A Three-Factor Product Construction for Mutually Orthogonal Latin Squares*

Peter J. Dukes1,** and Alan C.H. Ling2

1Mathematics and Statistics, University of Victoria, Victoria, Canada, E-mail: dukes@uvic.ca
2Computer Science, University of Vermont, Burlington, VT, USA, E-mail: aling@cems.uvm.edu

Received December 17, 2013; revised March 14, 2014

Published online 29 April 2014 in Wiley Online Library (wileyonlinelibrary.com).
DOI 10.1002/jcd.21393

Abstract: It is well known that mutually orthogonal latin squares, or MOLS, admit a (Kronecker) product construction. We show that, under mild conditions, “triple products” of MOLS can result in a gain of one square. In terms of transversal designs, the technique is to use a construction of Rolf Rees twice: once to obtain a coarse resolution of the blocks after one product, and next to reorganize classes and resolve the blocks of the second product. As consequences, we report a few improvements to the MOLS table and obtain a slight strengthening of the famous theorem of MacNeish. © 2014 Wiley Periodicals, Inc. J. Combin. Designs 23: 229–232, 2015

Keywords: orthogonal latin square; transversal design; direct product

1. INTRODUCTION

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 taken to be from $\{1, \ldots, n\}$. The integer $n$ is called the order of the square.

Two latin squares $L$ and $L'$ of order $n$ are orthogonal if $\{(L_{ij}, L'_{ij}) : 1 \leq i, j \leq n\} = \{1, \ldots, n\}^2$; that is, two squares are orthogonal if, when superimposed, all ordered pairs of symbols are distinct.

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 if

*In memory of Rolf Rees.
**Research of Peter Dukes is supported by NSERC grant number 312595-2010.
and only if there exists a projective plane of order $n$. Consequently, $N(q) = q - 1$ for prime powers $q$.

Given latin squares $L$, of order $m$, and $M$, of order $n$, their Kronecker product $L \otimes M$ is a latin square of order $mn$. If $\{L^{(1)}, \ldots, L^{(k)}\}$ and $\{M^{(1)}, \ldots, M^{(k)}\}$ are families of MOLS of orders $m$ and $n$, then $\{L^{(1)} \otimes M^{(1)}, \ldots, L^{(k)} \otimes M^{(k)}\}$ is a family of MOLS of order $mn$. Hence, $N(mn) \geq \min\{N(m), N(n)\}$. Combining this with the above remarks yields a “basic” lower bound on $N(n)$.

**Theorem 1.1** (MacNeish’s Theorem). If $n = q_1 \ldots q_t$ is factored as a product of powers of distinct primes, then $N(n) \geq \min\{q_i - 1 : i = 1, \ldots, t\}$.

Although it has long been known [2] that $N(n) \to \infty$ (in fact, $N(n) \geq n^{14}/1000$ for large $n$ is shown in [1]), 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. Our main result is a small improvement directed at these challenging cases.

## 2. TRANSVERSAL DESIGNS AND RESOLVABILITY

In what follows, it is convenient to reformulate our discussion of MOLS using the language of designs.

A *transversal design* $TD(k, n)$ 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 $k$ that are pairwise disjoint transversals of the partition. We have the existence of $r$ MOLS of order $n$ if and only if a $TD(r + 2, n)$ exists. The equivalence is seen by indexing groups of the partition by rows, columns, and symbols from each square.

In a $TD(k, n)$, a *parallel class* of blocks is a set of $n$ blocks that partition the points. If the blocks can be resolved into $n$ parallel classes, such a transversal design is called *resolvable* and denoted $RTD(k, n)$. The blocks of each parallel class in an $RTD(k, n)$ can be extended by one new point in an extra group. In this way, it is easy to see that an $RTD(k, n)$ is equivalent to a $TD(k + 1, n)$.

More generally, a *$\sigma$-parallel class* is a configuration of blocks that covers every point exactly $\sigma$ times. For a list of positive integers $\Sigma = [\sigma_1, \ldots, \sigma_t]$ summing to $n$, a $TD(k, n)$ is $\Sigma$-resolvable if the blocks can be resolved into $\sigma_i$-parallel classes for $i = 1, \ldots, t$. In writing a list $\Sigma$, we use “exponential notation” such as $\sigma^j$ to abbreviate $j$ occurrences of $\sigma$.

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. We should interpret $H \ast B$ as $|H|$ blocks obtained under action of $H$ on $B$. Note that $H$ need not consist of automorphisms of the TD; that is, the blocks in $H \ast B$ need not belong to $B$.

A $TD(k, m)$ always admits two “trivial” $(\sigma, \gamma)$-group partitions at each of two extremes. We have a $(1, m)$-group partition, in which $H$ is the identity subgroup and $b$ is the trivial partition with all blocks in the same class, and also an $(m, 1)$-group partition, in which $H = G$ is the full group and $b$ is the partition into singleton block classes. An $RTD(k, m)$ admits a $(1, 1)$-group partition.

The following is a special case of Construction 2 in [5], due to Rolf Rees. A similar construction by the same author later appears in [4] in the context of transversal designs.
Construction 2.1 (Rees, [4, 5]). 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 $i = 1, \ldots, t$.

This is essentially the standard direct product in which blocks of the TD($k$, $n$) are replaced by copies of the TD($k$, $m$). For resolving, the key idea is this: given a $\sigma$-parallel class $C$ in the TD($k$, $n$) and a $(\sigma, \gamma)$-group partition $(H, b)$ of the TD($k$, $m$), we can “split” the occurrences of blocks in $C$ incident with each point $x$ using bijections onto $\{x\} \times H$ in the product. Then, we can select $\gamma$-parallel classes in the product according to the action of $H$ on $b$.

Note that a $(\sigma, \gamma)$-group partition is a stronger hypothesis than is actually needed for the construction in [5], where different subsets of $G$ can be taken in each group. Since we only need the “easy” group partitions mentioned above, we adopt our stronger, simplified hypothesis for clarity. In any case, with this construction we are ready to state and prove our main result.

Theorem 2.2. For integers $a, b, c$ with $a \leq b \leq c$, we have

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

Proof. Equivalently, we construct an RTD($k$, $abc$) given TD($k$, $a$), RTD($k$, $b$), and RTD($k$, $c$). Put $c = aq + r$, $0 \leq r < a$. The last ingredient, an RTD($k$, $c$), can be regarded instead as a $\Sigma$-resolvable TD($k$, $c$), where $\Sigma = [1^r, a^q]$. Apply Construction 2.1, using $(1, a)$- and $(a, 1)$-group partitions of a TD($k$, $a$). The result is a $\Gamma$-resolvable TD($k$, $ac$), where

$$\Gamma = \left[1^{qa^2}, a^r\right].$$

Since $qa^2 + ar = ac > rb$, we may reorganize the classes to obtain a $\Gamma'$-resolvable TD($k$, $ac$), where

$$\Gamma' = \left[1^{qa^2-r(b-a)}, b^r\right] = \left[1^{ac-rb}, b^r\right].$$

Now, apply Construction 2.1 again with an RTD($k$, $b$), using $(1, 1)$- and $(b, 1)$-group partitions.

Corollary 2.3. For prime powers $p \leq q \leq r$, we have $N(pqr) \geq p$. \hfill $\square$

In particular, we have “easy” proofs of $N(18)$, $N(30) \geq 2$. In fact, Rees had already obtained those orthogonal latin squares using his construction, bypassing the step of “reorganizing” classes. This step is the key contribution of this paper; we next provide an example illustrating its usefulness.

Example 2.4. Consider $p = 8$, $q = 9$, $r = 13$. 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. It follows by Construction 2.1 that there exists a $[1^{64}, 8^5]$-resolvable TD(9, 104). Again, by restructuring classes, this can be viewed instead as $[1^{59}, 9^5]$-resolvable. Since there exists an RTD(9, 9), it admits both $(1, 1)$- and $(9, 1)$-group partitions. Applying Construction 2.1 again yields
TABLE I. Improvements to the table of MOLS in [3] from Theorem 2.2.

| Factorization   | $n$   | $N_{HCD}(n)$ | $N(n) \geq$ |
|-----------------|-------|--------------|-------------|
| $8 \times 9 \times 13$ | $= 936$ | $7$          | $8$         |
| $8 \times 9 \times 17$ | $= 1,224$ | $7$          | $8$         |
| $8 \times 11 \times 13$ | $= 1,144$ | $7$          | $8$         |
| $16 \times 17 \times 19$ | $= 5,168$ | $15$         | $16$        |
| $16 \times 17 \times 25$ | $= 6,800$ | $15$         | $16$        |
| $16 \times 19 \times 31$ | $= 9,424$ | $15$         | $16$        |
| $17 \times 19 \times 23$ | $= 7,429$ | $16$         | $17$        |
| $17 \times 19 \times 29$ | $= 9,367$ | $16$         | $17$        |

Table I gives a list of similar lower bounds on $N(n)$ that improve upon the bounds $N(n) \geq N_{HCD}(n)$ stated in [3] for $n < 10,000$. In fact, the entries of our table account for all integers $n$ having three or more prime power exact divisors such that $N_{HCD}(n)$ reports the MacNeish bound.

We should remark that $p, q, r$ need not be assumed relatively prime in Corollary 2.3. For instance, $N(31 \times 2^t) \geq 31$ for $t \geq 10$ by factoring $2^t = 2^5 \times 2^{t-5}$. However, we could find no cases for $n < 10,000$ where splitting prime powers improves the state of the art. We fail to improve $N_{HCD}(17 \cdot 2^4) = 16$, for instance, since $2^4 < 17$. In any case, we can conclude that “MacNeish numbers,” for which equality holds in Theorem 1.1, can only exist of the form $n = q_1q_2$ where $q_1 < q_2 := p^t$ and $p^{\lceil t/2 \rceil} < q_1$.

In closing, we should also note that Theorem 2.2 can be iterated, though in light of $N(n) \geq n^{1/p}$ for large $n$, it is not (at least asymptotically) worthwhile to iterate very often. But, for example, since $N(8 \times 9 \times 13) \geq 8$ and $8 \times 9 \times 13 < 5^5$, we also have $N(8 \times 9 \times 13 \times 5^{10}) \geq 9$.

REFERENCES

[1] T. Beth, Eine Bemerkung zur Abschätzung der Anzahl orthogonaler lateinischer Quadraten mittels Siebverfahren, Abh Math Sem Univ Hamburg 53 (1983), 284–288.
[2] S. Chowla, P. Erdős, and E. G. Strauss, On the maximal number of pairwise orthogonal latin squares of a given order, Canad J Math 12 (1960), 204–208.
[3] C. J. Colbourn and J. H. Dinitz, eds., The CRC Handbook of Combinatorial Designs, 2nd edition, CRC Press, Boca Raton, 2006.
[4] R. Rees, Truncated transversal designs: a new lower bound on the number of idempotent MOLS of side $n$, J Combin Theory Ser A 90 (2000), 257–266.
[5] R. Rees, Two new direct product-type constructions for resolvable group-divisible designs, J Combin Des 1 (1993), 15–26.