MITTEILUNGEN

aus dem

MATHEM. SEMINAR GIESSEN

Herausgegeben von den Professoren
des Mathematischen Instituts der Universität Giessen

Geschäftsführung: D. Gaier, G. Pickert

Heft 149

Herrn Professor Hermann Boerner

zum 75. Geburtstag gewidmet

GIESSEN 1981

SELBSTVERLAG DES MATHEMATISCHEN INSTITUTS
ISSN 0373 - 8221 CODEN: MMUGAU

EINIGE NEUE DIFFERENZENMATRIZEN

Dieter Jungnickel

Herrn Professor H. Boerner zum 75. Geburtstag gewidmet.

Eines der interessantesten und schwierigsten Probleme der Kombinatorik ist die Bestimmung der Maximalzahl $N(n)$ von paarweise orthogonalen lateinischen Quadraten (MOLS) der Ordnung n. Bekanntlich ist für $n > 1$ stets $N(n) \leq n-1$; Gleichheit gilt genau dann, wenn eine projektive Ebene der Ordnung n existiert, also insbesondere für Primzahlpotenzen n. Der einzige weitere bekannte Wert von $N(n)$ ist $N(6) = 1$ (Tarry[14]). Wir verwenden die Konvention $N(1) = \infty$. Eine Möglichkeit der Konstruktion von MOLS bieten die vom Verfasser in [8] eingeführten Differenzenmatrizen, die allerdings in äquivalenter Form schon von Dulmage, Johnson & Mendelsohn [5] zum Nachweis von $N(12) \geq 5$ benutzt worden sind. Wir wiederholen die Definition: G sei eine additiv geschriebene Gruppe der Ordnung n und $D = (d_{ij})$ $(i = 1,\ldots,k;\ \ j = 1,\ldots,n)$ eine Matrix mit Einträgen aus G. Dann heißt D eine $(n,k;G)$-Differenzenmatrix, wenn gilt:

(1) $\quad \{d_{ij}-d_{hj}\colon j=1,\ldots,n\} = G \quad$ für alle $i,h = 1,\ldots,k$ mit $i \neq h$.

Wir bemerken, daß wir in [8] den Parameter k durch $k-1$ ersetzt haben; die jetzige Notation stimmt mit der in [1] und [9] überein. Der allgemeinere Fall mehrfach auftretender Differenzen (wie in [9]) wird hier nicht benötigt. Es gilt nun:

Lemma

Die Existenz einer $(n,k;G)$-Differenzenmatrix impliziert die Existenz von $k-1$ MOLS der Ordnung n.

Differenzenmatrizen erlauben es aber nicht nur, den Rechenaufwand bei der Konstruktion von MOLS zu verringern (z.B. ist die Multiplikationstafel eines endlichen Körpers $GF(q)$ offenbar eine Differenzenmatrix für $(GF(q),+)$, was unmittelbar $N(q)=q-1$ liefert), sondern liefern auch besonders "schöne" MOLS: Die Gruppe G operiert als eine Automorphismengruppe der so konstruierten MOLS, die in [8] "regulär" genannt worden sind; dort findet man auch einen Äquivalenzsatz hierzu. (Wesentlich anschaulicher lassen sich die Differenzenmatrizen allerdings interpretieren, wenn man anstelle lateinischer Quadrate die "transversal designs" verwendet: G operiert dann regulär auf jeder Punktklasse des entsprechenden TD's, vgl. [8] und [9] . Dies wird auch - wie der gesamte hier angesprochene Themenkreis - ausführlich im Buch Beth, Jungnickel & Lenz [1] behandelt; eine nicht mehr ganz aktuelle Darstellung dieser Fragen findet sich auch in Hall [6]). Wir wollen nun für eine gegebene Gruppe G mit $R(G)$ den Maximalwert von k bezeichnen, für den eine $(|G|,k+1;G)$-Differenzenmatrix existiert, und mit $R(n)$ den Maximalwert von k, für den eine $(n,k+1;G)$-Differenzenmatrix in irgendeiner Gruppe G der Ordnung n existiert. In dieser Notation lautet das erwähnte Ergebnis in [4] also $R(12) \geq 5$. Wir vereinbaren die Konvention $R(1) = \infty$. Trivialerweise ist dann

(2) $\qquad R(n) \leq N(n) \qquad$ für alle n;

weiter gilt (vgl. [8])

(3) $\qquad R(n) = 1 \qquad$ für $n \equiv 2 \bmod 4$.

(3) ist ein Spezialfall des bekannten Satzes von Hall & Paige [7] über "complete mappings" und zeigt, daß die Eulersche Vermutung (nämlich $N(n) = 1$ für $n \equiv 2 \bmod 4$) für Differenzenmatrizen gilt, während sie bekanntlich für MOLS falsch ist: Nach Bose, Shrikhande & Parker [2] gilt $N(n) \geq 2$ für $n \neq 2,6$. Weiter zeigt man leicht

(4) $R(G \oplus G') \geq R(G)R(G')$

und daher wegen $R(q) = q-1$ für Primzahlpotenzen q

(5) $R(p_1^{e_1} \dots p_s^{e_s}) \geq \min \{p_i^{e_i}-1 : i=1,\dots,s\}$, wobei die p_i paarweise verschiedene Primzahlen seien;

das ist das Analogon des bekannten Satzes von McNeish für Differenzenmatrizen (vgl. [8]). Die McNeish'sche Vermutung (nämlich die Gültigkeit der Gleichheit in (6), sogar für N statt R) ist auch für R falsch, wie das oben erwähnte Ergebnis $R(12) \geq 5$ zeigt; weitere Beispiele dafür werden wir hier mit Hilfe projektiver und affiner Räume konstruieren. Diese Resultate verallgemeinern Ergebnisse aus [8] für projektive bzw. affine Ebenen. Zuvor sei jedoch noch das folgende Ergebnis von Bose, Shrikhande & Parker [2] erwähnt: Die Existenz eines PBDs (also einer Inzidenzstruktur, in der je zwei Punkte eine eindeutige Verbindungsgerade besitzen) auf v Punkten mit Geradengrößen $k_1,\dots,k_r$ impliziert $N(v) \geq \min \{N(k_i)-1 : i=1,\dots,r\}$; sind dabei die Geraden der Größen $k_1,\dots,k_l$ noch paarweise disjunkt, gilt sogar $N(v) \geq \min \{N(k_1),\dots,N(k_l), N(k_{l+1})-1,\dots,N(k_r)-1\}$. Aus der Existenz der projektiven bzw. affinen Geometrien über den endlichen Körpern $GF(q)$ (q Primzahlpotenz) folgen somit

(6) $N(q^d+\dots+q+1) \geq N(q+1)-1$

und

(7) $\quad N(q^d-1) \geq N(q-1)$

für alle $d \in \mathbb{N}$ und alle Primzahlpotenzen q (für(7) wird dabei noch ein Punkt aus AG(d,q) entfernt). Wir wollen nun Analoga von (6) und (7) für Differenzenmatrizen herleiten und dabei die Schranke in (6) um 1 verbessern.

Satz 1

q sei eine Primzahlpotenz, $d \in \mathbb{N}$ und $G = C_v$ die zyklische Gruppe der Ordnung $v = q^d+\ldots+q+1$. Dann gelten:

(8) $$R(G) \geq \begin{cases} N(q+1) & \text{für gerades } d \\ R(C_{q+1}) & \text{für ungerades } d \end{cases}$$

sowie stets

(9) $\quad N(q^d+\ldots+q+1) \geq N(q+1)$.

Insbesondere gilt

(10) $\quad N(q^d+\ldots+q+1) \geq q$,

falls sowohl q als auch q+1 Primzahlpotenzen sind.

Beweis. Nach dem Satz von Singer [13] läßt $\mathcal{P}$= PG(d,q) die Gruppe G als eine auf den Punkten (wie auf den Hyperebenen) reguläre Kollineationsgruppe zu; nach Wahl eines "Basispunktes" können dann die Punkte von $\mathcal{P}$ mit den Elementen von G identifiziert werden. Wir wollen die Bahnen von G auf den Geraden von $\mathcal{P}$ untersuchen. Falls $g \in G$ eine Gerade L festläßt, muß die Ordnung o(g) von g wegen der Regularität von G ein gemeinsamer Teiler von v und q+1 sein; falls d gerade ist, folgt o(g)=1 und G operiert regulär auf jeder Geradenbahn. Wählt man daher in jeder der Bahnen eine beliebige Gerade als "Startgerade" aus, so erhält man eine (v,q+1,1)-Differenzenfamilie

$\mathcal{D} = \{D_1,\dots,D_s\}$ mit $s = b/v$, wobei b die Anzahl der Geraden von $\mathcal{P}$ sei. Die Differenzen $x - x'$ mit $x \neq x'$, $x,x' \in D_i$ $(i = 1,\dots,s)$ enthalten also jedes von 0 verschiedene Element von G genau einmal (zu Differenzenfamilien vergleiche man [1] oder [6]).

Sei nun d ungerade. Wir fassen (wie im üblichen Beweis des Satzes von Singer, vgl. [1] oder [6]) $\mathcal{P}$ als den Unterraumverband von $GF(q^{d+1})$ als Vektorraum über GF(q) auf; dann ist $GF(q^2)$, das für ungerades d ja ein Unterkörper von $GF(q^{d+1})$ ist, eine Gerade von $\mathcal{P}$. Der Beweis des Satzes von Singer zeigt nun, daß die eindeutig bestimmte Untergruppe H der Ordnung q+1 von G die Gerade $GF(q^2)$ festläßt; der Startblock H ist also eine Gerade von $\mathcal{P}$, deren Bahn nur die Länge v/(q+1) hat. Falls nun $g \in G$ irgendeine Gerade L festläßt, ist mit x stets auch $x + g$ in L; diese Punkte sind aber bereits durch die Gerade $H + x$ verbunden, da o(g) ein Teiler von $q + 1$ ist und daher $g \in H$ gelten muß. Somit operiert G auf allen anderen Geradenbahnen regulär. Wenn wir in diesen Bahnen wieder Startgeraden $D_1,\dots,D_s$ wählen (diesmal mit $s = \frac{b}{v} - \frac{1}{q+1}$), so erhalten wir für ungerades d eine "partielle" (v,q+1,1)-Differenzenfamilie $\mathcal{D}$: jedes Element aus $G \setminus H$ kommt genau einmal unter den Differenzen aus $\mathcal{D}$ vor.

Wir wollen nun die Familie $\mathcal{D}$ zur Konstruktion der gewünschten Differenzenmatrizen verwenden. Es sei $N(q+1) = k$ bzw. $R(C_{q+1}) = k$; in beiden Fällen gibt es insbesondere k MOLS der Ordnung q+1 und daher ein "orthogonal array" OA(k+2;q+1) (man vergleiche hierzu [1] oder [6]), etwa auf den Symbolen 1,...,q+1. Nach Weglassen einer Zeile erhält man daraus ein OA(k+1;q+1), dessen letzte q+1 Spalten (durch Symbolumbenennung in jeder Zeile) als $(i,\dots,i)^T$ $(i = 1,\dots,q+1)$ angenommen werden können (geometrisch bedeutet dies den Übergang zu einem auflösbaren TD durch Weglassen einer Punktklasse des ursprünglichen TD's). Läßt man diese $q+1$ Spalten weg, ergibt sich eine $(k+1)\times(q^2+q)$-Matrix $A=(a_{ij})$ mit folgender Eigenschaft: Für je zwei Indizes h,i enthalten die Paare (a_{hj},a_{ij}) jedes geordnete Paar aus verschiedenen Elementen von $\{1,\dots,q+1\}$ genau einmal. Es sei nun $D=\{d_1,\dots,d_{q+1}\}$ eine Teilmenge von G; wenn man dann jeden Eintrag i von A durch d_i ersetzt, so enthalten die Differenzen $b_{hj}-b_{ij}$ $(j=1,\dots,q^2+q)$ für je zwei Zeilen der so entstandenen Matrix $B=(b_{ij})$ über G jedes Element von G genau so oft, wie es als Differenz aus D vorkommt.

Wir führen diese Konstruktion für $D=D_1,\dots,D_s$ durch und erhalten $(k+1)\times(q^2+q)$-Matrizen $B_1,\dots,B_s$ über G; es sei $C=(B_1\ \dots\ B_s)$. Ist dann d gerade, so ergeben je zwei Zeilen von C (da ja $\mathcal{D}$ eine Differenzenfamilie war) als Differenzen alle Elemente $\neq 0$ von G (und zwar je einmal). Wenn wir an C noch eine Spalte aus Nullen anfügen, erhalten wir die gewünschte $(v,k+1;G)$-Differenzenmatrix. Ist d dagegen ungerade, so enthalten die Differenzen je zweier Zeilen von C jedes Element von $G\setminus H$ genau einmal; wenn wir nun die nach Voraussetzung existierende $(q+1,k+1;H)$-Differenzenmatrix an C anfügen, bekommen wir wieder eine $(v,k+1;G)$-Differenzenmatrix. Damit ist die Gültigkeit von (8) nachgewiesen; hieraus folgt für gerades d unmittelbar (9) und dann direkt (10).

Es bleibt noch (9) für ungerade d zu beweisen. Dazu bilden wir die Matrix $M=(C\ \ C+g_2\ \dots\ C+g_v)$, wobei $g_2,\dots,g_v$ die von D verschiedenen Elemente von G seien; man sieht dann unmittelbar, daß je zwei Zeilen von M alle Paare $(x,y) \in G \times G$ enthalten (und zwar genau einmal), für die die Differenz $x-y$ nicht in H liegt. Nach Voraussetzung existiert weiter ein OA(k+1;q+1), etwa auf der Symbolmenge H; wir fügen die ersten k+1 Zeilen dieses OA an M an und erhalten jetzt in je zwei Zeilen auch alle Paare (x,y) mit $x,y \in H$. Wenn wir entsprechend mit jeder Nebenklasse von H verfahren, ergibt sich schließlich ein OA(k+1;v) M'. Zum endgültigen Nachweis von (9) muß M' noch zu einem OA(k+2;v) erweitert werden. Dazu definieren wir eine neue Zeile wie folgt: jeweils in der x-ten Spalte von C, $C+g_2, \dots, C+g_v$ sei der Eintrag der neuen Zeile x $(x=1,\dots,v-(q+1))$; damit enthalten die i-te und die neue Zeile alle Paare (x,y) mit $x = 1,\dots,v-(q+1)$. Schließlich ersetzen wir für jedes der angefügten OA(k+1;q+1) die Symbole in der (zuvor weggelassenen) (k+2)-ten Zeile in beliebiger Zuordnung durch die Elemente $v-q,\dots,v(=0)$ und erhalten so auch die Paare (x,y) mit $y = v-q,\dots,v$ aus der i-ten und der neuen Zeile. Damit ist der Satz vollständig bewiesen.

Bevor wir Beispiele für die Anwendung von Satz 1 geben, zunächst noch einige Bemerkungen: Der Fall d=2 von Satz 1 ist in [8] enthalten und die Verbesserung von (6) zu (9) geht für $d = 2$ bereits auf Bose, Shrikhande & Parker [2] zurück. Eine etwas schwächere Aussage als (9) steht für den Fall $d = 3$ auch in Lorimer [11], der daraus dann (10) für $d = 3$ erhalten hat. Schließlich sei noch erwähnt, daß (8) für ungerades d nur für gerades q interessant ist, da nach dem Satz von Hall & Paige [7] stets (3) gilt; wenn also q ungerade ist, ist $R(C_{q+1}) = 1$. Insbesondere läßt sich also (10) für ungerades d aus (8) nur für solche Werte von q herleiten, für die $q+1$ eine Fermatsche Primzahl ist.

Nun einige Beispiele zu Satz 1; dabei geben wir nur solche Fälle an, die gegenüber (4) eine verbesserte Schranke liefern. Für $d = 2$ ergeben sich z.B. $R(C_{21}) \geq 4$, $R(C_{57}) \geq 7$, $R(C_{273}) \geq 16$, $R(993) \geq 31$, $R(C_{16257}) \geq 127$. Der Fall $d = 3$ liefert

(11) $\quad N(585) \geq 8;$

dies stellt gegenüber der in Brouwer [3] angegebenen Schranke tatsächlich eine Verbesserung um 1 dar. (Natürlich ist dieses Ergebnis implizit in Lorimer's Arbeit, der es aber nicht bemerkt hat, wie er es überhaupt versäumt hat, seine Schranke mit zuvor bekannten Resultaten zu vergleichen.) Für $d = 3$ ergibt sich auch noch $N(30784) \geq 31$. Für $d \geq 4$ werden die erhaltenen Beispiele so groß, daß wir hier auf die Angabe verzichten wollen. Stattdessen sei noch das Differenzenmatrizenanalog von (7) vorgeführt, dessen Beweis dem von Satz 1 recht ähnlich ist und daher nur skizziert werden soll.

Satz 2

q sei eine Primzahlpotenz, $d \in \mathbb{N}$ und $G = C_v$ die zyklische Gruppe der Ordnung $v = q^d - 1$. Dann gilt:

(12) $\quad R(G) \geq R(C_{q-1})$.

Beweis. $\mathcal{A}$ sei die Inzidenzstruktur, die durch Entfernen des Punktes O und aller Hyperebenen durch O aus $AG(d,q)$ hervorgeht; dann läßt $\mathcal{A}$ die Gruppe G als auf den Punkten (und den restlichen Hyperebenen) reguläre Kollineationsgruppe zu, siehe etwa [10]. Wir betrachten die Bahnen von G auf den Geraden von $AG(d,q)$, die nicht durch O gehen; da q und q^d-1 teilerfremd sind, ist G auf jeder solchen Bahn regulär. Wählen wir in jeder Bahn einen Startblock, so erhalten wir eine "partielle" $(v,q,1)$-Differenzenfamilie $\mathcal{D}$: Jedes Element von G, das nicht in der eindeutig bestimmten Untergruppe der Ordnung q-1 von G liegt, erscheint genau einmal als Differenz aus $\mathcal{D}$. Wir benutzen nun wie im Beweis von Satz 1 k MOLS der Ordnung q (mit $k = R(C_{q-1})$; dies ist möglich, da q Primzahlpotenz ist) zur Konstruktion einer $(k+1) \times (q^2-q)$-Matrix $A = (a_{ij})$, für die je zwei Zeilen alle Paare aus verschiendenen Elementen von $\{1,\ldots,q\}$ enthalten. Sodann ersetzen wir für jeden Startblock $D = \{d_1,\ldots,d_q\}$ von $\mathcal{D}$ wie zuvor jeden Eintrag i von A durch d_i und erhalten so eine Matrix C über G, für die je zwei Zeilen alle Elemente in $G \setminus H$ als Differenzen liefern. Dann ergibt Anfügen einer $(q-1,k+1;H)$-Differenzenmatrix an C die gewünschte $(v,k+1;G)$-Differenzenmatrix.

Der Fall $d=2$ dieses Satzes ist wieder in [8] enthalten. Nun einige Beispiele, wobei sich allerdings wegen (7) keine verbesserten Schranken für N ergeben. Der Fall $d=2$ liefert z.B. $R(C_{255}) \geq 4$ (hierbei wird $R(C_{15}) \geq 4$ verwendet, siehe Schellenberg, Van Rees & Vanstone [12]), $R(C_{1023}) \geq 30$, $R(16383) \geq 126$, aber auch $R(C_{63}) \geq 6$ (zwar gilt $R(63) \geq 6$ auch nach (5), dabei wird aber nicht die zyklische Gruppe der Ordnung 63 verwendet, sondern $C_7 \oplus EA(9)$, wobei EA(v) die elementarabelsche Gruppe der Ordnung v bezeichnet). Für $d = 4$ ergibt sich z.B. $R(C_{4095}) \geq 7$ (gegenüber der nach (4) bekannten Schranke 2 für die zyklische Gruppe, wobei allerdings wieder $R(4095) \geq 4$ auch nach (5) folgt). Auf die Angabe größerer Beispiele sei wieder verzichtet.

Abschließend sei noch bemerkt, daß man in Satz 2 natürlich auch - analog zu Satz 1 - die Schranke $N(q^d-1) \geq N(q-1)$ erhalten kann, die aber nach (7) bereits bekannt und auf einfachere Weise beweisbar ist. Das hier vorgestellte Beweisverfahren läßt sich selbstverständlich auf beliebige "partielle" (v,k,1)-Differenzenfamilien (für die also genau die Elemente einer Untergruppe H von G nicht als Differenzen auftreten, während jedes andere Element genau einmal als Differenz auftritt) verallgemeinern; jedoch scheint dies zur Zeit aus Mangel an interessanten Anwendungen nicht sehr lohnend. Immerhin wollen wir das entsprechende Resultat ohne Beweis mitteilen:

<u>Satz 3</u>

sei eine partielle (v,K,1)-Differenzenfamilie in der Gruppe G bezüglich der Untergruppe H der Ordnung m, d.h. jedes Element in $G \setminus H$ tritt genau einmal und jedes Element in H überhaupt nicht unter den Differenzen aus auf und die Mengen in haben Mächtigkeiten aus K. Dann gelten:

(13) $\quad R(G) \geq R(H)$

und

(14) $\quad N(v) \geq \min(\{N(m)\} \cup \{N(k) : k \in K\})$

Das letzte Beispiel in Brouwer [4] ist eine (469,{9,13,16},1)-Differenzenfamilie in C_{469} und zeigt daher die Existenz einer $(469,9;C_{469})$-Differenzenmatrix.

Literatur

1. T.Beth, D.Jungnickel & H.Lenz: Design Theory I. Erscheint.
2. R.C.Bose, S.S.Shrikhande & E.T.Parker: Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture.
   Canad.J.Math. 12 (1960), 189-203.
3. A.E.Brouwer: The number of mutually orthogonal Latin squares - A table up to order 10,000. Mathematisch Centrum, Amsterdam 1979.
4. A.E.Brouwer: A series of separable designs with application to pairwise orthogonal Latin squares. Europ.J.Comb. 1 (1980), 39-41
5. A.K.Dulmage, D.Johnson & N.S.Mendelsohn: Orthomorphisms of groups and orthogonal Latin squares. Canad.J.Math. 13 (1961), 356-372.
6. M.Hall,Jr.: Combinatorial Theory Blaisdell, 1967.
7. M.Hall,Jr. & L.J.Paige: Complete mappings of finite groups. Pacific J.Math. 5 (1955), 541-549.
8. D.Jungnickel: On difference matrices and regular Latin squares. Abh.Math.Sem. Hamburg 50 (1980), 219-231.
9. D. Jungnickel: On difference matrices, resolvable transversal designs and generalized Hadamard matrices. Math.Z. 167 (1979), 49-60.
10. D.Jungnickel: On automorphism groups of divisible designs. Erscheint.
11. P.Lorimer: A method of constructing mutually orthogonal Latin squares. Nanta Math. 12 (1979), 158-165.
12. P.J.Schellenberg, G.H.J.van Rees & S.A.Vanstone: Four pairwise orthogonal Latin squares of order 15. Ars Combinatoria 8 (1978), 141-150.
13. J.Singer: A theorem in finite projective geometry and some applications to number theory. Trans.Amer.Math.Soc. 43 (1938), 377-385.
14. G.Tarry: Le probleme des 36 officiers. C.R.Assoc.Franc.Avanc.Sci.nat. 2 (1901), 170-203.

D.Jungnickel
Mathematisches Institut
Justus-Liebig-Universität Gießen
Arndtstr. 2
D 6300 Gießen