NTNU
Norwegian University of
Science and Technology

On Orthogonal Latin Squares

Yanling Chen
NTNU

Crypto-Seminar, Nov 9-10, Bergen

Latin Square (LS)

Definition

A *Latin square* of order n is an n-by-n array in which n distinct symbols are arranged so that each symbol occurs once in each row and column.

Latin Square (LS)

Definition

A *Latin square* of order n is an n-by-n array in which n distinct symbols are arranged so that each symbol occurs once in each row and column.

Examples

$$\boxed{1} \quad \boxed{\begin{array}{cc} 1 & 2 \\ 2 & 1 \end{array}} \quad \boxed{\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{array}} \quad \boxed{\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{array}} \quad \cdots$$

Orthogonal Latin Square

Definition

2 Latin squares of the same order n are said to be *orthogonal* if when they overlap, each of the possible n^2 ordered pairs occur exactly once.

NTNU
Norwegian University of
Science and Technology

Orthogonal Latin Square

Definition

2 Latin squares of the same order n are said to be *orthogonal* if when they overlap, each of the possible n^2 ordered pairs occur exactly once.

Example

$$\begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ \hline \end{array} \quad \perp \quad \begin{array}{|ccc|}\hline 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \\ \hline \end{array} \quad \Rightarrow \quad \begin{array}{|ccc|}\hline 11 & 22 & 33 \\ 23 & 31 & 12 \\ 32 & 13 & 21 \\ \hline \end{array}$$

History

Leonhard Euler [Euler 1782]

- the problem of 36 officers, 6 ranks, 6 regiments
- he concluded that no two 6×6 LS are orthogonal

L. Euler,
Recherches sur une nouvelle espèce de quarrés magiques,
Verh. Zeeuwsch. Genootsch. Wetensch. Vlissengen, 9, pp. 85–239, 1782

NTNU
Norwegian University of
Science and Technology

History

Euler's Conjecture

No pair of LS of order n are orthogonal for $n = 4k + 2, k \geq 0$.

NTNU
Norwegian University of
Science and Technology

History

Euler's Conjecture

No pair of LS of order n are orthogonal for $n = 4k + 2, k \geq 0$.

- $n = 2$:

$$\boxed{\begin{array}{cc} 1 & 2 \\ 2 & 1 \end{array}} \qquad \boxed{\begin{array}{cc} 2 & 1 \\ 1 & 2 \end{array}} \qquad \Rightarrow \qquad \boxed{\begin{array}{cc} 12 & 21 \\ 21 & 12 \end{array}}$$

History

Euler's Conjecture

No pair of LS of order n are orthogonal for $n = 4k + 2, k \geq 0$.

- $n = 2$:

$$\boxed{\begin{matrix}1 & 2\\ 2 & 1\end{matrix}} \qquad \boxed{\begin{matrix}2 & 1\\ 1 & 2\end{matrix}} \quad \Rightarrow \quad \boxed{\begin{matrix}12 & 21\\ 21 & 12\end{matrix}}$$

- $n = 6$: [Euler 1782]

  No orthogonal LS for $n = 6$, although without a complete proof

History

Euler's Conjecture

No pair of LS of order n are orthogonal for $n = 4k + 2, k \geq 0$.

- $n = 2$:

$$\begin{array}{|cc|}\hline 1 & 2 \\ 2 & 1 \\ \hline \end{array} \qquad \begin{array}{|cc|}\hline 2 & 1 \\ 1 & 2 \\ \hline \end{array} \quad \Rightarrow \quad \begin{array}{|cc|}\hline 12 & 21 \\ 21 & 12 \\ \hline \end{array}$$

- $n = 6$: [Euler 1782]

  No orthogonal LS for $n = 6$, although without a complete proof

- Construction: single-step for n odd, double-step for $n = 4k > 0$.

History

Gaston Tarry, 1900-01

- [Tarry 1900-01] proved that no orthogonal LS of order 6 exists
- 2 years of Sundays

NTNU
Norwegian University of
Science and Technology

History

Gaston Tarry, 1900-01

- [Tarry 1900-01] proved that no orthogonal LS of order 6 exists
- 2 years of Sundays

Bose, Shrikhande and Parker, 1959-60

- [Bose & Shrikhande 1959]: a pair of orthogonal LS of order 22.
- [Parker 1959]: a pair of orthogonal LS of order 10.
- [Bose, Shrikhande & Parker 1960]: counterexamples for all $n = 4k + 2 \geq 10$.

NTNU
Norwegian University of
Science and Technology

History

Gaston Tarry, 1900-01

- [Tarry 1900-01] proved that no orthogonal LS of order 6 exists
- 2 years of Sundays

Bose, Shrikhande and Parker, 1959-60

- [Bose & Shrikhande 1959]: a pair of orthogonal LS of order 22.
- [Parker 1959]: a pair of orthogonal LS of order 10.
- [Bose, Shrikhande & Parker 1960]: counterexamples for all $n = 4k + 2 \geq 10$.

[Zhu Lie 1982]: the most elegant disproof of Euler's conjecture

NTNU
Norwegian University of
Science and Technology

A Resolution of Euler's Conjecture

Orthogonal Latin Square

There exists a pair of orthogonal LS for all $n > 0$ with exception of $n = 2$ and $n = 6$.

NTNU
Norwegian University of
Science and Technology

Mutually Orthogonal LS (MOLS)

Definition

A set of LS that are pairwise orthogonal is called a set of *mutually orthogonal Latin squares* (MOLS)

NTNU
Norwegian University of
Science and Technology

Mutually Orthogonal LS (MOLS)

Definition

A set of LS that are pairwise orthogonal is called a set of *mutually orthogonal Latin squares* (MOLS)

Theorem

$N(n) \leq n - 1$. ($N(n)$: the number of MOLS that exist of order n.)

NTNU
Norwegian University of
Science and Technology

Mutually Orthogonal LS (MOLS)

Definition

A set of LS that are pairwise orthogonal is called a set of *mutually orthogonal Latin squares* (MOLS)

Theorem

$N(n) \leq n-1$. ($N(n)$: the number of MOLS that exist of order n.)

Theorem

If n is a power of a prime, then $N(n) = n-1$.

Hint: $L_i(x,y) = x + i * y$, where $i, x, y \in \mathrm{F}_n$, field with n elements.

NTNU
Norwegian University of
Science and Technology

Lower Bounds for $N(n), n \leq 100$

	0	1	2	3	4	5	6	7	8	9
0			1	2	3	4	1	6	7	8
10	2	10	5	12	3	4	15	16	3	18
20	4	5	3	22	6	24	4	26	5	28
30	4	30	31	5	4	5	6	36	4	5
40	7	40	5	42	5	6	4	46	7	48
50	6	5	5	52	5	6	7	7	5	58
60	4	60	4	6	63	7	5	66	5	6
70	6	70	7	72	5	5	6	6	6	78
80	9	80	8	82	6	6	6	6	7	88
90	6	7	6	6	6	6	7	96	6	8
100	8									

Some research problems

LS are widely used in cryptography, coding, experimental design and entertainment.

Some research problems

LS are widely used in cryptography, coding, experimental design and entertainment.

- Construction of LS which have particular orders and differ from the already known examples

NTNU
Norwegian University of
Science and Technology

Some research problems

LS are widely used in cryptography, coding, experimental design and entertainment.

- Construction of LS which have particular orders and differ from the already known examples
- Classifying LS of a given order n

NTNU
Norwegian University of
Science and Technology

Some research problems

LS are widely used in cryptography, coding, experimental design and entertainment.

- Construction of LS which have particular orders and differ from the already known examples
- Classifying LS of a given order n
- Extending (or reducing) LS of order n_1 to LS of order n_2

NTNU
Norwegian University of
Science and Technology

Some research problems

LS are widely used in cryptography, coding, experimental design and entertainment.

- Construction of LS which have particular orders and differ from the already known examples
- Classifying LS of a given order n
- Extending (or reducing) LS of order n_1 to LS of order n_2
- Completing partially filled matrices to LS (NP-complete)

NTNU
Norwegian University of
Science and Technology

Some research problems

LS are widely used in cryptography, coding, experimental design and entertainment.

- Construction of LS which have particular orders and differ from the already known examples
- Classifying LS of a given order n
- Extending (or reducing) LS of order n_1 to LS of order n_2
- Completing partially filled matrices to LS (NP-complete)
- $\cdots$

NTNU
Norwegian University of
Science and Technology

Quasigroup

Definition

A *quasigroup* is a set Q with a binary relation $*$ such that for all elements a and b, the following equations have unique solutions:

$$a * x = b \quad \text{and} \quad y * a = b.$$

Fact

Latin squares ↔ multiplication tables of finite quasigroups

MQQ: Multivariate Quadratic Quasigroup

- A quasigroup $(Q, *)$ of order 2^d, $a * b = c$, $a, b, c \in Q$.
- under a fixed bijection $\rho : Q \mapsto \{0, \cdots, 2^d - 1\}$,

$$\begin{aligned} \rho(a) &= (x_1, \cdots, x_d) \\ \rho(b) &= (y_1, \cdots, y_d) \\ \rho(c) &= (f_1, \cdots, f_d) \end{aligned}$$

- $a * b = c \Leftrightarrow (x_1, \cdots, x_d) *_{vv} (y_1, \cdots, y_d) = (f_1, \cdots, f_d)$.
- f_i are quadratic Boolean polynomials w.r.t $x_1, \cdots y_d$.

NTNU
Norwegian University of
Science and Technology

Motivation

Applications in MQQ based cryptosystems [Gligoroski et al. 08]

- Construction of MQQs of higher order and number of that
- Construction of MQQs of different types and number of that

Answers so far

- a randomized approach, of order $\sim 2^{14}$ [Ahlawat et al. 09]
- by T-functions [Samardjiska et al. 2010]
- based on matrix algebra [Chen et al. 2010]

NTNU
Norwegian University of
Science and Technology

Construction of MQQs

MQQ generating function

For any $\mathbb{A}$ such that correspondingly $\mathbf{A_1^*}, \mathbf{A_2^*}$, satisfy that

$$\det(\mathbf{A_1^*}) = \det(\mathbf{A_2^*}) = 1,$$

the vector valued operation $(x_1, \cdots, x_d) *_{vv} (y_1, \cdots, y_d)$ equal to

$$\mathbb{A} \odot \left[\mathrm{B}_1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \right] \cdot \left[\mathrm{B}_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} \right] + \mathrm{B}_1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} + \mathrm{B}_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} + \mathrm{c}$$

defines a MQQ for any nonsingular matrices $\mathrm{B}_1, \mathrm{B}_2$ and vector c.

Construction of MQQs

From $\mathbb{A}$ to $(\mathbf{A_1^*}, \mathbf{A_2^*})$

Let $\mathbb{A} = [a_{ij}]_{d\times d}$, where $a_{ij} = (f_1^{ij}, \cdots, f_d^{ij})$.

$$\mathbf{A_1^*} = \mathrm{I} + \begin{bmatrix} \quad (f_1^{ij}, \cdots, f_d^{ij}) \quad \end{bmatrix} \odot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix};$$

$$\mathbf{A_2^*} = \mathrm{I} + \begin{bmatrix} \quad (g_1^{ij}, \cdots, g_d^{ij}) \quad \end{bmatrix} \odot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix}.$$

- I: Identity matrix. $\odot$: symbolic dot product.
- $f_k^{ij} = g_j^{ik}$, for $1 \le i, j, k \le d$.

NTNU
Norwegian University of
Science and Technology

Construction of orthogonal LS

Orthogonal Latin squares of order 2^d

Consider two LS Q_1 and Q_2 defined by quasigroups

$$\begin{aligned} Q_1: &\quad (x_1, \cdots, x_d) *_1 (y_1, \cdots, y_d) = (f_1, \cdots, f_d); \\ Q_2: &\quad (x_1, \cdots, x_d) *_2 (y_1, \cdots, y_d) = (g_1, \cdots, g_d). \end{aligned}$$

When they overlap, we have a new mapping defined by

$$(x_1, \cdots, x_d) *_{vv} (y_1, \cdots, y_d) = (f_1, \cdots, f_d, g_1, \cdots, g_d).$$

If it is surjective, then we obtain an orthogonal Latin square.

NTNU
Norwegian University of
Science and Technology

Linear orthogonal Latin squares

Applying the MQQ generating function: $\mathbb{A} = \mathbf{0}$

Consider two LS Q_1 and Q_2 defined by

$$\begin{aligned} Q_1 : \quad & (x_1, \cdots, x_d) *_1 (y_1, \cdots, y_d) = \mathrm{B}_1\mathbf{x} + \mathrm{B}_2\mathbf{y} + \mathrm{c}_1; \\ Q_2 : \quad & (x_1, \cdots, x_d) *_2 (y_1, \cdots, y_d) = \mathrm{B}_3\mathbf{x} + \mathrm{B}_4\mathbf{y} + \mathrm{c}_2, \end{aligned}$$

where $\mathbf{x} = (x_1, \cdots, x_d)^{\mathrm{T}}$ and $\mathbf{y} = (y_1, \cdots, y_d)^{\mathrm{T}}$.

NTNU
Norwegian University of
Science and Technology

Linear orthogonal Latin squares

Applying the MQQ generating function: $\mathbb{A} = \mathbf{0}$

Consider two LS Q_1 and Q_2 defined by

$$\begin{aligned} Q_1: &\quad (x_1, \cdots, x_d) *_1 (y_1, \cdots, y_d) = \mathrm{B}_1\mathbf{x} + \mathrm{B}_2\mathbf{y} + \mathrm{c}_1; \\ Q_2: &\quad (x_1, \cdots, x_d) *_2 (y_1, \cdots, y_d) = \mathrm{B}_3\mathbf{x} + \mathrm{B}_4\mathbf{y} + \mathrm{c}_2, \end{aligned}$$

where $\mathbf{x} = (x_1, \cdots, x_d)^{\mathrm{T}}$ and $\mathbf{y} = (y_1, \cdots, y_d)^{\mathrm{T}}$. When they overlap

$$(x_1, \cdots, x_d) *_{vv} (y_1, \cdots, y_d) = \begin{bmatrix} \mathrm{B}_1 & \mathrm{B}_2 \\ \mathrm{B}_3 & \mathrm{B}_4 \end{bmatrix} \cdot \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} + \begin{pmatrix} \mathrm{c}_1 \\ \mathrm{c}_2 \end{pmatrix}.$$

NTNU
Norwegian University of
Science and Technology

Linear orthogonal Latin squares

Applying the MQQ generating function: $\mathbb{A} = \mathbf{0}$

Consider two LS Q_1 and Q_2 defined by

$$\begin{aligned} Q_1 : \quad & (x_1, \cdots, x_d) *_1 (y_1, \cdots, y_d) = \mathrm{B}_1\mathbf{x} + \mathrm{B}_2\mathbf{y} + \mathrm{c}_1; \\ Q_2 : \quad & (x_1, \cdots, x_d) *_2 (y_1, \cdots, y_d) = \mathrm{B}_3\mathbf{x} + \mathrm{B}_4\mathbf{y} + \mathrm{c}_2, \end{aligned}$$

where $\mathbf{x} = (x_1, \cdots, x_d)^{\mathrm{T}}$ and $\mathbf{y} = (y_1, \cdots, y_d)^{\mathrm{T}}$. When they overlap

$$(x_1, \cdots, x_d) *_{vv} (y_1, \cdots, y_d) = \begin{bmatrix} \mathrm{B}_1 & \mathrm{B}_2 \\ \mathrm{B}_3 & \mathrm{B}_4 \end{bmatrix} \cdot \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} + \begin{pmatrix} \mathrm{c}_1 \\ \mathrm{c}_2 \end{pmatrix}.$$

If $\det\left(\begin{bmatrix} \mathrm{B}_1 & \mathrm{B}_2 \\ \mathrm{B}_3 & \mathrm{B}_4 \end{bmatrix}\right) = 1$, then Q_1 and Q_2 are orthogonal.

NTNU
Norwegian University of
Science and Technology

Linear orthogonal Latin squares

Number of the linear orthogonal Latin squares pairs

By choosing appropriate $\mathrm{B}_1, \mathrm{B}_2, \mathrm{B}_3, \mathrm{B}_4$ and c, there are

$$N_d \cdot 2^{d(d-1)/2} \cdot \prod_{t=0}^{d-1} (2^d - 2^t)^3 \cdot 2^{2d}$$

pairs of orthogonal LS, where $N_0 = 1, N_d = (2^d - 1)N_{d-1} + (-1)^d$.

NTNU
Norwegian University of
Science and Technology

Linear orthogonal Latin squares

Number of the linear orthogonal Latin squares pairs

By choosing appropriate $\mathrm{B}_1, \mathrm{B}_2, \mathrm{B}_3, \mathrm{B}_4$ and c, there are

$$N_d \cdot 2^{d(d-1)/2} \cdot \prod_{t=0}^{d-1} (2^d - 2^t)^3 \cdot 2^{2d}$$

pairs of orthogonal LS, where $N_0 = 1, N_d = (2^d - 1)N_{d-1} + (-1)^d$.

Hint: Det of the block matrix !

$$\det\left(\begin{bmatrix} \mathrm{B}_1 & \mathrm{B}_2 \\ \mathrm{B}_3 & \mathrm{B}_4 \end{bmatrix}\right) = \det(\mathrm{I_d} - \mathrm{B}_1^{-1} \cdot \mathrm{B}_2 \cdot \mathrm{B}_4^{-1} \cdot \mathrm{B}_3) = 1.$$

NTNU
Norwegian University of
Science and Technology

Linear mutually orthogonal Latin squares

Recall $N(n) = n - 1$, for $n = 2^d$

Consider the LS $Q_i, 0 \leq i \leq 2^d - 2$ defined by

$$Q_i : \quad (x_1, \cdots, x_d) *_i (y_1, \cdots, y_d) = \mathbf{x} + \mathrm{B}^i \mathbf{y} + \mathrm{c}_i$$

where $\mathbf{x} = (x_1, \cdots, x_d)^{\mathrm{T}}$ and $\mathbf{y} = (y_1, \cdots, y_d)^{\mathrm{T}}$.

NTNU
Norwegian University of
Science and Technology

Linear mutually orthogonal Latin squares

Recall $N(n) = n - 1$, for $n = 2^d$

Consider the LS $Q_i, 0 \leq i \leq 2^d - 2$ defined by

$$Q_i : \quad (x_1, \cdots, x_d) *_i (y_1, \cdots, y_d) = \mathbf{x} + \mathrm{B}^i \mathbf{y} + \mathrm{c}_i$$

where $\mathbf{x} = (x_1, \cdots, x_d)^{\mathrm{T}}$ and $\mathbf{y} = (y_1, \cdots, y_d)^{\mathrm{T}}$.

Then $\{Q_0, Q_1, \cdots, Q_{2^d-2}\}$ defines a complete set of MOLS of order 2^d, if characteristic polynomial of B is a primitive polynomial of degree d.

NTNU
Norwegian University of
Science and Technology

Linear mutually orthogonal Latin squares

Existence of B

For a primitive polynomial $f(x) = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} + x^{d-1}$,

$$\text{let B} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{d-1} \end{pmatrix}.$$

NTNU
Norwegian University of
Science and Technology

Linear mutually orthogonal Latin squares

Number of choices of B [Choudhury 2005]

Let $\phi(\cdot)$ be Euler's totient function. Number of choices of B is

$$\prod_{i=1}^{d-1}(2^d - 2^i) \cdot \frac{\phi(2^d - 1)}{d}.$$

NTNU
Norwegian University of
Science and Technology

Quadratic orthogonal Latin squares

$$ {}^{1}\mathbb{A} = \begin{bmatrix} (1\ 0\ 1) & (0\ 1\ 1) & (1\ 1\ 0) \\ (1\ 0\ 1) & (0\ 1\ 1) & (0\ 1\ 1) \\ (1\ 0\ 1) & (0\ 1\ 1) & (1\ 0\ 1) \end{bmatrix} $$

$$ {}^{2}\mathbb{A} = \begin{bmatrix} (1\ 0\ 1) & (1\ 1\ 0) & (0\ 1\ 1) \\ (1\ 1\ 0) & (1\ 1\ 0) & (0\ 1\ 1) \\ (0\ 1\ 1) & (1\ 1\ 0) & (0\ 1\ 1) \end{bmatrix} \quad \mathrm{B} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} $$

NTNU
Norwegian University of
Science and Technology

Quadratic orthogonal Latin squares

$$Q_1: \quad {}^1\mathbb{A} \odot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

$$Q_2: \quad {}^2\mathbb{A} \odot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \cdot \mathrm{B} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \mathrm{B} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

NTNU
Norwegian University of
Science and Technology

Quadratic orthogonal Latin squares

Defined by $(x_1, x_2, x_3) *_{vv} (y_1, y_2, y_3)$ which is equal to

$$
\begin{aligned}
f_1 &= (x_1 + x_3)y_1 + (x_2 + x_3)y_2 + (x_1 + x_2)y_3 + x_1 + y_1 \\
f_2 &= (x_1 + x_3)y_1 + (x_2 + x_3)y_2 + (x_2 + x_3)y_3 + x_2 + y_2 \\
f_3 &= (x_1 + x_3)y_1 + (x_2 + x_3)y_2 + (x_1 + x_3)y_3 + x_3 + y_3 \\
g_1 &= (x_1 + x_2)y_1 + (x_2 + x_3)y_2 + (x_1 + x_2)y_3 + x_1 + y_3 \\
g_2 &= (x_1 + x_2)y_1 + (x_2 + x_3)y_2 + (x_1 + x_3)y_3 + x_2 + y_1 \\
g_3 &= (x_1 + x_2)y_1 + (x_2 + x_3)y_2 + x_3 + y_2 + y_3
\end{aligned}
$$

NTNU
Norwegian University of
Science and Technology

Quadratic orthogonal Latin squares

Defined by $(x_1, x_2, x_3) *_{vv} (y_1, y_2, y_3)$ which is equal to

					$y_1y_2y_3$				
	*	0	1	2	3	4	5	6	7
$x_1x_2x_3$	0	(0, 0)	(1, 5)	(2, 1)	(3, 4)	(4, 2)	(5, 7)	(6, 3)	(7, 6)
	1	(1, 1)	(3, 6)	(4, 7)	(6, 0)	(2, 3)	(0, 4)	(7, 5)	(5, 2)
	2	(2, 2)	(5, 3)	(7, 4)	(0, 5)	(6, 7)	(1, 6)	(3, 1)	(4, 0)
	3	(3, 3)	(7, 0)	(1, 2)	(5, 1)	(0, 6)	(4, 5)	(2, 7)	(6, 4)
	4	(4, 4)	(0, 7)	(6, 5)	(2, 6)	(7, 1)	(3, 2)	(5, 0)	(1, 3)
	5	(5, 5)	(2, 4)	(0, 3)	(7, 2)	(1, 0)	(6, 1)	(4, 6)	(3, 7)
	6	(6, 6)	(4, 1)	(3, 0)	(1, 7)	(5, 4)	(7, 3)	(0, 2)	(2, 5)
	7	(7, 7)	(6, 2)	(5, 6)	(4, 3)	(3, 5)	(2, 0)	(1, 4)	(0, 1)

NTNU
Norwegian University of
Science and Technology

Conclusions & Further work

Results

- MQQ generating function
- Construction of (linear) orthogonal Latin squares
- Construction of the complete set of (linear) MOLS
- Quadratic orthogonal Latin squares

NTNU
Norwegian University of
Science and Technology

Conclusions & Further work

Results

- MQQ generating function
- Construction of (linear) orthogonal Latin squares
- Construction of the complete set of (linear) MOLS
- Quadratic orthogonal Latin squares

On the way...

- Construction of quadratic orthogonal Latin squares
- Applications in cryptography and error detection/correction

NTNU
Norwegian University of
Science and Technology

References I

- G. Tarry,
  Le problème des 36 officiers,
  C. R. Assoc. Franc. Av. Sci., 1, pp. 122–123, 1900.
  C. R. Assoc. Franc. Av. Sci., 2, pp. 170–203, 1901.
- R. C. Rose and S. S. Shrikhande,
  On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order $4k + 2$,
  Proc. Nat. Acad. Sci. U. S. A., 45, pp. 734–737, 1959.
- E.T. Parker,
  Orthogonal Latin squares,
  Proc. Natl. Acad. Sci. U.S.A., 45, pp. 859–862, 1959.
- Z. Lie,
  A short disproof of Euler's conjecture concerning orthogonal Latin squares,
  Ars Combinatoria, 14, pp. 47–55, 1982.

References II

- R.C. Bose, S.S. Shrikhande and E.T. Parker,
  Further results on the constructive of mutually orthogonal Latin squares and the falsity of Euler's conjecture,
  Canad. J. Math., 12, pp. 189–203, 1960.
- Danilo Gligoroski, Smile Markovski and Svein J. Knapskog,
  A public key algorithm based on multivariate quadratic quasigroups,
  Proc. American Conference on Applied Mathematics, pp. 44-49, 2008.
- S. Samardjiska, S. Markovski and D. Gligoroski,
  Multivariate Quasigroups Defined by T-functions,
  2nd International Conference on Symbolic Computation and Cryptography, pp. 117–127, 2010.

NTNU
Norwegian University of
Science and Technology

References III

- Yanling Chen and Svein J. Knapskog and D. Gligorosk,
  Multivariate Quadratic Quasigroups (MQQs): Construction, Bounds and Complexity,
  6th International Conference on Information Security and Cryptology, 2010.
- Rohit Ahlawat, Kanika Gupta and Saibal K. Pal,
  Fast generation of multivariate quadratic quasigroups for cryptographic applications,
  Proc. 2009 Mathematics in Defence, 2009.
- Piyasi Choudhury,
  Generating matrices of highest order over a finite field,
  http://arxiv.org/abs/math/0511651, 2005.

NTNU
Norwegian University of
Science and Technology