On difference matrices and regular Latin squares

Dieter Jungnickel

Angaben zur Veröffentlichung / Publication details:

Jungnickel, Dieter. 1980. "On difference matrices and regular Latin squares." *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 50: 219–31. https://doi.org/10.1007/BF02941430.

ABHANDLUNGEN

aus dem Mathematischen Seminar
der Universität Hamburg

Band 50

GÖTTINGEN · VANDENHOECK & RUPRECHT · 1980

Hinweise für Autoren

Manuskripte müssen in völlig druckfertigem Zustand in zweifacher Ausfertigung eingereicht werden. Sie werden maschinengeschrieben mit doppeltem Zeilenabstand und breitem Rand auf einseitig beschriebenen Blättern erbeten. Diagramme und Zeichnungen sollten getrennt vom Text mit chinesischer Tusche in etwa doppelter Größe auf Pergamentpapier gezeichnet werden.

Jedem Manuskript sind auf gesondertem Blatt Anweisungen für den Setzer beizufügen, auf dem ein Kolumnentitel angegeben und die benutzen Kennzeichnungen sowie verwendete besondere Symbole erklärt werden. Dabei sind die folgenden Regeln zu beachten:

Die Wörter „Theorem", „Satz", „Lemma", „Corollar" etc. werden automatisch halbfett gesetzt, ihre Formulierung kursiv (im Manuskript zu unterstreichen). Die Wörter „Beweis", „Bemerkung", „Definition" etc. werden kursiv gesetzt, ihre Formulierung in antiqua.

Unterstreichungen für spezielle Alphabete und Schriftarten sollten nach folgenden Regeln vorgenommen werden:

Einfache (doppelte) farbliche Unterstreichung: Kleiner (großer) Buchstabe.

Schwarz	=	kursiv
gelb	=	geradestehend (besonders wichtig bei Formelbuchstaben, da diese sonst generell kursiv gesetzt werden)
rot	=	griechisch
blau	=	Fraktur (gotisch)
grün	=	Schreibschrift (skript)
braun	=	halbfett kursiv

Diese Farben können auch kombiniert werden.

Neben undeutlicher Unterscheidung zwischen Groß- und Kleinbuchstaben achte man auf häufig auftretende Fehlerquellen, wie z.B. *l* (Buchstabe) und 1 (eins), *0* (Buchstabe) und 0 (Null), x und κ etc.

In den Fahnenabzügen sollen nur Satzfehler verbessert, jedoch keine inhaltlichen oder stilistischen Änderungen vorgenommen werden. Nachträgliche (vom Manuskript abweichende) Korrekturen müssen den Autoren in Rechnung gestellt werden.

Die Autoren werden gebeten, ihre genaue postalische Anschrift anzugeben und eine evtl. Anschriftenänderung — auch vorübergehende — der Schriftleitung in ihrem eigenen Interesse unverzüglich mitzuteilen.

Autoren werden gebeten, Manuskripte bei der Schriftleitung oder bei einem der Redakteure einzureichen. (Adresse für Schriftleitung und Redakteure: Mathematisches Seminar der Universität Hamburg, Bundesstraße 55, D-2000 Hamburg 13.)

ISSN 0025-5858

On Difference Matrices and Regular Latin Squares

By DIETER JUNGNICKEL[1])

1. Introduction

One of the most thoroughly investigated branches of combinatorics is the theory of Latin squares. The outstanding problem has been (and still is) the determination of the maximum number $N(t)$ of pairwise orthogonal Latin squares of order t. One knows $N(q) = q - 1$ for prime powers q; but besides for $N(6) = 1$ these are the only known precise values. In 1922, MACNEISH [9] proved $N(t_1 t_2) \geq \min \{N(t_1), N(t_2)\}$ and conjectured that actually one would have equality, which would imply the validity of Euler's conjecture (stating $N(t) = 1$ whenever $t \equiv 2 \bmod 4$) that was disproved in 1960 by BOSE and SHRIKHANDE [3].

In this paper we will investigate a special class of orthogonal Latin squares, i.e. *regular* sets of pairwise orthogonal Latin squares: these are sets admitting a regular abelian automorphism group on the symbols, such that each automorphism is induced by the same row permutation for any of the given squares (see Definition 2). We will show that the concept of regular Latin squares may be described in an algebraic way by the concept of a difference matrix. A (t, r, G)-*difference matrix* is an $(r + 1) \times t$-matrix D with entries from an abelian group G of order t such that the difference of any two distinct rows of D contains each element of G exactly once (see Definition 1). We prove that the existence of a (t, r, G)-difference matrix is equivalent to the existence of a regular set of r mutually orthogonal Latin squares of order t with G as automorphism group (see Theorem 1).

We remark, that JOHNSON, DULMAGE and MENDELSOHN [8] have used a (12, 5)-difference matrix (without introducing this name) to construct 5 mutually orthogonal Latin squares of order 12. Thus one part of our equivalence theorem is known already. But up to now, emphasis has been on the construction of squares, not on their automorphism group; the aim of this paper is not the construction of squares in general, but the study of sets of squares with a nice automorphism group. We will be able to prove analogues of several well-known existence theorems for Latin squares in general. More specifically, we construct (t, r, G)-difference matrices in the following cases:

---

[1]) These results form parts of the author's doctoral dissertation that has been prepared under the supervision of Prof. Dr. H. Lenz at the Freie Universität Berlin.

(i) t a prime power, $r < t$, $G = EA(t)$ the elementary abelian group of order t;

(ii) $t = p^k$, p a prime, $r < p$, $G = \mathbb{Z}_t$ the cyclic group of order t;

(iii) $t = q^2 + q + 1$, q a prime power, $r \leqslant N(q+1)$, $G = \mathbb{Z}_t$;

(iv) $t = q^2 - 1$, q a prime power, there exists a $(q-1, r, \mathbb{Z}_{q-1})$-difference matrix and $G = \mathbb{Z}_t$;

(v) If there are (t, r, G)- and (t', r, G')-difference matrices, then there is a $(tt', r, G \oplus G')$-difference matrix.

If we denote by $R(t)$ the maximum cardinality of a regular set of pairwise orthogonal Latin squares of order t, we thus have $R(q) = q - 1$ for prime powers q and $R(t_1 t_2) \geqslant \min\{R(t_1), R(t_2)\}$ in analogy to the results on $N(t)$. But there is one startling difference: The class of regular sets of Latin squares satisfies Euler's conjecture: $R(t) = 1$ whenever $t \equiv 2 \bmod 4$ (see Corollary 4). Nevertheless MacNeish's conjecture still is not satisfied, as (iii) above shows (see Remark, p. 225).

This result is in fact a special case of the non-existence theorem of Hall and Paige (there is no complete mapping for a group G with a cyclic Sylow-2-subgroup, see e.g. Denes and Keedwell [5, Theorem 1.4.7]). We feel that our proof of this special case is interesting enough to be included here, as it uses only elementary counting arguments whereas the proof of the general result needs some rather non-trivial group theory. In a remark (see p. 227) we show how our proof of this special case of Hall's and Paige's theorem may be generalized to the non-abelian case.

2. Preliminaries

We refer the reader to the literature regarding the supposed pre-knowledge. As general references we mention [4], [7] and [11]. For latin squares, one may also consult [5]; for groups [6] and [12]; for difference sets [7, Ch. 11]; for affine difference sets [2].

3. Basic Results

Definition 1. Let G denote any abelian group of order t and let D be an $(r+1) \times t$-matrix over G satisfying

(DM) $\{d_{i1} - d_{j1}, d_{i2} - d_{j2}, \ldots, d_{it} - d_{jt}\} = G$ for all $i, j = 0, \ldots, r$ with $i \neq j$,

i.e., the difference of any two rows of D contains every element of G (exactly once for reasons of cardinality). Then D is called a (t, r, G)-*difference matrix*.

If D furthermore satisfies

(N_1) $$d_{r1} = d_{r2} = \cdots = d_{rt} = 0$$

and

$$(N_2) \qquad d_{0t} = d_{1t} = \cdots = d_{rt} = 0,$$

then D is called *normal.*

Proposition 1. *Let D be a (t, r, G)-difference matrix and let D' arise from D by transformation of the following kind:*

(a) *line permutations;*

(b) *addition of a fixed $a \in G$ to a column of D;*

(c) *addition of a fixed $a \in G$ to a row of D.*

Then D' is a (t, r, G)-difference matrix.

Proof. These operations do not change property (DM).

Corollary 1. *With any difference matrix D there is associated a normal difference matrix D' obtained from D by transformations of the types described in Proposition 1. D' furthermore satisfies*

(N_3) *Each row of D' (except for the last row) contains every element of G exactly once.*

(N_4) *No column of D' (except for the last column) contains an element of G twice.*

Proof. (N_1) may be achieved by operations of type (b), (N_2) by operations of type (c). (N_3) holds by (DM), for the difference between the ith and the rth row is simply the ith row by (N_1). (N_4) holds by (DM); for we must have $d_{ik} - d_{jk} \neq 0$ $(k \neq t, i \neq j)$ since already $d_{it} - d_{jt} = 0 - 0 = 0$ by (N_2).

Example 1.

$$G = \mathbb{Z}_3, r = 2 \qquad G = \mathbb{Z}_5, r = 4$$

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 2 & 4 & 3 & 1 & 0 \\ 4 & 3 & 1 & 2 & 0 \\ 3 & 1 & 2 & 4 & 0 \\ 1 & 2 & 4 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$G = GF(4), r = 3$, w generating element of $GF(4)^*$

$$\begin{pmatrix} w & w^2 & 1 & 0 \\ w^2 & 1 & w & 0 \\ 1 & w & w^2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Definition 2. Let $\mathfrak{A} = \{A_1, \ldots, A_n\}$ be a set of mutually orthogonal $t \times t$-matrices on the symbol set $S = \{s_1, \ldots, s_t\}$. Let G be a regular

abelian permutation group on S. If for each $\alpha \in G$ there is a permutation π of the cells (i, k) such that for each $j = 1, \ldots, n$

$$(a_{ik}^j)^\alpha = a_{hl}^j \quad \text{where } (i, k)^\pi = (h, l),$$

then $\mathfrak{A}$ is called *G-quasiregular*. If the permutations π are in fact permutations of the form $(i, k) \to (\sigma i, k)$ where σ is a permutation of $\{1, \ldots, t\}$, then $\mathfrak{A}$ is called *G-regular*. $\mathfrak{A}$ is called *(quasi-)regular*, if it is G-(quasi-) regular for some group G.

Theorem 1. *Let t,r be natural numbers and G an abelian group. Then the following statements are equivalent:*

(a) *There exists a (t, r, G)-difference matrix.*
(b) *There exists a G-regular set of $r + 1$ mutually orthogonal $t \times t$-matrices, r of which are Latin squares.*
(c) *There exists a G-quasiregular set of $r + 1$ mutually orthogonal $t \times t$-matrices, r of which are Latin squares.*
(d) *There exists a G-quasiregular set of $r + 1$ mutually orthogonal $t \times t$-matrices.*
(e) *There exists a G-regular set of r mutually orthogonal Latin squares.*

Proof

I. $(a) \Rightarrow (b)$. Let D be a (t, r, G)-difference matrix and let $a_1 := 0$ and $a_2, \ldots, a_t$ be the non-zero elements of G. For $i = 0, \ldots, r$ define the $t \times t$-matrix $A_i = (a_{hk}^i)$ by

$$a_{hk}^i := d_{ik} + a_h.$$

The matrices thus defined are mutually orthogonal; for consider A_i and A_j $(i \neq j)$ and let (x, y) be any pair of elements of G. Let $d := x - y$. By (DM), d occurs exactly once as a difference $d = d_{ik} - d_{jk}$. Let $-d_{ik} + x := a_h$. Then we have

$$a_{hk}^i = d_{ik} + a_h = d_{ik} - d_{ik} + x = x$$

and

$$a_{hk}^j = d_{jk} + a_h = d_{jk} - d_{ik} + x = y.$$

Thus $\{(a_{hk}^i, a_{hk}^j): h, k = 1, \ldots, t\} = G \times G$, i.e. A_i and A_j are orthogonal.

For each $g \in G$, we let g act on G by $x^g := x + g$ (for each $x \in G$). Thus G clearly acts as a regular permutation group on itself. We assert, that our matrices defined above are G-regular; for consider any element of G, $g = a_l$ say. Denote $a_h + a_l := a_{h'}$. Then

$$(a_{hk}^i)^g = (d_{ik} + a_h)^g = d_{ik} + a_h + a_l = d_{ik} + a_{h'} = a_{h'k}^i$$

i.e.

$$(a_{hk}^i)^g = a_{mn}^i \quad \text{where } (m, n) = (h, k)^\pi$$

and the permutation π of the cells is defined by $(h, k)^\pi := (h', k)$. Finally we observe, that $A_0, \ldots, A_{r-1}$ are Latin squares (to this purpose we

assume w.l.o.g. D to be normal according to Corollary 1): Consider a fixed $i \neq r$. By (N_3) (and since G is a group) each row of A_i contains each element of G exactly once. Since also each column of A_i contains each element of G exactly once (since it is of the form $d_{ik} + G$), A_i is a Latin square.

II. $(b) \Rightarrow (c)$ trivial.

III. $(c) \Rightarrow (d)$ trivial.

IV. $(d) \Rightarrow (a)$. Let $A_0, \ldots, A_r$ be mutually orthogonal $t \times t$-matrices on the symbol set S, that are G-quasiregular. Since G is regular on S, we may identify S and G and consider S as an abelian group: After choosing a fixed element $0 \in S$, we identify the element $s \in S$ with the uniquely determined $\alpha_s \in G$ with $0^{\alpha_s} = s$. Then we may write $s + g$ instead of s^g for $s \in S$, $g \in G$. Let $a_1 := 0$ and $a_2, \ldots, a_t$ be the elements of $S = G$. Since a G-quasiregular set of mutually orthogonal matrices obviously is transformed into a G-quasiregular set of mutually orthogonal matrices by permuting the cells, we may assume w.l.o.g. that we have

$$a^r_{11} = a^r_{12} = \cdots = a^r_{1t} = 0.$$

By hypothesis, there are permutations $\sigma_h (h = 1, \ldots, t)$ of the t^2 cells such that

$$a^i_{jk} + a_h = a^i_{\sigma_h(j,k)} \quad \text{for } i = 0, \ldots, r,$$

in particular

$$a_h = a^r_{1k} + a_h = a^r_{\sigma_h(1,k)}.$$

After another appropriate permutation of the cells we may assume w.l.o.g. that

$$\sigma_h(1, k) = (h, k),$$

hence

$$a^i_{hk} = a^i_{1k} + a_h \quad \text{for each } i = 0, \ldots, r.$$

We now define the $(r + 1) \times t$-matrix $D = (d_{ik})$ by putting

$$d_{ik} := a^i_{1k} \quad (i = 0, \ldots, r; k = 1, \ldots, t).$$

Consider rows i and j $(i \neq j)$ of D. Since A_i and A_j are orthogonal, the pair $(x, 0) \in G \times G$ occurs (exactly once) as (a^i_{hk}, a^j_{hk}), i.e.

$$x = a^i_{hk} = a^i_{1k} + a_h = d_{ik} + a_h$$
$$0 = a^j_{hk} = a^j_{1k} + a_h = d_{jk} + a_h$$

i.e. $x = x - 0 = d_{ik} - d_{jk}$. Thus the difference of rows i and j has to contain each element of G (exactly once), i.e. D is a (t, r, G)-difference matrix.

V. $(b) \Rightarrow (e)$ trivial.

VI. $(e) \Rightarrow (b)$. Let $A_0, \ldots, A_{r-1}$ be a G-regular set of mutually orthogonal Latin squares. Define $A = (a^r_{ik})$ by

$$a^r_{i1} = a^r_{i2} = \cdots = a^r_{it} := a^0_{it}$$

Since $A_0, \ldots, A_{r-1}$ are Latin squares, clearly $A_0, \ldots, A_r$ are a set of mutually orthogonal $t \times t$-matrices, r of which are Latin squares. It remains to show that this set is G-regular. For every $a \in G$ there is a row permutation σ_a such that for $j < r$ and every i, k

$$a^j_{ik} + a = a^j_{\sigma_a i,k},$$

in particular

$$a^0_{it} + a = a^0_{\sigma_a i,t},$$

that is

$$a^r_{ik} + a = a^r_{\sigma_a i,k}, \quad \text{q.e.d.}$$

Example 2. Using the example for $t = 5$, $r = 4$ in Example 1, the construction of theorem 1 yields the following 4 orthogonal Latin squares of order 5 (taking $a_h := h - 1$):

$$\begin{pmatrix} 2 & 4 & 3 & 1 & 0 \\ 3 & 0 & 4 & 2 & 1 \\ 4 & 1 & 0 & 3 & 2 \\ 0 & 2 & 1 & 4 & 3 \\ 1 & 3 & 2 & 0 & 4 \end{pmatrix} \begin{pmatrix} 4 & 3 & 1 & 2 & 0 \\ 0 & 4 & 2 & 3 & 1 \\ 1 & 0 & 3 & 4 & 2 \\ 2 & 1 & 4 & 0 & 3 \\ 3 & 2 & 0 & 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 1 & 2 & 4 & 0 \\ 4 & 2 & 3 & 0 & 1 \\ 0 & 3 & 4 & 1 & 2 \\ 1 & 4 & 0 & 2 & 3 \\ 2 & 0 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 4 & 3 & 0 \\ 2 & 3 & 0 & 4 & 1 \\ 3 & 4 & 1 & 0 & 2 \\ 4 & 0 & 2 & 1 & 3 \\ 0 & 1 & 3 & 2 & 4 \end{pmatrix}$$

plus the square A

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 & 4 \end{pmatrix}$$

admitting $\mathbb{Z}_5$ as regular automorphism group.

4. Existence Results

Theorem 2. *Let t be a prime power and $EA(t)$ the elementary abelian group of order t. Then there exists a $(t, r, EA(t))$-difference matrix whenever $r \leqslant t - 1$.*

Proof: Note that there cannot be a $(t, r, EA(t))$-difference matrix with $r \geqslant t$ by (N_4). Consider $EA(t)$ as the additive group of the Galois field $F := GF(t)$. Let w be a generating element of F^* and define the $(r + 1) \times t$-matrix D by $D = (d_{ik})$ $(i = 0, \ldots, r;\ k = 1, \ldots, t)$ with

$$d_{ik} := \begin{cases} 0 & \text{if } i = r \text{ or } k = t \\ w^{i+k} & \text{otherwise} \end{cases}$$

i.e.

$$D = \begin{pmatrix} w & w^2 & w^3 & \cdots & w^{t+1} & 0 \\ w^2 & w^3 & w^4 & \cdots & w^t & 0 \\ \vdots & & & & & \vdots \\ w^r & w^{r+1} & w^{r+2} & \cdots & w^{t+r-2} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

(Note that $w^{t-1} = 1$).

It is easy to show that D satisfies property (DM) of Definition 1.

Theorem 3. *Let $t = p^n$ be a prime power and let $r \leqslant p - 1$. Then there exists a $(t, r, \mathbb{Z}_{p^n})$-difference matrix.*

Proof. Define the $(r + 1) \times t$-matrix $D = (d_{ik})$ $(i = 0, \ldots, r; k = 1, \ldots, t)$ by

$$d_{ik} := \begin{cases} 0 & \text{if } i = r \text{ or } k = t \\ (i + 1)k & \text{otherwise} \end{cases}$$

(everything mod p^n), i.e.

$$D = \begin{pmatrix} 1 & 2 & 3 & \cdots & p^n - 1 & 0 \\ 2 & 4 & 6 & \cdots & 2(p^n - 1) & 0 \\ \vdots & & & & & \vdots \\ \mathrm{r} & 2r & 3r & \cdots & r(p^n - 1) & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

It is easily seen that D is a difference matrix.

Theorem 4. *If there exist a (t, r, G)-difference matrix and a (tt', r, G')-difference matrix, then there exists an $(tt', r, G \oplus G')$-difference matrix.*

Proof. Let $D = (d_{ik})$ be a (t, r, G)-difference matrix and $D' = (d'_{ik})$ be a (t', r, G')-difference matrix. Define an $(r + 1) \times tt'$-matrix $D'' = D \oplus D'$ over $G \oplus G'$ by

$$d''_{ik} := (d_{i,\alpha k}, d'_{i,k-(\alpha k-1)t'}) \quad (i = 0, \ldots, r; k = 1, \ldots, tt')$$

where αk denotes the smallest integer $\geqslant k/t'$. Hence we obtain

$$\begin{pmatrix} (d_{01}, d'_{01}) \ldots (d_{01}, d'_{0t'}) & \cdots & (d_{0t}, d'_{01}) \ldots (d_{0t}, d'_{0t'}) \\ \vdots & & \vdots \\ (d_{r1}, d'_{r1}) \ldots (d_{r1}, d'_{rt'}) & \cdots & (d_{rt}, d'_{r1}) \ldots (d_{rt}, d'_{rt'}) \end{pmatrix}$$

D'' satisfies (DM): For suppose that $d''_{ik} - d''_{jk} = d''_{il} - d''_{jl}$ $(i \neq j)$. Then

$$d_{i,\alpha k} - d_{j,\alpha k} = d_{i,\alpha l} - d_{j,\alpha l}$$

and

$$d'_{i,k-(\alpha k-1)t'} - d'_{j,k-(\alpha k-1)t'} = d'_{i,l-(\alpha l-1)t'} - d'_{j,l-(\alpha l-1)t'}.$$

Since D is a difference matrix, we must have $\alpha k = \alpha l$. Since D' is a difference matrix, we must have $k - (\alpha k - 1)t' = l - (\alpha l - 1)t'$. Both conditions together yield at once $k = l$. Hence D'' satisfies (DM) and is thus a difference matrix. If D and D' are normal, so obviously is D''.

Example 3. We consider the following difference matrices over $\mathbb{Z}_3$ and $\mathbb{Z}_5$ ($r = 2$):

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 2 & 4 & 3 & 1 & 0 \\ 4 & 3 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The construction in Theorem 4 yields the following difference matrix over $\mathbb{Z}_{15} = \mathbb{Z}_3 \oplus \mathbb{Z}_5$ (we write x_y instead of (x, y)):

$$\begin{pmatrix} 2_2 & 2_4 & 2_3 & 2_1 & 2_0 & 1_2 & 1_4 & 1_3 & 1_1 & 1_0 & 0_2 & 0_4 & 0_3 & 0_1 & 0_0 \\ 1_4 & 1_3 & 1_1 & 1_2 & 1_0 & 2_4 & 2_3 & 2_1 & 2_2 & 2_0 & 0_4 & 0_3 & 0_1 & 0_2 & 0_0 \\ 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 & 0_0 \end{pmatrix}$$

Corollary 2. *Let $t = q_1 \ldots q_n$ where the q_i are prime powers and let $r \leqslant q_i - 1$ for $i = 1, \ldots, n$. Then there exists a $(t, r, EA(q_1) \oplus \cdots \oplus EA(q_n))$-difference matrix.*

Corollary 3. *Let G be any abelian group of order t. Let $t = p_1^{n_1} \ldots p_k^{n_k}$ be the prime power factorization of t; let $p := \min\{p_1, \ldots, p_k\}$ and $q := \min\{p_1^{n_1}, \ldots, p_k^{n_k}\}$. G is the direct sum of cyclic p_i-groups ($i = 1, \ldots, k$; cf.* [6, p. 40]); *if all these groups are elementary abelian, there exist (t, r, G)-difference matrices for at least $0 \leqslant r \leqslant q - 1$, otherwise for at least $0 \leqslant r \leqslant p - 1$.*

Theorem 5. *Let $t = 2n$ with $(n, 2) = t$. Then there cannot exist a $(t, 2, G)$-difference matrix.*

Proof. Assume that D is a $(t, 2)$-difference matrix over G. Since $(2, n) = 1$, by the fundamental theorem on abelian groups $G = \mathbb{Z}_2 \oplus G_n$ for some abelian group G_n. Thus the elements of G have the form $(0, x)$ resp. $(1, x)$ (with $x \in G_n$). We assume D to be normal by Corollary 1 and consider the differences between the zeroth and the 1st row of D. n of these elements must be of the form $(0, x)$ and the remaining n of the form $(1, x)$. Suppose that there are u elements $(0, x)$ below elements $(0, x')$. Since these yield u differences with first component 0, we must have $n - u$ elements $(1, x)$ below $n - u$ elements $(1, x')$ to get the remaining $n - u$ differences with first component 0. The remaining $n - u$ elements $(0, x)$ must be below the remaining u elements $(1, x')$, which yields $n - u = u$ or $2u = n$, contradicting $(n, 2) = 1$. Hence there cannot exist a $(t, 2)$-difference matrix.

Corollary 4. *The class of regular Latin squares satisfies Euler's conjecture: If $t \equiv 2 \bmod 4$, there cannot be a regular set of 2 orthogonal Latin squares.*

Remarks

a. The construction given in Theorem 2 occurs in an equivalent though different form already in [1].

b. Corollary 4 shows that the class RMOLS of regular sets of mutually orthogonal Latin squares is a proper subclass of the class MOLS of sets of mutually orthogonal Latin squares (see [3]) and $R(t) < N(t)$ for $6 < t \equiv 2 \bmod 4$. Open question: For which t is $R(t) < N(t)$?

c. Corollary 2 shows that the class RMOLS satisfies the theorem of MACNEISH as known for the class MOLS (if $t = q_1 \cdots q_n$ is the prime power factorization of t and $r \leqslant q_i - 1$ for $i = 1, \ldots, n$ then there exist $r - 1$ mutually orthogonal Latin squares of order t). In 1922, MACNEISH conjectured (cf. [9]), that MOLS would also satisfy the converse of the theorem mentioned above; since this would imply the validity of Euler's conjecture for MOLS, this was disproved by [3] together with Euler's conjecture. But as RMOLS satisfies Euler's conjecture, it would seem conceivable that RMOLS even satisfies MACNEISH's conjecture. That this is not true, will be demonstrated by the following construction.

Theorem 6. *Let q be a prime power and $v := q^2 + q + 1$. If there exists a set or r mutually orthogonal Latin squares of order $q + 1$, then there exists a $(v, r, \mathbb{Z}_v)$-difference matrix.*

Proof. Since q is a prime power, Singer's theorem (cf. [10] or [7]) assures the existence of a difference set $\{a_0, \ldots, a_q\}$ in $\mathbb{Z}_v$. By hypothesis, there exists a set $D_1, \ldots, D_r$ of mutually orthogonal Latin squares of order $q + 1$ (w.l.o.g. on the symbols $0, \ldots, q$ and all squares with zeroth row $0, \ldots, q$). Let D_0 be the square with all rows $0, \ldots, q$. Let $\mathbf{d}_k^i$ denote the kth row of square D_i. Form the matrix

$$D' = \begin{pmatrix} \mathbf{d}_1^0 & \cdots & \mathbf{d}_q^0 \\ \vdots & & \vdots \\ \mathbf{d}_1^r & \cdots & \mathbf{d}_q^r \end{pmatrix}$$

and obtain the $(r + 1) \times (q(q + 1) + 1)$-matrix D by replacing each element i in D' by a_i $(i = 0, \ldots, q)$ and by adding a zero column. Then D is a $(q^2 + q + 1, r)$-difference matrix: Consider the ith and the kth row of D. Since D_i and D_k are orthogonal, by construction each pair (l, j) $(l \neq j; l, j = 0, \ldots, q)$ occurs in exactly one column of D' in the ith row and kth row of D'. Thus in the ith and kth row of D, every difference $a_i - a_j$ $(i \neq j)$ occurs exactly once, i.e. each element $\neq 0$ of $\mathbb{Z}_v$ occurs exactly once (since $\{a_0, \ldots, a_r\}$ is a difference set); finally the difference 0 occurs precisely in the last column of D.

Example 4. After putting the squares of order 5 (in Example 2) in standard form, one gets (using the difference set $\{3, 6, 12, 7, 14\}$ of $\mathbb{Z}_{21}$) the following (21, 4)-difference matrix:

$$\begin{pmatrix} 3 & 6 & 12 & 7 & 14 & 3 & 6 & 12 & 7 & 14 & 3 & 6 & 12 & 7 & 14 & 3 & 6 & 12 & 7 & 14 & 0 \\ 6 & 12 & 7 & 14 & 3 & 7 & 14 & 3 & 6 & 12 & 14 & 3 & 6 & 12 & 7 & 12 & 7 & 14 & 3 & 6 & 0 \\ 12 & 7 & 14 & 3 & 6 & 6 & 12 & 7 & 14 & 3 & 7 & 14 & 3 & 6 & 12 & 14 & 3 & 6 & 12 & 7 & 0 \\ 14 & 3 & 6 & 12 & 7 & 12 & 7 & 14 & 3 & 6 & 6 & 12 & 7 & 14 & 3 & 7 & 14 & 3 & 6 & 12 & 0 \\ 7 & 14 & 3 & 6 & 12 & 14 & 3 & 6 & 12 & 7 & 12 & 7 & 14 & 3 & 6 & 6 & 12 & 7 & 14 & 3 & 0 \end{pmatrix}$$

and after normalizing according to Corollary 1.

$$\begin{pmatrix} 17 & 13 & 9 & 1 & 2 & 10 & 3 & 6 & 16 & 7 & 12 & 20 & 19 & 4 & 8 & 18 & 15 & 5 & 14 & 11 & 0 \\ 20 & 19 & 4 & 8 & 12 & 14 & 11 & 18 & 15 & 5 & 2 & 17 & 13 & 9 & 1 & 6 & 16 & 7 & 10 & 3 & 0 \\ 5 & 14 & 11 & 18 & 15 & 13 & 9 & 1 & 2 & 17 & 16 & 7 & 10 & 3 & 6 & 8 & 12 & 20 & 19 & 4 & 0 \\ 7 & 10 & 3 & 6 & 16 & 19 & 4 & 8 & 12 & 20 & 15 & 5 & 14 & 11 & 18 & 1 & 2 & 17 & 13 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

We give the following numerical examples (only those not already known by Corollary 3, s gives the value known by Corollary 3):

q	4	7	16	19	31	49	61	64	67	
$q+1$	5	8	17	20	32	50	62	65	68	
r	4	7	16	3	31	6*)	4**)	7**)	5**)	
v	21	57	273	381	993	2451	3783	4161	4557	
s	2	2	2	2	2	2	2	2	2	etc.

Theorem 7. *Let q be a prime power and assume the existence of a $(q-1, r, \mathbb{Z}_{q-1})$-difference matrix. Then there exists a $(t, r, \mathbb{Z}_t)$-difference matrix with $t := q^2 - 1$.*

Proof. Since q is a prime power, there exists an affine difference set in $\mathbb{Z}_t$, say $\{a_1, \ldots, a_q\}$, i.e. the differences $a_i - a_j$ $(i \neq j, i, j = 1, \ldots, q)$ contain each element x of $\mathbb{Z}_t$ with $x \not\equiv 0 \pmod{q+1}$ exactly once (cf. [2] or [4, p. 210–211]). Thus the elements having no difference representation from $\{a_1, \ldots, a_r\}$, i.e. $0, q+1, \ldots, (q-2)(q+1)$, form a cyclic group $\{b_0, \ldots, b_{q-2}\} \simeq \mathbb{Z}_{q-1}$.

By (N4) we have $r \leqslant q-2$; hence there exist $r+1$ pairwise orthogonal Latin squares of order q, say $D_0, \ldots, D_r$. We may assume w.l.o.g. that the underlying symbol set is $\{1, \ldots, q\}$ and that all squares have first row $1 \cdots q$. Denote by $\mathbf{d}_k^i$ the kth row of square D_i and put

$$A := \begin{pmatrix} \mathbf{d}_2^0 & \cdots & \mathbf{d}_q^0 \\ \vdots & & \vdots \\ \mathbf{d}_2^r & \cdots & \mathbf{d}_q^r \end{pmatrix}$$

By replacing each element i in A by a_i we get a $(r+1) \times q(q-1)$-matrix A' such that the difference of any two distinct rows of A' contains each element from $\mathbb{Z}_t$ except for $b_0, \ldots, b_{q-2}$ (exactly once). Now let B be a

*) Wilson [15]. **) Van Lint [12, p. 117].

$(q-1, r, \mathbb{Z}_{q-1})$-difference matrix and obtain B' by replacing each element i in B by b_i. Then B' is an $(r+1) \times (q-1)$-matrix such that the difference of any two distinct rows of B' contains precisely the elements $b_0, \ldots, b_{q-2}$. Hence

$$D := (A'B')$$

is a $(t, r, \mathbb{Z}_t)$-difference matrix.

Example 5. We only give examples not already known by Corollary 3. (s is the value known by Corollary 3.):

q	32	128	513	2048	
$q-1$	31	127	511	2047	
r	30	126	6	22	
q^2-1	1023	$129 \cdot 127$	$511 \cdot 513$	$2047 \cdot 2049$	
s	2	2	2	2	etc.

We remark that Theorems 6 and 7 are analogues of existence results of BOSE and SHRIKHANDE [3] for Latin squares in general.

Remark: The non-abelian case. It is obvious how to generalize Definitions 1 and 2 to the case of non-abelian groups G. Theorem 1 then remains true (the proof carries over if we just take a bit more care of the order of additions). As all our interesting examples yielding information on $R(t)$ (i.e. Theorems 2, 4, 6 and 7) are taken from abelian groups, it did not seem worthwhile to consider the general situation. But we will remark that Theorem 5 and thus Corollary 4 remain true for non-abelian groups and that thus the class of (in the generalized sense) regular sets of Latin squares still satisfies Euler's conjecture. Thus let G be any group of order $2n$ with $(n, 2) = 1$ and assume the existence of a $(t, 2, G)$-difference matrix (in the generalized sense). Then G has a normal subgroup N of order n (see e.g. [13, 4.6]). Let a be an element in G of order 2 and put $A := \langle a \rangle$. Then clearly $G = \langle A, N \rangle$ and $A \cap N = \{0\}$. Thus G is the semidirect product of N by A (see e.g. [6, 6.5.3]). Hence—if we identify A with $\mathbb{Z}_2$—the elements of G take the form $(0, x)$ resp. $(1, x)$ with $x \in N$ and the group operation means for the first components just ordinary addition in $\mathbb{Z}_2$. The remainder of the proof is now as in Theorem 5.

Remark: Difference matrices and regular TD's. The correspondence between $(t, r+2)$-nets and sets of r mutually orthogonal Latin squares of order t is well-known (see [5] or [7]). There is an analogue for regular sets of Latin squares which we will sketch briefly. For reasons of convenience, we shall use the dual structure of a net, i.e. a TD ("transversal design"). We recall, that a (t, r)-TD consists of r "groups" of t points each (there is no connection to the algebraic notion of a group), such that points are joined by a line if and only if they are in the same group.

Furthermore each of the (t^2) lines meets each group. Such a TD Π is called *G-regular*, if G acts as a collination group of Π which is regular on each group and semiregular on the line set of Π. One then has the following result:

Let D be a (t, r, G)-difference matrix with $r \geqslant 2$ and define an incidence structure $\Sigma = (\mathfrak{P}, \mathfrak{B}, I)$ by

$$\mathfrak{P} := \{(i, x) : i = 0, \ldots, r; x \in G\}$$
$$\mathfrak{B} := \{G_i^x : i = 1, \ldots, t; x \in G\},$$

where

$$G_i^x := \{(0, d_{0i} + x), (1, d_{1i} + x), \ldots, (r, d_{ri} + x)\}.$$

Then Σ is a G-regular $(t, r + 1)$-TD with groups $\mathfrak{P}_i := \{(i, x) : x \in G\}$. Conversely, each G-regular $(t, r + 1)$-TD may be described in this way.

The proof is not too difficult and will be left as an exercise. By introducing infinite points and considering the groups as new lines, it is then possible to obtain the following result on projective planes: A $(t, t - 1, G)$-difference matrix D with $t \geqslant 3$ exists if and only if there is a projective plane of order t which is (p, L)-transitive for a suitable flag (p, L) and which has G as the elation group $G_{(p,L)}$.

This result shows that the notions of difference matrices and regular sets of Latin squares are in a way generalizations of the notion of (p, L)-transitivity for projective planes. Also, the geometric interpretation gives a stronger motivation for Definition 2 which may not seem really natural at first sight.

Acknowledgement

The author would like to thank H. Lenz, W. H. Mills, J. Röhmel and A. Neumaier for their helpful comments and suggestions.

References

[1] R. C. Bose: On the application of properties of Galois fields to the problem of construction of hypergraecolatin squares. Sankhyā **3**, 328–338 (1938).

[2] R. C. Bose: An affine analogue of Singer's theorem. J. Ind. Math. Soc. **6**, 1–15 (1942).

[3] R. C. Bose and S. Shrikhande: On the construction of sets of mutually orthogonal Latin squares and the falsity of Euler's conjecture. Trans. Am. Math. Soc. **95**, 191–200 (1960).

[4] P. Dembowski: Finite Geometries. Springer, Berlin-Heidelberg-New York (1968).

[5] J. Denes and A. D. Keedwell: Latin squares and their applications. The English Universities Press, London (1974).

[6] M. Hall, Jr.: The theory of groups. Macmillan, New York (1959).

[7] M. Hall, Jr.: Combinatorial theory. Blaisdell, Waltham-Toronto-London (1967).

[8] D. JOHNSON, A. K. DULMAGE and N. S. MENDELSOHN: Orthomorphisms of groups and orthogonal Latin squares. Can. J. Math. **13**, 356–372 (1961).
[9] H. F. MACNEISH: Euler squares. Ann. Math. **23**, 221–227 (1922).
[10] J. SINGER: A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. **43**, 377–385 (1938).
[11] B. L. VAN DER WAERDEN: Algebra I. Springer, Berlin-Heidelberg-New York (8. Auflage 1971).
[12] J. H. VAN LINT: Combinatorial Theory Seminar Eindhoven University of Technology, Springer, Berlin-Heidelberg-New York (1974).
[13] H. WIELANDT: Finite permutation groups. Academic Press, New York-London (1968).
[14] R. M. WILSON: Concerning the number of mutually orthogonal Latin squares. discr. math. **9**, 181–198 (1974).
[15] R. M. WILSON: A few more squares. Proceedings of the 5th Southeastern Conference on Combinatorics, Graph Theory and Computing (1975).

Eingegangen am 3.5.76—in revidierter Fassung am 20.10.78.

Anschrift des Autors: D. Jungnickel, F.U. Berlin, Königin-Luisestr. 24/26. D-1000 Berlin (West) 33.

Note added in proof: The author has generalized the concept of a difference matrix from the case $\lambda = 1$ (each group element occurs precisely once as a difference from any two rows) to arbitrary λ and studied the connections to transversal designs and to generalized Hadamard matrices in his paper "On difference matrices, resolvable transversal designs and generalized Hadamard matrices", Math. Z. **167** (1979), 49–60.