A three-factor product construction for mutually orthogonal latin squares

Peter J. Dukes
(joint work with Alan C.H. Ling, UVM)

June 17, 2014
Introduction

Latin squares and MOLS
Product construction

Main result: triple products gain one square
Statement and corollaries
Transversal designs and parallel classes
A construction of Rolf Rees
Proof sketch
Improvements to the MOLS table
Remarks

References
Latin squares

A *latin square* is an $n \times n$ array with entries from an $n$-element set of symbols such that every row and column exhausts the symbols (with no repetition). Often the symbols are $[n] := \{1, \ldots, n\}$. The integer $n$ is called the *order* of the square.

**Examples.**

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

▶ sudoku squares
▶ addition table of a group
Orthogonality

Two latin squares $L$ and $L'$ of order $n$ are **orthogonal** if
\[ \{(L_{ij}, L'_{ij}) : 1 \leq i, j \leq n\} = [n]^2 \]

**Examples.**

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

▶ 36 officers problem

\[
\begin{array}{cccc}
\text{A} & \text{J} & \text{Q} & \text{K} \\
\text{J} & \text{A} & \text{K} & \text{Q} \\
\text{Q} & \text{K} & \text{A} & \text{J} \\
\text{K} & \text{Q} & \text{J} & \text{A}
\end{array}
\]
A family of pairwise orthogonal latin squares is normally called *mutually orthogonal latin squares*, and abbreviated ‘MOLS’.

The maximum size of a family of MOLS of order $n$ is denoted $N(n)$.

It is easy to see that $N(n) \leq n - 1$ for $n > 1$, with equality iff there exists a projective plane of order $n$. So $N(q) = q - 1$ for prime powers $q$. 
Product construction

Given latin squares $L$, of order $l$, and $M$, of order $m$, their Kronecker product $L \otimes M$ is a latin square of order $lm$.

If \{\(L^{(1)}, \ldots, L^{(k)}\)\} and \{\(M^{(1)}, \ldots, M^{(k)}\)\} are families of MOLS of orders $l$ and $m$, then \{\(L^{(1)} \otimes M^{(1)}, \ldots, L^{(k)} \otimes M^{(k)}\)\} is a family of MOLS of order $lm$. Hence, \(N(lm) \geq \min\{N(l), N(m)\}\). Combining with prime powers yields a ‘basic’ lower bound on \(N(n)\).

**Theorem (MacNeish)**

If \(n = q_1 \ldots q_t\) is factored as a product of powers of distinct primes, then \(N(n) \geq \min\{q_i - 1\}\).
History:

▶ Euler: conjectures $N(n) = 1$ for $n \equiv 2 \pmod{4}$
▶ Bose-Parker-Shrikhandhe: $N(n) \geq 2$ for $n \notin \{2, 6\}$
▶ Chowla-Erdős-Strauss: $N(n) \to \infty$
▶ Wilson-Beth: $N(n) \geq n^{\frac{1}{14.8}}$ for large $n$

Even still, MacNeish’s Theorem remains the best known result for many values of $n$, particularly when $n$ has a small number of prime power factors about the same size.
Main Result

Theorem
For integers $a, b, c$ with $a \leq b \leq c$, we have

$$N(abc) \geq \min\{N(a) + 1, N(b), N(c)\}.$$  

Remark. Here $a, b, c$ need not be coprime.

Corollary
For prime powers $p \leq q \leq r$, we have $N(pqr) \geq p$.

Corollary
$N(p \times 2^t) \geq p$ for prime powers $p < 2^{|t/2|}$.  

Main Result

**Theorem**

For integers $a, b, c$ with $a \leq b \leq c$, we have

$$N(abc) \geq \min\{N(a) + 1, N(b), N(c)\}.$$ 

**Remark.** Here $a, b, c$ need not be coprime.

**Corollary**

For prime powers $p \leq q \leq r$, we have $N(pqr) \geq p$.

**Corollary**

$N(p \times 2^t) \geq p$ for prime powers $p < 2^\lceil t/2 \rceil$. 
Main Result

Theorem
For integers $a, b, c$ with $a \leq b \leq c$, we have

$$N(abc) \geq \min\{N(a) + 1, N(b), N(c)\}.$$ 

Remark. Here $a, b, c$ need not be coprime.

Corollary
For prime powers $p \leq q \leq r$, we have $N(pqr) \geq p$.

Corollary
$N(p \times 2^t) \geq p$ for prime powers $p < 2^\lfloor t/2 \rfloor$. 
A \textit{transversal design} $\text{TD}(k, n)$ consists of an $nk$-element set of points partitioned into $k$ groups, each of size $n$, and equipped with a family of $n^2$ blocks of size $k$ which are pairwise disjoint transversals of the partition.

We can slightly change notation to get an \textit{orthogonal array}: an $n^2 \times k$ array with entries from $[n]$, such that in any two columns we see $[n]^2$.

We have the existence of $r$ MOLS of order $n$ if and only if a $\text{TD}(r + 2, n)$ exists.
Example.

\[
\begin{align*}
\text{TD}(4, 3) & \\
1111 & \text{Two MOLS of order 3} \\
2221 & \begin{bmatrix}
1 & 3 & 2 \\
3 & 2 & 1 \\
2 & 1 & 3 \\
\end{bmatrix}
\\n3331 & \begin{bmatrix}
1 & 2 & 3 \\
3 & 1 & 2 \\
2 & 3 & 1 \\
\end{bmatrix}
\\n1232 & \\
2312 & \\
3122 & \\
1323 & \\
2133 & \\
3213 & \\
\end{align*}
\]
Example.

<table>
<thead>
<tr>
<th>TD(4, 3)</th>
<th>Two MOLS of order 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1111</td>
<td>1 3 2</td>
</tr>
<tr>
<td>2221</td>
<td>3 2 1</td>
</tr>
<tr>
<td>3331</td>
<td>2 1 3</td>
</tr>
<tr>
<td>1232</td>
<td>1 2 3</td>
</tr>
<tr>
<td>2312</td>
<td>3 1 2</td>
</tr>
<tr>
<td>3122</td>
<td>2 3 1</td>
</tr>
<tr>
<td>1323</td>
<td></td>
</tr>
<tr>
<td>2133</td>
<td></td>
</tr>
<tr>
<td>3213</td>
<td></td>
</tr>
</tbody>
</table>
Resolvability and thick classes

In a TD($k, n$), a *parallel class* of blocks is a set of $n$ blocks which partition the points. If the blocks can be resolved into $n$ parallel classes, such a transversal design is called *resolvable* and denoted RTD($k, n$).

**Fact.** $\text{RTD}(k, n) \iff \text{TD}(k + 1, n)$

More generally, a *σ-parallel class* is a configuration of blocks which covers every point exactly $σ$ times. For a list of positive integers $Σ = [σ_1, \ldots, σ_t]$ summing to $n$, a TD($k, n$) is *Σ-resolvable* if the blocks can be resolved into $σ_i$-parallel classes for $i = 1, \ldots, t$. 
Example.

RTD(3, 3)

\[
\begin{array}{ccc}
111 \\
222 \\
333 \\
123 \\
231 \\
312 \\
132 \\
213 \\
321 \\
\end{array}
\]

Two MOLS of order 3

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

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

RTD(3, 3)

\[
\begin{array}{c}
111 \\
222 \\
333 \\
123 \\
231 \\
312 \\
132 \\
213 \\
321 \\
\end{array}
\]

Two MOLS of order 3

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

$[1,2]$-res TD$(3, 3)$

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Two MOLS of order 3

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>
Group partitions

Let us say that a TD($k, m$) admits a $(\sigma, \gamma)$-group partition if each of the groups of size $m$ is written on some (algebraic) group $G$, if there exists a subset $H$ of $G$ with $|H| = \sigma$ and there exists a partition $b$ of the blocks so that, for every class $B \in b$, the set $\{H \ast B : B \in B\}$ is a $\gamma$-parallel class.

A TD($k, m$) always admits two ‘trivial’ $(\sigma, \gamma)$-group partitions at each of two extremes.

$(1, m)$-group partition: $H = \{id\}$ and $b = \{B\}$.

$(m, 1)$-group partition: $H = G$ and $b =$ singletons.

An RTD($k, m$) admits a $(1, 1)$-group partition.
Let us say that a TD($k, m$) admits a \((\sigma, \gamma)\)-group partition if each of the groups of size $m$ is written on some (algebraic) group $G$, if there exists a subset $H$ of $G$ with $|H| = \sigma$ and there exists a partition $b$ of the blocks so that, for every class $B \in b$, the set \( \{ H \ast B : B \in B \} \) is a $\gamma$-parallel class.

A TD($k, m$) always admits two ‘trivial’ $(\sigma, \gamma)$-group partitions at each of two extremes.

(1, $m$)-group partition: $H = \{ id \}$ and $b = \{ B \}$.

($m$, 1)-group partition: $H = G$ and $b =$ singletons.

An RTD($k, m$) admits a (1, 1)-group partition.
Theorem (Rees)

Let \( \Sigma = [\sigma_1, \ldots, \sigma_t] \). Suppose there exists a \( \Sigma \)-resolvable TD\((k, n)\) and a TD\((k, m)\) admitting, for each \( i \), a \((\sigma_i, \gamma_i)\)-group partition. Then there exists a \( \Gamma \)-resolvable TD\((k, mn)\), where \( \Gamma \) consists of \( m\sigma_i/\gamma_i \) copies of \( \gamma_i \), for \( i = 1, \ldots, t \).

Proof idea. This is a standard product, except for a key variation: we use ‘splitting bijections’ to arbitrarily lift a \( \sigma_i \)-parallel class to distinct points in the product, and then let \( H \) act on these blocks.
Proof sketch

Theorem (Main result, restated)

$TD(k, a), RTD(k, b), RTD(k, c)$ imply an $RTD(k, abc)$

Proof sketch.
Form many $a$-parallel classes in the $RTD(k, c)$.
Take Rees product $c \times a$, resulting in a $TD(k, ac)$ with many parallel classes and some $a$-parallel classes.
Join ‘1’s with ‘a’s to form $b$-parallel classes (and leftover ‘1’s).
Take another Rees product with $b$, yielding a resolvable TD.
Theorem (Main result, restated)

\( TD(k, a), \ RTD(k, b), \ RTD(k, c) \) imply an \( RTD(k, abc) \)

**Proof sketch.**
Form many \( a \)-parallel classes in the \( RTD(k, c) \).
Take Rees product \( c \times a \), resulting in a \( TD(k, ac) \) with many parallel classes and some \( a \)-parallel classes.
Join ‘1’s with ‘a’s to form \( b \)-parallel classes (and leftover ‘1’s).
Take another Rees product with \( b \), yielding a resolvable TD.\qed
An example

Consider $a = 8$, $b = 9$, $c = 13$. There exists an RTD(9, 13). By amalgamating parallel classes, this can be viewed also as a $[1^5, 8]$-resolvable TD(9, 13).

Now, consider a TD(9, 8), which admits both an $(8, 1)$- and a $(1, 8)$-partition. Rees then gives a $[1^{64}, 8^5]$-resolvable TD(9, 104).

Reorganizing, this is also $[1^{59}, 9^5]$-resolvable. Since there exists an RTD(9, 9), it admits both $(1, 1)$- and $(9, 1)$-group partitions. A second application of Rees gives a $[1^{9 \times 59}, 1^{5 \times 81}]$-resolvable TD(9, 936).

In other words, we have an RTD(9, 936) or equivalently a TD(10, 936). We conclude that $N(936) \geq 8$. 
An example

Consider $a = 8$, $b = 9$, $c = 13$. There exists an RTD(9, 13). By amalgamating parallel classes, this can be viewed also as a $[1^5, 8]$-resolvable TD(9, 13).

Now, consider a TD(9, 8), which admits both an $(8, 1)$- and a $(1, 8)$-partition. Rees then gives a $[1^{64}, 8^5]$-resolvable TD(9, 104).

Reorganizing, this is also $[1^{59}, 9^5]$-resolvable. Since there exists an RTD(9, 9), it admits both $(1, 1)$- and $(9, 1)$-group partitions. A second application of Rees gives a $[1^{9\times59}, 1^{5\times81}]$-resolvable TD(9, 936).

In other words, we have an RTD(9, 936) or equivalently a TD(10, 936). We conclude that $N(936) \geq 8$. 
An example

Consider $a = 8$, $b = 9$, $c = 13$. There exists an RTD(9, 13). By amalgamating parallel classes, this can be viewed also as a $[1^5, 8]$-resolvable TD(9, 13).

Now, consider a TD(9, 8), which admits both an $(8, 1)$- and a $(1, 8)$-partition. Rees then gives a $[1^{64}, 8^5]$-resolvable TD(9, 104).

Reorganizing, this is also $[1^{59}, 9^5]$-resolvable. Since there exists an RTD(9, 9), it admits both $(1, 1)$- and $(9, 1)$-group partitions. A second application of Rees gives a $[1^{9 \times 59}, 1^{5 \times 81}]$-resolvable TD(9, 936).

In other words, we have an RTD(9, 936) or equivalently a TD(10, 936). We conclude that $N(936) \geq 8$. 
An example

Consider $a = 8$, $b = 9$, $c = 13$. There exists an RTD(9, 13). By amalgamating parallel classes, this can be viewed also as a $[1^5, 8]$-resolvable TD(9, 13).

Now, consider a TD(9, 8), which admits both an $(8, 1)$- and a $(1, 8)$-partition. Rees then gives a $[1^{64}, 8^5]$-resolvable TD(9, 104).

Reorganizing, this is also $[1^{59}, 9^5]$-resolvable. Since there exists an RTD(9, 9), it admits both $(1, 1)$- and $(9, 1)$-group partitions. A second application of Rees gives a $[1^{9\times59}, 1^{5\times81}]$-resolvable TD(9, 936).

In other words, we have an RTD(9, 936) or equivalently a TD(10, 936). We conclude that $N(936) \geq 8$. 
## Improvements to the MOLS table

<table>
<thead>
<tr>
<th>factorization</th>
<th>$n$</th>
<th>$N_{\text{HCD}}(n)$</th>
<th>$N(n) \geq$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$8 \times 9 \times 13$</td>
<td>936</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>$8 \times 9 \times 17$</td>
<td>1224</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>$8 \times 11 \times 13$</td>
<td>1144</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>$16 \times 17 \times 19$</td>
<td>5168</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>$16 \times 17 \times 25$</td>
<td>6800</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>$16 \times 19 \times 31$</td>
<td>9424</td>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>$17 \times 19 \times 23$</td>
<td>7429</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>$17 \times 19 \times 29$</td>
<td>9367</td>
<td>16</td>
<td>17</td>
</tr>
</tbody>
</table>
Remarks

Our result implies that equality holds in MacNeish’s Theorem only for prime powers and possibly numbers of the form $n = q_1 q_2$ where $q_1 < q_2 := p^t$ and $p^\lfloor t/2 \rfloor < q_1$.

The technique can be iterated, but in light of $N(n) \geq n^{\frac{1}{14.8}}$ it is not worthwhile to do so very often.

The hypothesis (in the reformulated result) that there be an $\text{RTD}(k, c)$ can be weakened a little.
References


- THE END -