A GENERALIZATION OF WILSON'S CONSTRUCTION FOR MUTUALLY ORTHOGONAL LATIN SQUARES

Douglas Stinson

Abstract

Wilson's construction for mutually orthogonal Latin squares is generalized, and is used to construct 8 orthogonal squares of 98 orders where 8 orthogonal squares were not previously known. If $N(n)$ denotes the maximum number of mutually orthogonal Latin squares of order n, then $N(n) \geq 8$ if $n > 7474$.

1. *Introduction*

We assume that the reader is familiar with the terms *Latin square* and *mutually orthogonal Latin squares* (henceforth MOLS). Let $N(n)$ denote the maximum number of MOLS of order n.

For a list of lower bounds for $N(n)$, $n \leq 10000$, see Brouwer [1]. Also of interest are values n_r, where n_r denotes the largest order for which r MOLS are not known. For some small values of r, upper bounds for n_r have been obtained. See, for example, [1], [5], [6], and [7].

Some constructions for MOLS can be more easily described using the language of transversal designs, which we now define. We use the notation of Wilson [7].

Let $k \geq 2$, $n \geq 1$. A *transversal design*, abbreviated as $TD(k,n)$ is a triple $(X, G, \mathcal{A})$ where X is a set of kn elements, or *points*, $G = \{G_1, G_2, \ldots, G_k\}$ is a partition of X into k *groups* of n points each, and $\mathcal{A}$ is a set of subsets of X, called *blocks*, each containing exactly one point from each group, such that each pair $\{x,y\}$ of points from different groups occurs in an unique block of $\mathcal{A}$.

Thus it follows that each block contains k points, each point occurs

ARS COMBINATORIA, Vol. 8 (1979), pp. 95-105.

in n blocks, and there are n^2 blocks. It is convenient to define a TD(k,0) as having no points, k empty groups, and no blocks. Also, a TD(k,1) exists for any positive integer k.

The following is well-known (see, for example, [7]).

LEMMA 1.1. *There exist* k-2 *MOLS of order* n *if and only if there exists a* TD(k,n).

In [7], Wilson proves the following recursive construction for transversal designs.

THEOREM 1.2. *Let* (X, G, a) *be a* $TD(k + \ell, t)$ *where*

$$G = \{G_1,\ldots,G_k, H_1,\ldots,H_\ell\}.$$

Let $S \subseteq H_1 \cup \ldots \cup H_\ell$, *and let*

$$m \geq 0.$$

Suppose the following two conditions are satisfied.

(i) If $1 \leq j \leq \ell$, *then there exists a* $TD(k,h_j)$, *where* $h_j = |S \cap H_j|$

(ii) For each block $A \in a$, *there exists a* $TD(k,m + u_A)$ *having* $u_A = |S \cap A|$ *disjoint blocks.*

Then there exists a $TD(k,mt + s)$, *where* $s = |S|$.

In this paper, we extend Wilson's construction, in the direction of constructing a $TD(k,mt + ns)$. We are then able to construct eight MOLS of several orders where eight MOLS were not previously known.

2. *The Construction*

We first define the terms sub-TD and disjoint sub-TDs. Let (X, G, a) be a $TD(k,t)$. A sub-$TD(k,t')$ is a triple (Y, H, β) which is itself a $TD(k,t')$, with $Y \subseteq X$, $H = \{H_1,\ldots, H_k\}$, $H_i \subseteq G_i$ $1 \leq i \leq k$, and $\beta \subseteq a$. Suppose each (Y_i, H_i, β_i), $1 \leq i \leq j$, is a sub-$TD(k,t')$

of (X,G,a), a $TD(k,t)$. We say that the sub-TDs are *disjoint* if $Y_i \cap Y_{i'} = \emptyset$ if $i \neq i'$.

THEOREM 2.1. *Let* (X,G,a) *be a* $TD(k + \ell, t)$, *where* $G = \{G_1,\dots,G_k, H_1,\dots,H_\ell\}$. *Let* $S \subseteq H_1 \cup \dots \cup H_\ell$, *and let* $m, n \geq 0$. *Suppose the following two conditions are satisfied.*

(i) If $1 \leq j \leq \ell$, *then there exists a* $TD(k,nh_j)$, *where* $h_j = |S \cap H_j|$

(ii) For each block $A \in a$, *there exists a* $TD(k,m + nu_A)$ *containing* $u_A = |S \cap A|$ *disjoint sub-TDs* (k,n).

Then there exists a $TD(k,mt + ns)$, *where* $s = |S|$.

REMARKS

(1) If $n = 1$, we have Wilson's construction.

(2) If $s = 1$, we have a Moore-type construction (see [4] and [8]).

Proof. We use Wilson's notation. Let $X_0 = G_1 \cup G_2 \cup \dots \cup G_k$. For each block $A \in a$, put $A_o = A \cap X_o$, $A' = A \cap S$. Let M and N be sets of m and n elements respectively, and let $I_k = \{1,2,\dots,k\}$. We will construct (X^*, G^*, a^*), a $TD(k,mt + ns)$.

Let $X^* = (X_o \times M) \cup (I_k \times N \times S)$. Let $G^* = \{G_1^*,\dots,G_k^*\}$, where $G_i^* = (G_i \times M) \cup (\{i\} \times N \times S)$, for $1 \leq i \leq k$. It remains to describe the blocks.

For each block $A \in a$, construct a $TD(k,m + nu_A)$ with points $(A_o \times M) \cup (I_k \times N \times A')$, groups $((A_o \cap G_i) \times M) \cup (\{i\} \times N \times A')$, $1 \leq i \leq k$, and blocks β_A. We may specify that we have u_A disjoint sub-TDs as follows. For each $z \in A'$, we have groups $\{i\} \times N \times \{z\}$, $1 \leq i \leq k$, and blocks $\beta(A,z)$. Put $\beta_A' = \beta_A - \cup\, \beta_{(A,z)}$, and put $\beta = \bigcup_{A \in a} \beta_A'$.

Now, for each $j = 1,2,\ldots,\ell$, construct a $TD(k, nh_j)$ on points $I_k \times N \times (S \cap H_j)$, with groups $\{i\} \times N \times (S \cap H_j)$, $1 \le i \le k$, and blocks $\mathcal{C}_j$.

Put $\mathcal{a}^* = \beta \cup C_1 \cup C_2 \cup \ldots \cup C_\ell$. Then $(X^*, G^*, \mathcal{a}^*)$ is the required $TD(k,mt + ns)$.

We will verify that two points, x and y, from different groups G^*_i, $G^*_{i'}$, occur in a unique block of $\mathcal{a}^*$. We have three cases.

(1) $x = (g,m)$, $y = (g',m')$, $g \in G_i$, $g' \in G_{i'}$, $m,m' \in M$

(2) $x = (g,m)$, $y = (i',n,h)$, $g \in G_i$, $m \in M$, $h \in H_j$, $n \in N$

(3) $x = (i,n,h)$, $y = (i',n',h')$, $n,n' \in N$, $h \in H_j$, $h' \in H_j'$.

Case (1) There is a unique block $A \in \mathcal{a}$ such that $\{g,g'\} \subseteq A$. There is a unique block $B \in \beta'_A$ such that $\{(g,m), (g',m')\} \subseteq \beta'_A$. Since blocks of the $\mathcal{C}_j$s contain only points of $I_k \times N \times S$, therefore, B is the desired (unique) block.

Case (2) There is a unique block $A \in \mathcal{a}$ such that $\{g,h\} \subseteq A$. There is a unique block $B \in \beta'_A$ such that $\{(g,m), (i',n,h)\} \subseteq \beta'_A$. As in Case (1), B is the desired unique block.

Case (3) We have three subcases;

(a) $h = h'$ (hence $j = j'$)

(b) $h \neq h'$, $j \neq j'$.

(c) $h \neq h'$, $j = j'$.

Subcase (a): Whenever $h \in A$, where $A \in \mathcal{a}$, we have,

$$\{(i,n,h), (i',n',h')\} \subseteq \beta_{(A,h)}.$$

Thus $\{(i,n,h), (i',n',h')\}$ is contained in no block of β. However, $\{(i,n,h), (i',n',h')\}$ is contained in a unique block C of $\mathcal{C}_j$, and is contained in no block of any $\mathcal{C}_k$, if $k \neq j$.

Subcase (b): There is a unique block $A \in \alpha$ such that $\{h,h'\} \subseteq A$, since h,h' are in different groups of (X, G, α). Thus, there is a unique block $B \in \beta_A$ such that $\{(i,n,h),(i',n',h')\} \subseteq \beta_A$. B is the desired unique block of α^*.

Subcase (c): (i,n,h) and (i',n',h') are contained in a unique block of c_j, and in no other block of α^*.

We desire a corollary to theorem 2.1.

COROLLARY 2.2. *Suppose there exists a* TD(k+1, t), TD(k,nu), TD(k,m), *and a* TD(k, m+n) *containing a sub*-TD(k,n), *where* $0 \le u \le t$. *Then there exists a* TD(k,mt + nu).

Proof. In Theorem 2.1, take $\ell = 1$. Then, for each block A, $u_A = 0$ or 1. The results follows.

3. *Eight Mutually Orthogonal Latin Squares*

It is shown in [5] that $n_8 \le 9402$, and $N(n) \ge 8$ if $n \ge 7768$, $n \ne 9402$. In [1], Brouwer indicates that $N(9402) \ge 9$, but does not give details of the construction. For completeness we give the details here.

The following three corollaries of Wilson's construction are needed.

COROLLARY 3.1. *If* $0 \le w \le t$, *then* $N(mt + w) \ge \min \{N(m), N(m+1), N(t) - 1, N(w)\}$.

Proof. See [9].

COROLLARY 3.2. *If* $0 \le t \le w$, *then* $N(mt + w) \ge \min \{N(m), N(m+1), N(m+w) - 1, N(t) - w\}$.

Proof. See [11].

COROLLARY 3.3. *If* $t \ge w + \frac{1}{2}v(v-1)$, *then* $N(mt + v + w) \ge \min \{N(m), N(m+1), N(m+2), N(w), N(t) - v - 1\}$.

Proof. See [7].

As well, we use the following lemma.

LEMMA 3.4. *If* $n \geq 2$ *has prime power factorization*

$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots, p_k^{\alpha_k}$, *then* $N(n) \geq \min\{p_i^{\alpha_i}-1 : 1 \leq i \leq k\}$.

Also, N(1) *is greater than any finite number.*

Proof. For $n \geq 2$, see [2]. The statement regarding N(1) follows from lemma 1.1, and the existence of a TD(k,1) for any positive integer k.

LEMMA 3.5. $N(9402) \geq 9$.

Proof. The following sequence of constructions implies the result.

TABLE I

n	bound for N(n)	m	t	v	w	Corollary or Lemma
31	30					3.4
32	31					3.4
23	22					3.4
41	40					3.4
723	12	31	23		10	3.2
724	10	31	23		11	3.1
725	24					3.4
1	∞					3.4
13	12					3.4
9402	9	723	13	2	1	3.3

A list of orders for which 8 MOLS are not known can be found in [1]. Using our construction, we are able to eliminate many of the previous unknown orders. In order to apply corollary 2.2 we need a TD(10, m+n) containing a sub-TD(10, m). We will use the following.

LEMMA 3.6. *(1) There exists a* TD(10, 82) *containing a* sub-TD(10, 9).

(2) There exists a TD(10, 100) *containing a* sub-TD(10, 11).

Proof. The TD's are constructed in [3]. Although it is not explicitly stated there, they do contain the desired sub-TD's. This is evident from the fact that the TD(10, 82) is "constructed from" GF(73), together with 9 ideal elements. A similar remark applies to the TD(10, 100). For details of the method of construction, see [10].

Thus, we obtain the following,

COROLLARY 3.7. *If* $0 \le u \le t$, $N(t) \ge 9$, *and* $N(9u) \ge 8$, *then* $N(73t + 9u) \ge 8$.

Proof. The result follows immediately from lemma 1.1, corollary 2.2, and lemmata 3.4 and 3.6.

In an analagous manner, we also have

COROLLARY 3.8. *If* $0 \le u \le t$, $N(t) \ge 9$, *and* $N(11u) \ge 8$, *then* $N(89t + 11u) \ge 8$.

We list applications of corollaries 3.7 and 3.8 in Table II below. Orders for which 7 MOLS were not previously known are indicated by *. The required number of MOLS of orders t, 9u, and 11u are guaranteed by lemma 3.4, with the exception that $N(315) \ge 8$, which can be obtained by taking $m = 16$, $t = 19$, and $u = 11$ in corollary 3.1, since $N(16)$, $N(9)$, $N(11) \ge 8$, and $N(19) \ge 9$, all by lemma 3.4.

TABLE II

t	u	Corollary	order of MOLS constructed	
11	1	3.7	812	*
11	3	3.7	830	*
11	9	3.7	884	*
13	1	3.7	958	*
13	9	3.7	1030	
13	11	3.7	1048	
11	9	3.8	1078	*
17	1	3.7	1250	*
13	9	3.8	1256	
17	3	3.7	1268	
13	11	3.8	1278	
17	11	3.7	1340	
19	1	3.7	1396	
19	3	3.7	1414	
17	1	3.8	1524	
17	9	3.8	1612	*
19	1	3.8	1702	
23	3	3.7	1706	*
23	11	3.7	1778	

TABLE II (continued)

t	u	Corollary	order of MOLS constructed
19	9	3.8	1790
23	13	3.7	1796
23	17	3.7	1832
25	1	3.7	1834
23	19	3.7	1850
25	13	3.7	1942
25	17	3.7	1978
27	1	3.7	1980
27	3	3.7	1998
27	11	3.7	2070
27	19	3.7	2142
23	9	3.8	2146
25	1	3.8	2236
29	17	3.7	2270 *
29	25	3.7	2342
31	9	3.7	2344
25	11	3.8	2346
31	13	3.7	2380
25	17	3.8	2412
31	19	3.7	2434
31	23	3.7	2470
31	27	3.7	2506
37	1	3.7	2710
29	13	3.8	2724
29	23	3.8	2834
37	17	3.7	2854
29	25	3.8	2856
31	9	3.8	2858
31	13	3.8	2902
37	23	3.7	2908
37	25	3.7	2926
37	29	3.7	2962
31	19	3.8	2968
37	31	3.7	2980
41	17	3.7	3146
43	3	3.7	3166
43	11	3.7	3238
43	13	3.7	3256
37	1	3.8	3304
43	19	3.7	3310
43	33	3.7	3436
37	27	3.8	3590
37	31	3.8	3634
47	23	3.7	3638
47	25	3.7	3656
49	9	3.7	3658
41	1	3.8	3660
49	17	3.7	3730
49	19	3.7	3748

TABLE II (continued)

t	u	Corollary	order of MOLS constructed
49	25	3.7	3802
53	3	3.7	3896
49	37	3.7	3910
43	9	3.8	3926
43	27	3.8	4124
43	29	3.8	4146
53	35	3.7	4184
53	37	3.7	4202
53	39	3.7	4220
53	41	3.7	4238
43	37	3.8	4234
59	13	3.7	4424
59	19	3.7	4478
47	29	3.8	4502
47	31	3.8	4524
59	31	3.7	4586
59	33	3.7	4604
61	17	3.7	4606
53	29	3.8	5036
67	17	3.7	5044
67	23	3.7	5098
67	51	3.7	5350
61	25	3.8	5704
83	27	3.7	6302
79	61	3.7	6316
71	1	3.8	6330
97	33	3.7	7378
101	9	3.7	7454
103	1	3.7	7528
79	67	3.8	7768

We obtain the following new bound for n_8.

THEOREM 3.4. $n_8 \leq 7474$.

Proof. In [5], it is shown that $N(n) \geq 8$ if $n > 7474$ and $n \neq 7528$, 7768, or 9402. Eight MOLS of order 9402 exist by lemma 3.5. In Table II, eight MOLS of order 7528 and 7768 are constructed. Thus, we have the result.

5. *Conclusion*

Thus, we have constructed eight MOLS of 98 new orders, and obtained the new bound $n_8 \leq 7474$.

REFERENCES

[1] A.E. Brouwer, *Mutually Orthogonal Latin Squares*, Math. Centr. report ZN 81/78.

[2] H.F. MacNeish, *Euler Squares*, Ann. Math. 23(1922) 221-227.

[3] R.C. Mullin, P.J. Schellenberg, D.R. Stinson, and S.A. Vanstone, *Some Results on the Existence of Squares*, Proceedings of the Symposium on Combinatorial Mathematics and Optimal Design, Fort Collins (1978), (to appear).

[4] E.H. Moore, *Concerning Triple Systems*, Math. An. 43(1893), 271-285.

[5] R.C. Mullin, P.J. Schellenberg, D.R. Stinson, and S.A. Vanstone, *On the Existence of 7 and 8 Mutually Orthogonal Latin Squares*, Dept. of Combinatorics and Optimization Research Report CORR, 78-14 (1978), University of Waterloo.

[6] D.R. Stinson, *A Note on the Existence of 7 and 8 Mutually Orthogonal Latin Squares*, Ars Combinatoria 6, (to appear).

[7] G.H.J. van Rees, *A Corollary to a Theorem of Wilson*, Research Report CORR 78-15 (1978), University of Waterloo.

[8] W.D. Wallis, A.P. Street, J.S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Lecture Notes in Mathematics, no. 292, Springer-Verlag, Berlin 1972.

[9] R.M. Wilson, *Concerning the Number of Mutually Orthogonal Latin Squares*, Discrete Math. 9 (1974), 181-198.

[10] R.M. Wilson, *A Few More Squares*, Proc. 5th Southeastern Conf. on Combinatorics, Graph Theory and Computing, Boca Raton, Fla., (1974), 675-680.

[11] W. Wotjas, *On Seven Mutually Orthogonal Latin Squares*, Discrete Math. 20 (1977), 193-201.

The Ohio State University
Columbus, Ohio.