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

\[
\begin{array}{ccc}
1 & 2 & 3 \\
2 & 3 & 1 \\
3 & 1 & 2 \\
\end{array}
\]

\[
\begin{array}{cccc}
1 & 2 & 3 & 4 \\
2 & 3 & 4 & 1 \\
3 & 4 & 1 & 2 \\
4 & 1 & 2 & 3 \\
\end{array}
\]

\[
\begin{array}{cccc}
\ldots
\end{array}
\]
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.
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**

\[
\begin{array}{ccc}
1 & 2 & 3 \\
2 & 3 & 1 \\
3 & 1 & 2 \\
\end{array}
\quad \perp \quad
\begin{array}{ccc}
1 & 2 & 3 \\
3 & 1 & 2 \\
2 & 3 & 1 \\
\end{array}
\Rightarrow
\begin{array}{ccc}
11 & 22 & 33 \\
23 & 31 & 12 \\
32 & 13 & 21 \\
\end{array}
\]
History

**Leonhard Euler** [Euler 1782]

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

**L. Euler,**

Recherches sur une nouvelle espèce de quarrés magiques,

History

Euler’s Conjecture

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

Euler’s Conjecture

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

- \( n = 2 \):
  \[
  \begin{array}{cc}
  1 & 2 \\
  2 & 1 \\
  \end{array}
  \quad \Rightarrow 
  \begin{array}{cc}
  12 & 21 \\
  21 & 12 \\
  \end{array}
  \]
History

Euler’s Conjecture

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

- $n = 2$:
  
  $\begin{array}{cc}
  1 & 2 \\
  2 & 1 \\
  \end{array}$  \quad $\Rightarrow$  \quad $\begin{array}{cc}
  2 & 1 \\
  1 & 2 \\
  \end{array}$

- $n = 6$: [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 \( n = 4k + 2, k \geq 0 \).

- \( n = 2 \):

\[
\begin{array}{cc}
1 & 2 \\
2 & 1 \\
\end{array}
\quad
\begin{array}{cc}
2 & 1 \\
1 & 2 \\
\end{array}
\implies
\begin{array}{cc}
12 & 21 \\
21 & 12 \\
\end{array}
\]

- \( n = 6 \): [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
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 $n = 4k + 2 \geq 10$. 
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
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 \( n = 6 \).
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:
$L(x, y) = x + i \cdot y$, where $i, x, y \in F_n$, field with $n$ elements.
Mutually Orthogonal LS (MOLS)

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

Theorem
\[ N(n) \leq n - 1. \]  
\((N(n) : \text{the number of MOLS that exist of order } n.\)
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: \( L_i(x, y) = x + i \cdot y, \) where \( i, x, y \in F_n, \) field with \( n \) elements.
### Lower Bounds for $N(n), n \leq 100$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>10</td>
<td>5</td>
<td>12</td>
<td>3</td>
<td>4</td>
<td>15</td>
<td>16</td>
<td>3</td>
<td>18</td>
</tr>
<tr>
<td>20</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>22</td>
<td>6</td>
<td>24</td>
<td>4</td>
<td>26</td>
<td>5</td>
<td>28</td>
</tr>
<tr>
<td>30</td>
<td>4</td>
<td>30</td>
<td>31</td>
<td>5</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>36</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>40</td>
<td>7</td>
<td>40</td>
<td>5</td>
<td>42</td>
<td>5</td>
<td>6</td>
<td>4</td>
<td>46</td>
<td>7</td>
<td>48</td>
</tr>
<tr>
<td>50</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>52</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>5</td>
<td>58</td>
</tr>
<tr>
<td>60</td>
<td>4</td>
<td>60</td>
<td>4</td>
<td>6</td>
<td>63</td>
<td>7</td>
<td>5</td>
<td>66</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>70</td>
<td>6</td>
<td>70</td>
<td>7</td>
<td>72</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>78</td>
</tr>
<tr>
<td>80</td>
<td>9</td>
<td>80</td>
<td>8</td>
<td>82</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>88</td>
</tr>
<tr>
<td>90</td>
<td>6</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>96</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>100</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
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 \( n \)
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 $n_2$
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)
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)
• …
### 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 $\leftrightarrow$ 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 \(\rho : Q \mapsto \{0, \cdots, 2^d - 1\}\),

\[
\begin{align*}
\rho(a) &= (x_1, \cdots, x_d) \\
\rho(b) &= (y_1, \cdots, y_d) \\
\rho(c) &= (f_1, \cdots, f_d)
\end{align*}
\]

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

MQQ generating function

For any $A$ such that correspondingly $A_1^*, A_2^*$, satisfy that

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

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

$A \odot \left[ B_1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \right] \cdot \left[ B_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} \right] + B_1 \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} + B_2 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} + c$

defines a MQQ for any nonsingular matrices $B_1, B_2$ and vector $c$. 
Construction of MQQs

From $\mathbb{A}$ to $(\mathbb{A}^*_1, \mathbb{A}^*_2)$

Let $\mathbb{A} = [a_{ij}]_{d \times d}$, where $a_{ij} = (f^{ij}_1, \ldots, f^{ij}_d)$.

\[
\mathbb{A}^*_1 = I + \begin{bmatrix} (f^{ij}_1, \ldots, f^{ij}_d) \end{bmatrix} \circ \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} ;
\]

\[
\mathbb{A}^*_2 = I + \begin{bmatrix} (g^{ij}_1, \ldots, g^{ij}_d) \end{bmatrix} \circ \begin{pmatrix} y_1 \\ \vdots \\ y_d \end{pmatrix} .
\]

- **I**: Identity matrix. \(\circ\): symbolic dot product.
- \(f^{ij}_k = g^{ik}_j\), for $1 \leq i, j, k \leq d$. 

Yanling Chen, On Orthogonal Latin Squares
Construction of orthogonal LS

Orthogonal Latin squares of order $2^d$

Consider two LS $Q_1$ and $Q_2$ defined by quasigroups

$$Q_1 : (x_1, \cdots, x_d) *_1 (y_1, \cdots, y_d) = (f_1, \cdots, f_d);$$

$$Q_2 : (x_1, \cdots, x_d) *_2 (y_1, \cdots, y_d) = (g_1, \cdots, g_d).$$

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.
Linear orthogonal Latin squares

Applying the MQQ generating function: \( \mathbf{A} = 0 \)

Consider two LS \( Q_1 \) and \( Q_2 \) defined by

\[
Q_1 : \ (x_1, \cdots, x_d) \ast_1 (y_1, \cdots, y_d) = B_1 \mathbf{x} + B_2 \mathbf{y} + c_1;
\]
\[
Q_2 : \ (x_1, \cdots, x_d) \ast_2 (y_1, \cdots, y_d) = B_3 \mathbf{x} + B_4 \mathbf{y} + c_2,
\]

where \( \mathbf{x} = (x_1, \cdots, x_d)^T \) and \( \mathbf{y} = (y_1, \cdots, y_d)^T \).
**Linear orthogonal Latin squares**

Applying the MQQ generating function: $A = 0$

Consider two LS $Q_1$ and $Q_2$ defined by

$$Q_1: \quad (x_1, \cdots, x_d) *_1 (y_1, \cdots, y_d) = B_1 x + B_2 y + c_1;$$
$$Q_2: \quad (x_1, \cdots, x_d) *_2 (y_1, \cdots, y_d) = B_3 x + B_4 y + c_2,$$

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

$$(x_1, \cdots, x_d) *_{vv} (y_1, \cdots, y_d) = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}.$$
**Linear orthogonal Latin squares**

Applying the MQQ generating function: \( A = 0 \)

Consider two LS \( Q_1 \) and \( Q_2 \) defined by

\[
Q_1 : \ (x_1, \ldots, x_d) \ast_1 (y_1, \ldots, y_d) = B_1 x + B_2 y + c_1;
\]
\[
Q_2 : \ (x_1, \ldots, x_d) \ast_2 (y_1, \ldots, y_d) = B_3 x + B_4 y + c_2,
\]

where \( x = (x_1, \ldots, x_d)^T \) and \( y = (y_1, \ldots, y_d)^T \). When they overlap

\[
(x_1, \ldots, x_d) \ast vv (y_1, \ldots, y_d) = \left[ \begin{array}{cc} B_1 & B_2 \\ B_3 & B_4 \end{array} \right] \cdot \left( \begin{array}{c} x \\ y \end{array} \right) + \left( \begin{array}{c} c_1 \\ c_2 \end{array} \right).
\]

If \( \det \left( \begin{array}{cc} B_1 & B_2 \\ B_3 & B_4 \end{array} \right) = 1 \), then \( Q_1 \) and \( Q_2 \) are orthogonal.
Linear orthogonal Latin squares

Number of the linear orthogonal Latin squares pairs

By choosing appropriate $B_1, B_2, B_3, B_4$ 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 $N_0 = 1, N_d = (2^d - 1)N_{d-1} + (-1)^d$. 
Linear orthogonal Latin squares

Number of the linear orthogonal Latin squares pairs

By choosing appropriate $B_1, B_2, B_3, B_4$ 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!

$$\det \left( \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix} \right) = \det(I_d - B_1^{-1} \cdot B_2 \cdot B_4^{-1} \cdot B_3) = 1.$$
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

$$Q_i : (x_1, \cdots, x_d) *_i (y_1, \cdots, y_d) = x + B^i y + c_i$$

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

$$Q_i: \ (x_1, \cdots, x_d) * i (y_1, \cdots, y_d) = x + B^i y + c_i$$

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

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 $d$. 
**Linear mutually orthogonal Latin squares**

Existence of B

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

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

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

$1_A = \begin{bmatrix}
(1 & 0 & 1) & (0 & 1 & 1) & (1 & 1 & 0) \\
(1 & 0 & 1) & (0 & 1 & 1) & (0 & 1 & 1) \\
(1 & 0 & 1) & (0 & 1 & 1) & (1 & 0 & 1)
\end{bmatrix}$

$2_A = \begin{bmatrix}
(1 & 0 & 1) & (1 & 1 & 0) & (0 & 1 & 1) \\
(1 & 1 & 0) & (1 & 1 & 0) & (0 & 1 & 1) \\
(0 & 1 & 1) & (1 & 1 & 0) & (0 & 1 & 1)
\end{bmatrix}$

$B = \begin{bmatrix}
0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 1
\end{bmatrix}$
**Quadratic orthogonal Latin squares**

\[ Q_1: \quad 1A \otimes \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \]

\[ Q_2: \quad 2A \otimes \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \cdot B \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} + \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + B \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \]
**Quadratic orthogonal Latin squares**

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

\[
\begin{align*}
  f_1 &= (x_1 + x_3)y_1 + (x_2 + x_3)y_2 + (x_1 + x_2)y_3 + x_1 + y_1 \\
  f_2 &= (x_1 + x_3)y_1 + (x_2 + x_3)y_2 + (x_2 + x_3)y_3 + x_2 + y_2 \\
  f_3 &= (x_1 + x_3)y_1 + (x_2 + x_3)y_2 + (x_1 + x_3)y_3 + x_3 + y_3 \\
  g_1 &= (x_1 + x_2)y_1 + (x_2 + x_3)y_2 + (x_1 + x_2)y_3 + x_1 + y_3 \\
  g_2 &= (x_1 + x_2)y_1 + (x_2 + x_3)y_2 + (x_1 + x_3)y_3 + x_2 + y_1 \\
  g_3 &= (x_1 + x_2)y_1 + (x_2 + x_3)y_2 + x_3 + y_2 + y_3
\end{align*}
\]
**Quadratic orthogonal Latin squares**

Defined by \((x_1, x_2, x_3) \ast_{vv} (y_1, y_2, y_3)\) which is equal to

<table>
<thead>
<tr>
<th>*</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(0, 0)</td>
<td>(1, 5)</td>
<td>(2, 1)</td>
<td>(3, 4)</td>
<td>(4, 2)</td>
<td>(5, 7)</td>
<td>(6, 3)</td>
<td>(7, 6)</td>
</tr>
<tr>
<td>1</td>
<td>(1, 1)</td>
<td>(3, 6)</td>
<td>(4, 7)</td>
<td>(6, 0)</td>
<td>(2, 3)</td>
<td>(0, 4)</td>
<td>(7, 5)</td>
<td>(5, 2)</td>
</tr>
<tr>
<td>2</td>
<td>(2, 2)</td>
<td>(5, 3)</td>
<td>(7, 4)</td>
<td>(0, 5)</td>
<td>(6, 7)</td>
<td>(1, 6)</td>
<td>(3, 1)</td>
<td>(4, 0)</td>
</tr>
<tr>
<td>3</td>
<td>(3, 3)</td>
<td>(7, 0)</td>
<td>(1, 2)</td>
<td>(5, 1)</td>
<td>(0, 6)</td>
<td>(4, 5)</td>
<td>(2, 7)</td>
<td>(6, 4)</td>
</tr>
<tr>
<td>4</td>
<td>(4, 4)</td>
<td>(0, 7)</td>
<td>(6, 5)</td>
<td>(2, 6)</td>
<td>(7, 1)</td>
<td>(3, 2)</td>
<td>(5, 0)</td>
<td>(1, 3)</td>
</tr>
<tr>
<td>5</td>
<td>(5, 5)</td>
<td>(2, 4)</td>
<td>(0, 3)</td>
<td>(7, 2)</td>
<td>(1, 0)</td>
<td>(6, 1)</td>
<td>(4, 6)</td>
<td>(3, 7)</td>
</tr>
<tr>
<td>6</td>
<td>(6, 6)</td>
<td>(4, 1)</td>
<td>(3, 0)</td>
<td>(1, 7)</td>
<td>(5, 4)</td>
<td>(7, 3)</td>
<td>(0, 2)</td>
<td>(2, 5)</td>
</tr>
<tr>
<td>7</td>
<td>(7, 7)</td>
<td>(6, 2)</td>
<td>(5, 6)</td>
<td>(4, 3)</td>
<td>(3, 5)</td>
<td>(2, 0)</td>
<td>(1, 4)</td>
<td>(0, 1)</td>
</tr>
</tbody>
</table>
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
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
References I

G. Tarry,
Le problème des 36 officiers,

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 $4k + 2$,

E.T. Parker,
Orthogonal Latin squares,

Z. Lie,
A short disproof of Euler’s conjecture concerning orthogonal Latin squares,
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,

Danilo Gligoroski, Smile Markovski and Svein J. Knapskog,
A public key algorithm based on multivariate quadratic quasigroups,

S. Samardjiska, S. Markovski and D. Gligoroski,
Multivariate Quasigroups Defined by T-functions,
References III

Yanling Chen and Svein J. Knapskog and D. Gligorosk,
Multivariate Quadratic Quasigroups (MQQs): Construction, Bounds and Complexity,

Rohit Ahlawat, Kanika Gupta and Saibal K. Pal,
Fast generation of multivariate quadratic quasigroups for cryptographic applications,

Piyasi Choudhury,
Generating matrices of highest order over a finite field,