ein $(4, q^2, 3)$-Code

$\Leftrightarrow$

$A = (a_{ij})$ und $B = (b_{ij})$ ist ein Paar von paarweise orthogonalen lateinischen Quadraten

Beweis Theorem 10.5

Die minimale Distanz $d(C)$ ist 3 $\Leftrightarrow$ für alle Codewörter $x, y \in C$ gilt $(x_i, x_j) \neq (y_i, y_j)$ $\forall i,j \in \{1,\dots,4\}$

$\Leftrightarrow$

1.) Die q^2 Paare (i, a_{ij}) und die q^2 Paare (j, a_{ij}) sind verschieden $\Leftrightarrow$ A ist ein lateinisches Quadrat

2.) Analog folgt die gleiche Äquivalenz für B

und:

3.) Die q^2 Paare (a_{ij}, b_{ij}) sind verschieden $\Leftrightarrow$ A und B sind paarweise orthogonal

$\Rightarrow$ $A_q(4,3) = q^2$ $\Leftrightarrow$ 3 Paar von paarweise orthogonalen lateinischen Quadraten

Theorem 10.8. Ist $q \neq 2$ eine Primzahl, dann existiert ein Paar von paarweise orthogonalen lateinischen Quadraten.

Beweis: Sei $\mathbb{F}_q = \{0, 1, \dots, q-1\} (\equiv GF(q))$ und μ und τ zwei unterschiedliche, von 0 verschiedene Elemente aus $\mathbb{F}_q$. Sei $A = [a_{ij}]$ und $B = [b_{ij}]$ zwei $q \times q$ arrays definiert durch:

$$a_{ij} = i + \mu \cdot j \quad , \quad b_{ij} = i + \tau \cdot j \quad , \quad i,j \in \mathbb{F}_q$$

A, B sind lateinische Quadrate, denn wären zwei Einträge derselben Zeile in A gleich, dann hätten wir:

$$i + \mu \cdot j = i + \mu \cdot j' \Rightarrow \mu \cdot j = \mu \cdot j' \overset{\substack{j,j' \in \mathbb{F}_q \\ q \text{ prim}}}{\Rightarrow} j = j'$$

für zwei gleiche Einträge einer Spalte folgt:

$$i + \mu \cdot j = i' + \mu \cdot j \Rightarrow i = i'$$

$\rightarrow$ Analoger Beweis für B.

Außerdem sind A und B orthogonal, denn für $(a_{ij}, b_{ij}) = (a_{i'j'}, b_{i'j'})$ $i,i',j,j' \in \mathbb{F}_q$ folgt:

1. $i + \mu \cdot j = i' + \mu \cdot j'$ und 2. $i + \nu \cdot j = i' + \nu \cdot j'$

$\Rightarrow (\mu - \nu) j = (\mu - \nu) \cdot j' \overset{\mu \neq \nu}{\Rightarrow} j = j' \Rightarrow i = i'$

$\Rightarrow (a_{ij}, b_{ij}) \neq (a_{i'j'}, b_{i'j'}) \; \forall i,i',j,j' \in \mathbb{F}_q$ mit $i \neq i', j \neq j'$.
$\Rightarrow A, B$ orthogonal
$\Rightarrow \exists$ ein Paar von paarweise orthogonalen lateinischen Quadraten.

Beispiel 10.9. Sei $q = 3 \Rightarrow \mathbb{F}_q = \{0,1,2\}$, $\mu = 1$, $\nu = 2$

$a_{ij} = i + \mu \cdot j = i + j$ $\quad b_{ij} = i + \nu \cdot j = i + 2j$

$\Rightarrow$

$$A = \begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad B = \begin{array}{ccc} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{array}$$

$\rightarrow$ Der zugehörige $(4,9,3)$-Code, gegeben durch:

$C = \{(i,j,a_{ij},b_{ij}) \mid (i,j) \in (\mathbb{F}_3)^2\}$ ist dann:

i	j	a_{ij}	b_{ij}
0	0	0	0
0	1	1	2
0	2	2	1
1	0	1	1
1	1	2	0
1	2	0	2
2	0	2	2
2	1	0	1
2	2	1	0

$\Rightarrow C = \text{Ham}(2,3)$ (siehe Bsp. 10.6)

Theorem 10.10: Wenn ein Paar von paarweise orthogonalen lateinischen Quadraten der Ordnung m und ein Paar von paarweise orthogonalen lateinischen Quadraten der Ordnung n existiert, dann existiert ein Paar von paarweise orthogonalen lateinischen Quadraten der Ordnung $m \cdot n$.

Beweis: Angenommen A_1, A_2 seien ein Paar von paarweise orthogonale lateinischen Quadraten der Ordnung m und B_1, B_2 seien ein Paar von paarweise orthogonalen lateinischen Quadraten der Ordnung n.

Der (i,j)te Eintrag von A_k sei $a_{ij}^{(k)}$ $(k=1,2)$ und analog sei der (i,j)te Eintrag von B_k $b_{ij}^{(k)}$ $(k=1,2)$

Seien nun C_1, C_2 die $m \cdot n \times m \cdot n$ Quadrate definiert durch:

$$C_k = \begin{matrix} (a_{00}^{(k)}, B_k) & (a_{01}^{(k)}, B_k) & \cdots & (a_{0m-1}^{(k)}, B_k) \\ (a_{10}^{(k)}, B_k) & & & \\ \vdots & & & \vdots \\ (a_{m-1,0}^{(k)}, B_k) & \cdots & & (a_{m-1,m-1}^{(k)}, B_k) \end{matrix}$$

wobei $(a_{ij}^{(k)}, B_k)$ ein $n \times n$ Array ist mit dem (r,s)ten Eintrag $(a_{ij}^{(k)}, b_{rs}^{(k)})$.

$$\Rightarrow (a_{00}^{(1)}, B_1) = \begin{matrix} (a_{00}^{(1)}, b_{00}^{(1)}) & \cdots & (a_{00}^{(1)}, b_{0n-1}^{(1)}) \\ \vdots & & \vdots \\ (a_{00}^{(1)}, b_{n-1,0}^{(1)}) & \cdots & (a_{00}^{(1)}, b_{n-1,n-1}^{(1)}) \end{matrix}$$

Da $a_{ij}^{(k)} \neq a_{i'j'}^{(k)}$, $\forall i,j,j' \in \{0,\dots,m-1\}$, $j \neq j'$, $k \in \{1,2\}$ gilt und $a_{ij}^{(k)} \neq a_{i'j}^{(k)}$ $\forall i,i',j \in \{0,\dots,m-1\}$, $i \neq i'$, $k \in \{1,2\}$, folgt:

$(a_{ij}^{(k)}, B_k) \neq (a_{i'j}^{(k)}, B_k)$ und $(a_{ij}^{(k)}, B_k) \neq (a_{ij'}^{(k)}, B_k)$ $\forall i,i',j,j' \in \{0,\dots,m-1\}$ $i \neq i'$, $j \neq j'$, $k \in \{1,2\}$.

$\Rightarrow (a_{ij}^{(k)}, b_{rs}^{(k)}) \neq (a_{i'j}^{(k)}, b_{rs}^{(k)})$ und $(a_{ij}^{(k)}, b_{rs}^{(k)}) \neq (a_{ij'}^{(k)}, b_{rs}^{(k)})$ $\forall i,i',j,j' \in \{0,\dots,m-1\}$ $i \neq i'$, $j \neq j'$, $k \in \{1,2\}$, $(a_{ij}^{(k)}, b_{rs}^{(k)}) \neq (a_{ij}^{(k)}, b_{r's}^{(k)})$ und $(a_{ij}^{(k)}, b_{rs}^{(k)}) \neq (a_{ij}^{(k)}, b_{rs'}^{(k)})$ $\forall r,r',s,s' \in \{0,\dots,n-1\}$, $r \neq r'$, $s \neq s'$, $k \in \{1,2\}$

$\Rightarrow$ C_1 und C_2 sind lateinische Quadrate.

$$C_1 C_2 = \begin{pmatrix} ((a_{00}^{(1)}, B_1), (a_{00}^{(2)}, B_2)) & \cdots & ((a_{0m-1}^{(1)}, B_1), (a_{0m-1}^{(2)}, B_2)) \\ \vdots & & \vdots \\ ((a_{m-1,0}^{(1)}, B_1), (a_{m-1}^{(2)}, B_2)) & \cdots & ((a_{m-1,m-1}^{(1)}, B_1), (a_{m-1,m-1}^{(2)}, B_2)) \end{pmatrix}$$

Es folgt $((a_{ij}^{(1)}, B_1), (a_{ij}^{(2)}, B_2)) \neq ((a_{i'j'}^{(1)}, B_1), (a_{i'j'}^{(2)}, B_2))$ für $i \neq i'$, $j \neq j'$, da $(a_{ij}^{(1)}, a_{ij}^{(2)}) \neq (a_{i'j'}^{(1)}, a_{i'j'}^{(2)})$ und $(b_{rs}^{(1)}, b_{rs}^{(2)}) \neq (b_{r's'}^{(1)}, b_{r's'}^{(2)})$ $\forall i \neq j', j \neq j', r \neq r', s \neq s'$

$\Rightarrow$ C_1 und C_2 sind paarweise orthogonal.

Beispiel 10.11.

$$A_1 = \begin{matrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{matrix}, \quad A_2 = \begin{matrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{matrix},$$

A_1, A_2 sind paarweise orthogonal zueinander und lateinische Quadrate

$$B_1 = \begin{matrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{matrix}, \quad B_2 = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{matrix},$$

B_1, B_2 ist ein Paar von paarweise orthogonalen lateinischen Quadraten

Wir konstruieren nun ein Paar von paarweise orthogonalen lateinischen Quadraten der Ordnung 12 wie im Beweis von Theorem 10.10:

$C_1 = (0, B_1)\ (1, B_1)\ (2, B_1)$

$(1, B_1)\ (2, B_1)\ (0, B_1)$

$(2, B_1)\ (0, B_1)\ (1, B_1)$

$C_2 = (0, B_2)\ (1, B_2)\ (2, B_2)$

$(2, B_2)\ (0, B_2)\ (1, B_2)$

$(1, B_2)\ (2, B_2)\ (0, B_2)$

$\Rightarrow C_1 =$

00 01 02 03	10 11 12 13	20 21 22 23
01 00 03 02	11	21
02 03 00 01	12 ...	22 ...
03 02 01 00	13 ...	23
10 11 12 13	20 21 22 23	00 01 02 03
11	21	01
12 ...	22 ...	02 ...
13	23	03
20 21 22 23	00 01 02 03	10 11 12 13
21	01	11
22 ...	02 ...	12 ...
23	03	13

$C_2 =$

00 01 02 03	10 11 12 13	20 21 22 23
02 03 00 01	12	22
03 02 01 00	13	23
01 00 03 02	11	21
20 21 22 23	00 01 02 03	10 11 12 13
22	02	12
23	03	13
21	01	11
10 11 12 13	20 21 22 23	00 01 02 03
12	22	02
13	23	03
11	21	01

$C_1 C_{2_{00}} = ((0, b^1_{00}), (0, b^2_{00})) = ((00)(00))$

$C_1 C_2 =$

$((0,B_1),(0,B_2))$	$((1,B_1),(1,B_2))$	$((2,B_1),(2,B_2))$
$((1,B_1),(2,B_2))$	$((2,B_1),(0,B_2))$	$((0,B_1),(1,B_2))$
$((2,B_1),(1,B_2))$	$((0,B_1),(2,B_2))$	$((1,B_1),(0,B_2))$

Theorem 10.12. Ist $q \equiv 0, 1, 3 \pmod 4$, dann existiert ein Paar von paarweise orthogonalen lateinischen Quadraten.

Beweis: Sei $q \equiv 0, 1, 3 \pmod 4$. Dann ist q ungerade oder durch 4 teilbar. Sei nun die Primfaktorzerlegung von $q = p_1^{h_1} p_2^{h_2} \dots p_t^{h_t}$, wobei $p_1, \dots, p_t$ verschiedene Primzahlen und $h_1, \dots, h_t \in \mathbb{N} \setminus \{0\}$.
Nach Theorem 10.8. existiert ein Paar von paarweise orthogonalen lateinischen Quadraten $p_i^{h_i}$ $\forall i \in \{1, \dots, t\}$.
Mit wiederholter Anwendung von Theorem 10.10 folgt die Aussage.

Theorem 10.13. (Bose, Shrikhande und Parker (1960))
Für alle $q \in \mathbb{N} \setminus \{2,6\}$ existiert ein Paar von paarweise orthogonalen lateinischen Quadraten der Ordnung q.

Beweis: hier zu umfangreich!

Korollar 10.14 $A_q(4,3) = q^2$ für alle $q \neq 2,6$

Beweis: Aus Theorem 10.5. folgt: $A_q(4,3) \leq q^2$. Aus Theorem 10.7 folgt, dass ein q-närer $(4, q^2, 3)$-Code existiert
$\Leftrightarrow$ $\exists$ ein Paar von paarweise orthogonalen lateinischen Quadraten der Ordnung q
$\Leftrightarrow$ $q \neq 2,6$
↑ Theorem 10.13

Theorem 10.15: $A_6(4,3) = 34$

Beweis:

$$A = \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 2 & 5 & 4 \\ 2 & 3 & 5 & 4 & 0 & 1 \\ 3 & 2 & 4 & 5 & 1 & 0 \\ 4 & 5 & 1 & 0 & 3 & 2 \\ 5 & 4 & 0 & 1 & 2 & 3 \end{array} \quad \text{und} \quad B = \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 0 & 1 \\ 1 & 0 & 3 & 2 & 5 & 4 \\ 5 & 4 & 0 & 1 & 3 & 2 \\ 3 & 2 & 5 & 4 & 1 & 0 \\ 4 & 5 & 1 & 0 & 2 & 3 \end{array}$$

→ A und B sind ein Paar von lateinischen Quadraten, die am nächsten an „paarweise Orthogonalität" herankommen.
Mit $(a_{54}, b_{54}) = (2,2) = (a_{02}, b_{02})$ und $(a_{55}, b_{55}) = (3,3) = (a_{03}, b_{03})$

Da ansonsten alle anderen Tupel paarweise verschieden sind folgt

$\{(i,j,a_{ij},b_{ij}) \mid (i,j) \in (\mathbb{F}_6)^2, (i,j) \neq (5,4) \text{ oder } (5,5)\}$
ist ein $(4,34,3)$-Code.

Angenommen, es gäbe ein $(4,35,3)$-Code C über $\mathbb{F}_6$, dann hätte C die Form

$$\{(i,j,a_{ij},b_{ij}) \mid (i,j) \in (\mathbb{F}_6)^2, (i,j) \neq (i_0,j_0)\}, \text{ für ein}$$

$(i_0,j_0) \in (\mathbb{F}_6)^2$.
Dann sind $A=[a_{ij}]$ und $B=[b_{ij}]$ zwei 6×6 arrays, bei denen der (i_0,j_0)-te Eintrag fehlt.
$\Rightarrow$ Bis auf (i_0,j_0) sind A und B ein Paar von paarweise orthogonalen lateinischen Quadraten
$\Rightarrow$ unter den 6^2 vielen Tupeln taucht ein eindeutig bestimmtes Tupel (x,y) nicht auf.
$\Rightarrow$ Da A und B bis auf den (i_0,j_0)-ten Eintrag lateinische Quadrate sind, folgt, dass in A und in B alle Elemente bis auf x 6-mal in A bzw. y in B vorkommt

$$- \quad - \quad \underset{\uparrow}{x} \quad - \quad - \quad x$$

$\Rightarrow a_{i_0j_0}=x$, $b_{i_0j_0}=y$
$\Rightarrow$ Angenommen in der Zeile i_0 würde x schon einmal vorkommen: $\exists z \in \mathbb{F}_6 \setminus \{x\}$ s.d. z nicht in der i_0-ten Zeile vorkommt
$\Rightarrow z$ muss in einer anderen Zeile 2-mal vorkommen $\lightning$

$\Rightarrow$ analog für die Spalten in A
$\Rightarrow$ analog für B

$\Rightarrow$ A, B sind paarweise orthogonal und A, B sind lateinische Quadrate
$\lightning$ Theorem 10.13

Theorem 10.16.:

$A_q(4,3) = q^2 \quad \forall q \neq 2,6$

$A_2(4,3) = 2$

$A_6(4,3) = 34$

Theorem 10.17 (Die Singleton Schranke (1964))

Die Singleton-Schranke ist:

$$A_q(n,d) \leq q^{n-d+1}$$

Beweis: Angenommen C ist ein q-närer (n, M, d)-Code. Wie in Theorem 10.5, können wir die letzten $d-1$ Koordinaten von jedem Codewort „auslöschen", d.h. es reicht die ersten Koordinaten i, $i \leq n-(d-1)$ zu betrachten.

$\Rightarrow$ Unsere verschiedenen M Vektoren haben also die Länge $n-d+1$

$\Rightarrow M \leq q^{n-d+1}$

Mengen von t paarweise orthogonalen lateinischen Quadraten

Definition Eine Menge $\{A_1, A_2, \ldots, A_t\}$ von lateinischen Quadraten der Ordnung q heißt eine Menge von paarweise orthogonalen lateinischen Quadraten, wenn jedes Paar A_i, A_j ein Paar von paarweise orthogonalen lateinischen Quadraten ist $(1 \leq i < j \leq t)$.

Theorem 10.18. Es gibt maximal $q-1$ lateinische Quadrate in jeder Menge von paarweise orthogonalen lateinischen Quadraten der Ordnung q.

Beweis: Sei $A = \{A_1, \dots, A_t\}$ eine Menge von paarweise orthogonalen lateinischen Quadraten der Ordnung q. Wenn wir die Elemente von einem beliebigen A_i, A_j umbenennen, verletzt dies die Orthogonalität von zwei lateinischen Quadrate aus A nicht.
Also seien die Elemente von A_i, $\forall i \in \{0, \dots, t-1\}$ so, dass die erste Zeile $0 \dots q-1$ sei.
Nun betrachte die t Einträge in der zweiten Zeile in der ersten Spalte der t lateinischen Quadrate
Keiner dieser t Einträge kann 0 sein, da $(0,0)$ schon der Eintrag in der ersten Spalte und der ersten Zeile von $A_i A_j$ $\forall i,j \in \{0, \dots, t-1\}$ ist.
Außerdem können keine zwei Einträge dieser t-Einträge dieselben sein (denn wäre ein weiteres Tupel von $A_i A_j$ (r,r) für $r \in \{1, \dots, q-1\}$, dann wären $A_i A_j$ nicht mehr orthogonal.
$\Rightarrow$ $t \leq q-1$.

Definition Wenn eine Menge von $q-1$ paarweise orthogonalen lateinischen Quadraten existiert, dann heißt sie **vollständig**.

Theorem 10.19. Ist q prim, dann existiert eine vollständige Menge von paarweise orthogonalen lateinischen Quadraten der Ordnung q.

Beweis: Sei $GF(q) = \mathbb{F}_q = \{0, \dots, q-1\}$. Seien $A_1, A_2, \dots, A_{q-1}$ $q \times q$ Arrays, wobei $A_k = (a_{ij}^{(k)})$ sei mit

$$a_{ij}^{(k)} = i + k \cdot j \quad , \quad i, k, j \in \mathbb{F}_q \quad , \quad k \neq 0$$

Wie in Theorem 10.8. folgt, dass alle $A_1, \dots, A_{q-1}$ paarweise orthogonal sind, somit folgt $\{A_1, A_2, \dots, A_{q-1}\}$ ist eine vollständige Menge paarweise orthogonaler lateinischer Quadrate.

Theorem 10.20. Ein q-närer $(n, q^2, n-1)$-Code ist äquivalent zu einer Menge mit $n-2$ paarweise orthogonalen lateinischen Quadraten.

Beweis: Wie in Theorem 10.7. können wir einen $(n, q^2, n-1)$-Code C über $\mathbb{F}_q$ als

$$C = \{ (i, j, a_{ij}^{(1)}, a_{ij}^{(2)}, \dots, a_{ij}^{(n-2)}) \mid (i,j) \in (\mathbb{F}_q)^2 \}$$

schreiben.

Es bleibt zu zeigen, dass $d(C) = n-1 \iff \{A_1, A_2, \dots, A_{n-2}\}$, wobei $A_k = [a_{ij}^{(k)}]$, eine Menge paarweise orthogonaler lateinischer Quadrate ist.

$d(C) = n-1 \iff$ für $x = i, j, a_{ij}^{(1)}, \dots, a_{ij}^{(n-2)}$, $y = i', j', a_{i'j'}^{(1)}, \dots, a_{i'j'}^{(n-2)}$ verschiedene Codewörter aus C folgt:

$$(i,j) \neq (i',j') \qquad \forall\, i,i',j,j' \in \mathbb{F}_q,\ i \neq i',\ j \neq j'$$

und $(i, a_{ij}^{(k)}) \neq (i', a_{i'j}^{(k)})$ $\forall\, i, i', j \in \mathbb{F}_q,\ i \neq i'$

und $(j, a_{ij}^{(k)}) \neq (j', a_{ij'}^{(k)})$ $\forall\, i, j, j' \in \mathbb{F}_q$, $j \neq j'$

und $(a_{ij}^{(k)}, a_{ij}^{(k')}) \neq (a_{ij}^{(\ell)}, a_{ij}^{(\ell')})$ $\forall\, k, k', \ell, \ell' \in \mathbb{F}_q$ wobei $k \neq \ell$, $k \neq k'$, $\ell \neq \ell'$

$\Rightarrow$

$d(C) = n-1 \iff \forall\, A_k, A_{k'}$ gilt: $A_k, A_{k'}$ sind paarweise orthogonal und lateinische Quadrate

$\iff \{A_1, \dots, A_{n-2}\}$ Menge von paarweise orthogonalen lateinischen Quadraten

Korollar 10.21: $A_q(3,2) = q^2 \qquad \forall\, q \in \mathbb{N}$

Beweis: Der $(3, q^2, 2)$-Code ist äquivalent zu einem lateinischen Quadrat der Ordnung q (ex. nach Theorem 10.2)

Nach der Singleton-Schranke gilt $(i\ j\ \underline{a_{ij}})$

$$A_q(3,2) \leq q^{3-2+1} = q^2 .$$

Korollar 10.22. Ist q prim und $n \leq q+1$, dann folgt

$$A_q(n, n-1) = q^2$$

Beweis: Nach der Singleton-Schranke folgt: $A_q(n, n-1) \leq q^{n-(n-1)+1} = q^2$
Nach Theorem 10.19 existiert eine vollständige Menge von paarweise orthogonalen lateinischen Quadraten der Ordnung q, da q prim.
Nach Theorem 10.20 ist diese vollständige Menge äquivalent zu einem q-nären $(n, q^2, n-1)$ Code.
$\Rightarrow A_q(n, n-1) = q^2$.