N(n) and $\nu(n)$: Similarities and Differences

Charles J. Colbourn
Department of Computer Science and Electrical Engineering
University of Vermont
Burlington, VT 05405

Jeffrey H. Dinitz
Department of Mathematics
University of Vermont
Burlington, VT 05405

November 3, 2017

1 Introduction and Definitions

Much has been written about the construction of sets of mutually orthogonal latin squares (MOLS). In [8], a lengthy survey of these constructions is given. Existence of MOLS is tabulated in [1], historical information appears in [9, 21], and proofs of many of the existence results appear in [1, 4, 21]. Rather than repeat these surveys here, we instead explore how some of the available constructions can be applied to a similar problem that has not been studied quite as extensively. We begin with some definitions.

A *latin square* of *side* n is an $n \times n$ array in which each cell contains a single element from an n-set S, such that each element occurs exactly once in each row and exactly once in each column. A latin square L of side n is *symmetric* if $L(i,j) = L(j,i)$ for all $1 \leq i,j \leq n$. A latin square L of side n is *idempotent* if $L(i,i) = i$ for all $1 \leq i \leq n$. Two latin squares L and L' of the same order are *orthogonal* if $L(a,b) = L(c,d)$ and $L'(a,b) = L'(c,d)$, implies $a = c$ and $b = d$. An equivalent definition for orthogonality is: Two latin squares of side n, $L = (a_{i,j})$ (on symbol set S) and $L' = (b_{i,j})$ (on symbol set S'), are *orthogonal* if every element in $S \times S'$ occurs exactly once among the n^2 pairs $(a_{i,j}, b_{i,j})$, $1 \leq i, j \leq n$.

A set of latin squares $L_1, \ldots, L_m$ is *mutually orthogonal*, or a set of *MOLS*, if for every $1 \leq i < j \leq m$, L_i and L_j are orthogonal. One of the most fundamental questions in combinatorics is: What is the size of the maximum set of mutually orthogonal latin squares of order n? Let $N(n)$ denote this number. It is easily shown that for all n, $N(n) \leq n - 1$. Good *lower* bounds for $N(n)$ are more difficult to establish. In Table 1 we give the current best lower bound for $N(n)$ for $n \leq 50$ when n is not a power of a prime. In the case that n is a prime power, that $N(n) = n - 1$ is well known, as we see later. Lower bounds for $N(n)$ for $n \leq 10,000$ are tabulated in [1], along with explicit constructions for small values of n. The dates of the results in Table 1 are interesting, pointing again to the fact that much research has been done recently in this area.

Order	$N(n) \geq$	Year	Reference(s)	Order	$N(n) \geq$	Year	Reference(s)
6	1	1900	[25]	33	5	1994	[1]
10	2	1960	[5]	34	4	1994	[1]
12	5	1961	[17]	35	5	1995	[32]
14	3	1985	[27]	36	5	1994	[23]
15	4	1978	[24]	38	4	1993	[3]
18	3	1978	[30]	39	4	1977	[18]
20	4	1989	[28]	40	7	1994	[2]
21	5	1991	[20]	42	5	1995	[1]
22	3	1978	[30]	44	5	1995	[1]
24	5	1992	[2, 22]	45	6	1995	[1]
26	4	1994	[7]	46	4	1974	[31]
28	5	1995	[1]	48	6	1996	[33]
30	4	1993	[3]	50	6	1974	[31]

Table 1: Best Current Lower Bounds on $N(n)$

We consider the analogue of orthogonal latin squares in the case where the latin squares are required to be symmetric. Suppose that L and M are idempotent, symmetric latin squares of the same order. Then L and

M are *orthogonal symmetric* latin squares if, for any two elements x and y, there exists at most one ordered pair (i, j) with $i < j$ such that $L(i, j) = x$ and $M(i, j) = y$. Orthogonal symmetric latin squares are not orthogonal latin squares, but they are as "orthogonal" as possible, given that they are symmetric. Necessarily, n is odd.

A set of symmetric latin squares $L_1, \ldots, L_m$ is *pairwise orthogonal symmetric*, or a set of *POSLS*, if for every $1 \leq i < j \leq m$, L_i and L_j are orthogonal. For odd n, let $\nu(n)$ denote the maximum size of a set of POSLS(n). Questions about $\nu(n)$, analogous to those asked about $N(n)$, are natural. One remark should be made immediately. While it is trivial to prove an attainable upper bound for $N(n)$, at this time a comparable upper bound for $\nu(n)$ has eluded researchers. In fact, there are two conflicting conjectures. It has been conjectured by Gross, Mullin, and Wallis [15] that $\nu(n) \leq (n-1)/2$, while Teirlinck [26] has conjectured that $\nu(n) \leq n-2$, with equality infinitely often. We return to the discussion of upper bounds for ν in Section 4.

n	$\nu(n) \geq$	n	$\nu(n) \geq$	n	$\nu(n) \geq$	n	$\nu(n) \geq$
1	$= \infty$	27	13	53	17	79	39
3	$= 1$	29	13	55	5	81	5
5	$= 1$	31	15	57	5	83	41
7	$= 3$	33	5	59	29	85	5
9	$= 4$	35	5	61	21	87	5
11	5	37	15	63	5	89	11
13	5	39	5	65	5	91	5
15	4	41	9	67	33	93	5
17	5	43	21	69	5	95	5
19	9	45	5	71	35	97	5
21	5	47	23	73	9	99	5
23	11	49	5	75	5	101	31
25	7	51	5	77	5	103	51

Table 2: Best Current Lower Bounds on $\nu(n)$

In Table 2, we give the current best lower bound for $\nu(n)$ for small values of n. These bounds come essentially from only three sources. In [19] it was shown that if $q \equiv 3 \pmod 4$, then $\nu(q) \geq (q-1)/2$. In [11] it was shown that if $n \geq 11$ ($n \neq 15$), then $\nu(n) \geq 5$. The other results are all in the case when q is a prime power and $q \equiv 3 \pmod 4$; these can be found in [10]. One can contrast this small number of sources with the much larger number of sources for the small values of N(n) given in Table 1. An extensive survey for all results on $\nu(n)$ is [13].

2 Transversal Designs and Villa Designs

Many combinatorial objects are intimately related to sets of MOLS. In this section and the next we examine some parallels between these objects, and similar objects that are related to sets of mutually orthogonal symmetric latin squares.

The first and most fundamental of these structures is the transversal design. A *transversal design* of *order* or *groupsize* n, and *blocksize* k, denoted $TD(k,n)$, is a triple $(V, \mathcal{G}, \mathcal{B})$, where

1. V is a set of kn elements;
2. $\mathcal{G}$ is a partition of V into k classes (called *groups*), each of size n (in each group the elements are labeled $1, \ldots, n$);
3. $\mathcal{B}$ is a collection of k-subsets of V (called *blocks*);
4. every unordered pair of elements from V is either contained in exactly one group, or is contained in exactly one block, but not both.

A transversal design is *idempotent* if it contains each block in which every entry is i, for $1 \leq i \leq n$. The existence of a $TD(k,n)$ is equivalent to the existence of $k-2$ mutually orthogonal latin squares of order n. To motivate our analogue in the case of symmetric latin squares, we review this equivalence.

Let $(V, \mathcal{G}, \mathcal{B})$ be a $TD(k,n)$. Now given any block $B \in \mathcal{B}$, say that B contains the element r from the first group and c from the second group. For $1 \leq t \leq n-2$ construct a latin square L_t by letting $L_t(r,c) = x$ if block B contains the element x in group number $t+2$. The conditions on the TD imply that each of the L_t are indeed latin and are pairwise orthogonal. This construction can be reversed. Obviously, $N(n)$ is the maximum k such that there exists a $TD(k+2,n)$.

We now define a new structure which is intended to be the analogue of transversal designs in the case where the latin squares in the construction of the preceding paragraph are orthogonal symmetric latin squares.

A *villa design* of *order* or *groupsize* n, and *blocksize* k, denoted $VD(k,n)$, is a triple $(V, \mathcal{G}, \mathcal{B})$, where

1. V is a set of kn elements;
2. $\mathcal{G} = \{G_1, \ldots, G_k\}$ is a partition of V into k classes (called *groups*), each of size n (denote $G_i = \{g_{i1}, \ldots, g_{in}\}$);
3. $\mathcal{B}$ is a collection of k-subsets of V (called *blocks*), each containing exactly one element from each group;
4. For $\{i,j\} \subset \{1,2,\ldots n\}$, $i \neq j$, there is either
   (a) exactly one block containing $\{g_{1i}, g_{2j}\}$ and no block containing $\{g_{2i}, g_{1j}\}$; or
   (b) exactly one block containing $\{g_{2i}, g_{1j}\}$ and no block containing $\{g_{1i}, g_{2j}\}$;
5. For $3 \leq h \leq k$ and $1 \leq i,j \leq n$, with $i \neq j$, element g_{hi} is contained in exactly one block intersecting $\{g_{1j}, g_{2j}\}$;
6. If $3 \leq h < \ell \leq k$ and $1 \leq i,j \leq n$, with $i \neq j$, the pair $\{g_{hi}, g_{\ell j}\}$ appears in at most one block;
7. If $1 \leq h < \ell \leq k$ and $1 \leq i \leq n$, the pair $\{g_{hi}, g_{\ell i}\}$ appears in no block.

There is a natural connection between villa designs and orthogonal symmetric latin squares.

Theorem 2.1 *There exists a villa design $VD(k,n)$ if and only if there exist $k-2$ pairwise orthogonal symmetric latin squares of order n.*

Proof: The proof is very similar to the proof that a $TD(k,n)$ is equivalent to $k-2$ MOLS. Let $(V, \mathcal{G}, \mathcal{B})$ be a $VD(k,n)$. Given any block $B \in \mathcal{B}$ say that B contains g_{1r} and g_{2c}. For $1 \leq t \leq k-2$ construct a latin square L_t by letting $L_t(r,c) = x$ *and* $L_t(c,r) = x$ if block B contains the element $g_{(t+2)x}$ in group G_{t+2}. Also let $L_t(i,i) = i$ for $1 \leq i \leq n$. Conditions 4 and

7 of the definition of VD imply that these squares are well defined and that they are symmetric and idempotent. Condition 5 implies that each of these squares is indeed a latin square, while condition 6 ensures that these squares are orthogonal symmetric latin squares. Again, this construction is easily reversed, proving the theorem. □

Obviously, $\nu(n)$ is the maximum k such that there exists a $VD(k+2, n)$. Much of the progress in finding new lower bounds for $N(n)$ has been facilitated by the use of recursive and direct constructions for transversal designs. Villa designs are introduced here in order to help researchers make renewed progress on questions concerning $\nu(n)$. Indeed we are able for the first time to give an analogue of what is arguably the most powerful TD construction, the Wilson construction, to the symmetric latin square case. This is done in Section 5.

3 Other Equivalences

We now examine several other analogies between MOLS and POSLS. Let S be a set of $n+1$ elements (*symbols*). A *Room square* of side n (on symbol set S) is an $n \times n$ array, F, which satisfies the following properties:

1. every cell of F either is empty or contains an unordered pair of symbols from S,
2. each symbol of S occurs once in each row and column of F,
3. every unordered pair of symbols occurs in precisely one cell of F.

A Room square of side n is *standardized* (with respect to the symbol ∞) if the cell (i, i) contains the pair $\{\infty, i\}$. The existence of a pair of orthogonal symmetric latin squares A and B on the symbol set $\{1, 2, \ldots n\}$ is equivalent to the existence of a Room square R of side n. Merely put the pair $\{x, y\}$ in cell (r, c) of R if $A(x, y) = r$ and $B(x, y) = c$. Similarly, to construct a Room square from a $VD(4, n)$, put the pair $\{x, y\}$ in cell (r, c) if the block B of the VD contains $g_{1x} \in G_1$, $g_{2y} \in G_2$, $g_{3r} \in G_3$ and $g_{4c} \in G_4$. Both of these constructions are easily reversed.

The notion of Room square generalizes to higher dimensions. A *Room d-cube* of side n is a d-dimensional cube of side n with the property that every 2-dimensional projection is a Room square of side n. The constructions of the previous paragraph carry over to this higher dimensional case. For example, given a set of d pairwise orthogonal symmetric latin squares $A_1, A_2, \ldots, A_d$ all on the symbol set $\{1, 2, \ldots n\}$ now put the pair $\{x, y\}$ in cell $(c_1, c_2, \ldots c_d)$ of R if $A_i(x, y) = c_i$ for all $1 \leq i \leq d$.

A *graeco-latin square* of side n is an $n \times n$ array where each cell contains an ordered pair ordered pair of elements and in addition, if a new square L is made from the first element from each of the cells and a second square R is made from the second element of each of the cells, then L and R are orthogonal latin squares of side n. With this definition, the existence of a graeco-latin square of side n is equivalent to the existence of a pair of orthogonal latin squares of side n. (The term graeco-latin is derived from the the fact that the first elements are often taken from the Greek alphabet, while the second elements are from the Latin alphabet).

Room squares and graeco-latin squares again evoke the similarity between these two concepts. One of the main differences is that Room squares have unordered pairs in each cell, while the pairs in the graeco-latin squares are ordered.

A further set of analogous objects are best described in graph terminology. A *1-factor* of a graph G is a set of edges from G which contain each vertex exactly once. A *1-factorization* of a graph G is a set $\mathcal{F} = \{F_1, \ldots, F_k\}$ of edge-disjoint 1-factors of G whose edge-sets partition the edge-set of G. Two 1-factorizations $\mathcal{F} = \{F_1, \ldots, F_k\}$ and $\mathcal{G} = \{G_1, \ldots, G_\ell\}$ of a graph are *orthogonal* if each 1-factor of $\mathcal{F}$ has at most one edge in common with each 1-factor of $\mathcal{G}$.

The existence of k orthogonal 1-factorizations of the complete bipartite graph $K_{n,n}$ is equivalent to the existence of k orthogonal latin squares of side n, while the existence of k orthogonal 1-factorizations of the complete graph K_n is equivalent to the existence of k orthogonal symmetric latin squares of side n.

The proof is essentially the same in both cases. Given a 1-factorization $\mathcal{F} = \{F_1, \ldots, F_n\}$ of $K_{n,n}$ construct a square $L = L(i, j)$ by $L(i, j) = x$ if the edge (i, j) is in F_x. An $n \times n$ square so constructed is indeed latin square. Given a set of k orthogonal 1-factorizations, the k latin squares formed by this procedure can be shown to be orthogonal.

When the underlying graph is K_n, in order to have a 1-factor it is necessary that n be even. So a 1-factor contains $n/2$ edges and a 1-factorization contains $n - 1$ 1-factors. Given a 1-factorization $\mathcal{F} = \{F_1, \ldots, F_{n-1}\}$ of K_n

construct a square $L = L(i,j)$ by $L(i,j) = x$ and $L(j,i) = x$ if the edge $\{i,j\}$ is in F_x. Also let $L(i,i) = i$ for $1 \leq i \leq n-1$. Here we have constructed a symmetric idempotent latin square of side $n-1$. Given a set of k orthogonal 1-factorizations of K_n the k symmetric latin squares formed by this procedure can be shown to be a set of symmetric orthogonal latin squares.

We summarize our discussions in the following two corollaries.

Corollary 3.1 *The existence of the following are equivalent:*

1. $N(n) \geq k$;
2. *k pairwise orthogonal latin squares of side n;*
3. *A transversal design $TD(k,n)$;*
4. *A set of k pairwise orthogonal 1-factorizations of the graph $K_{n,n}$.*

Corollary 3.2 *The existence of the following are equivalent:*

1. $\nu(n) \geq k$;
2. *k pairwise orthogonal symmetric latin squares of side n;*
3. *A villa design $VD(k,n)$;*
4. *A set of k pairwise orthogonal 1-factorizations of the graph K_{n+1};*
5. *A Room k-cube of side n.*

There are even more equivalent combinatorial structures. See [1, 12, 13] for further examples.

4 Finite Fields and the Upper Bounds

In this short section we briefly discuss the direct construction of MOLS and POSLS from algebraic structures like groups and fields.

The most basic construction gives a pair of orthogonal latin squares for every *odd* order n. Merely take the addition and subtraction tables in the group Z_n to get two orthogonal latin squares of side n. This construction was known to Euler [14], the first mathematician who had an interest in latin squares. There is no known comparable direct method (in Z_n or any other group) to get a pair of orthogonal symmetric latin squares.

Now let q be a prime power. In this case there is a well-known construction that gives $q-1$ MOLS of side q. For each $\alpha \in \mathrm{GF}(q)\backslash\{0\}$, define the latin square $L_\alpha(i,j) = i + \alpha j$, where $i, j \in \mathrm{GF}(q)$ where all the algebra is performed in GF(q). The set of latin squares $\{L_\alpha | \alpha \in \mathrm{GF}(q) \backslash \{0\}\}$ is a set of $q-1$ MOLS of side q.

In the case of orthogonal symmetric latin squares there is also a construction in the Galois field. The interested reader can find this construction in [13]. The theorem states that if $q = 2^k t + 1$ where t is odd, then there are t POSLS of side q. When $k = 1$, then $t = (q-1)/2$ which is one of the conjectured upper bounds for sets of POSLS of side q.

A set of $n-1$ MOLS of side n is called a *complete set* of MOLS(n) since it meets the upper bound. In this case it is known that the existence of a complete set of MOLS is equivalent to the existence of a projective plane of order n and indeed a complete set of MOLS exists for all prime power orders. Interestingly, in the case where the upper bound for the number of MOLS is met, there exists an extremely nice geometric object (the projective plane) that is equivalent to this set of MOLS. This is not known to be the case for symmetric latin squares. Not only is there no upper bound known that is attained infinitely often, but no nice geometric object is known to be equivalent to a "complete" set (whatever that might mean) of orthogonal symmetric latin squares. This is a crucial difference between the status of $N(n)$ and $\nu(n)$.

5 Splitting a Transversal Design

In this section we set up a framework for dealing with questions about $\nu(n)$ by using known constructions for MOLS and TDs. Our goal is to exploit the substantial knowledge about transversal designs to generate new discoveries concerning lower (and hopefully also upper) bounds for $\nu(n)$. This framework revolves around a connection between villa designs and transversal designs.

Let $V_1 = (V, \mathcal{G}, \mathcal{B}_1)$ be a villa design $VD(k,n)$ and let $\mathcal{B}_3$ be the set of idempotent blocks B_i (i.e. for each $1 \leq i \leq n$, B_i is the block containing the element i from each group). If there exists another villa design $V_2 = (V, \mathcal{G}, \mathcal{B}_2)$ with the property that $T = (V, \mathcal{G}, \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3)$ is a transversal design $TD(k,n)$, then V_1 is called an *embeddable* villa design (an EVD). Conversely, if a idempotent transversal design $TD(k,n)$ can be decomposed into two villa designs $VD(k,n)$ (plus the idempotent lines), then the transversal design is called *splittable* (STD).

Suppose that R is a standardized Room square of side r in which the entry $\{\infty, x\}$ has been replaced by $\{x, x\}$ for every x. Wallis [29] calls R an *embedded Room square* if it is possible to order every entry of R, replacing $\{x, y\}$ by either (x, y) or (y, x), and then to add further entries in such a way that the resulting array is a graeco-latin square of side r. We have the following proposition whose proof is left as an exercise for the interested reader.

Proposition 5.1 *The existence of an embedded Room square of side r is equivalent to the existence of an embeddable villa design of order r and block-size 4, an $EVD(4, r)$.*

A villa design $VD(k, n)$ has $\binom{n}{2}$ blocks while a $TD(k, n)$ has n^2 blocks so since $\binom{n}{2} + \binom{n}{2} + n = n^2$, the existence of a $EVD(k, n)$ is at least numerically possible. Indeed the following theorem proves their existence in the case when $k = 3$.

Lemma 5.2 *All $VD(3, n)$ are embeddable in a $TD(3, n)$.*

Proof: Let V_1 be a $VD(3, n)$. We construct V_2, also a $VD(3, n)$, which is disjoint from V_1. Let $\{g_{1a}, g_{2b}, g_{3c}\}$ be any block in V_1. Then let $\{g_{1b}, g_{2a}, g_{3c}\}$ be a block in V_2. From the properties of a villa design the blocks of V_1 are disjoint from the blocks of V_2 and the union of all these blocks, plus the idempotent blocks, gives an idempotent $TD(3, n)$. $\square$

In the next theorem we give an infinite class of EVDs for larger blocksize. We first need some definitions. Let G be an additive abelian group of odd order n. A *starter* in G is a set of unordered pairs $S = \{\{s_i, t_i\} : 1 \leq i \leq (n-1)/2\}$ which satisfies the following two properties:

1. $\{s_i : 1 \leq i \leq (n-1)/2\} \cup \{t_i : 1 \leq i \leq (n-1)/2\} = G \backslash \{0\}$
2. $\{\pm(s_i - t_i) : 1 \leq i \leq (n-1)/2\} = G \backslash \{0\}$

Let $S = \{\{s_i, t_i\} : 1 \leq i \leq (n-1)/2\}$ and $T = \{\{u_i, v_i\} : 1 \leq i \leq (n-1)/2\}$ be two starters in G. Without loss of generality, we may assume that $s_i - t_i = u_i - v_i$, for all i. Then S and T are said to be *orthogonal* starters if $u_i - s_i = u_j - s_j$ implies $i = j$, and if $u_i \neq s_i$ for all i.

Orthogonal starters were developed to construct sets of POSLS (see [13]). In our new terminology we have: The existence of k pairwise orthogonal starters in an abelian group G of order n implies the existence of a VD(k, n). It is instructive to see how this construction works. Let $S_1, S_2, \ldots S_k$ be a set of orthogonal starters in an abelian group of order n. From each starter $S = \{\{s_i, t_i\} : 1 \le i \le (n-1)/2\}$ define the translate $S+\alpha = \{\{s_i+\alpha, t_i+\alpha\} : 1 \le i \le (n-1)/2\}$. Then from the properties of starters, given any unordered pair $\{x, y\} \subset G$ there is precisely one $\alpha \in G$ such that $\{x, y\} \in S + \alpha$. Now to construct a VD(k, n), for each $\{x, y\} \in G$ define the block $B_{x,y}$ as the set of points $\{g_{1x}, g_{2y}, g_{3\alpha_1}, g_{4\alpha_2}, \ldots g_{k+2,\alpha_k}\}$ where $S_i + \alpha_i$ is the unique translate of the starter S_i that contains the pair $\{x, y\}$. Using the conditions on orthogonality of starters, it can be shown that the set of blocks $B_{x,y}$ where $\{x, y\} \in G$ defines a VD(k, n).

The most important class of orthogonal starters are the Mullin-Nemeth starters. Suppose q is a prime power with $q \equiv 3 \pmod 4$. Let R denote the set of residues in the multiplicative group of $GF(q)$ and let N denote the set of nonresidues. Now, for every $a \in N$, define $T_a = \{\{x, ax\} : x \in R\}$. The $(q-1)/2$ starters thus obtained are termed the *Mullin-Nemeth* starters. They have the property that they are all pairwise orthogonal. Thus there exists a $VD((q+3)/2, q)$ for all prime powers $q \equiv 3 \pmod 4$. The following theorem states that this VD is indeed embeddable.

Theorem 5.3 *Let $q \equiv 3$ (mod 4) be a prime power. Then there exists a $EVD((q+3)/2, q)$.*

Proof: Begin with $V_1 = (V, \mathcal{G}, \mathcal{B}_1)$, the $VD((q+3)/2, q)$ that is constructed from the Mullin-Nemeth starters. We assume that the groups are labeled G_1, G_2 and G_a for each $a \in N$, the nonresidues of GF(q). For a block $B \in V_1$, define $-B$ by $g_{i(-x)} \in -b$ if $g_{ix} \in B$ and let $\mathcal{B}_2 = \{-B | B \in \mathcal{B}_1\}$. We show that $(V, \mathcal{G}, \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3)$ is an idempotent TD$((q+3)/2, q)$, where $\mathcal{B}_3$ is the set of idempotent lines.

Let $a \in N$. For every $x \in R$ there is exactly one block B_x of V_1 that comes directly from the Mullin-Nemeth starter T_a (and not a translate of it). The block B_x contains the points $g_{1x}, g_{2(ax)}$ and for each $c \in N$ it contains $g_{c\alpha_c}$ where $T_c + \alpha_c$ is the unique translate of the starter T_c that contains the pair $\{x, ax\}$. Let $\mathcal{B}_{T_a}$ denote this set of blocks. Then $\alpha_a = 0$ for all blocks $b_x \in B_{T_a}$; in other words, all blocks in $\mathcal{B}_{T_a}$ contain the point g_{a0}.

Let $c \in N$. We must show, given any $u \ne v$, that exactly one block from either V_1 or V_2 contains $\{g_{au}, g_{cv}\}$. Now, all blocks of $\mathcal{B}_1$ are translates of the blocks in $\mathcal{B}_{T_a}$ and all blocks in $\mathcal{B}_2$ are translates of the blocks $\{-B|B \in \mathcal{B}_{T_a}\}$. So, it suffices to show that if a block $B_x \in \mathcal{B}_{T_a}$ contains the point $g_{c\omega}$, then there is no block in $\mathcal{B}_{T_a}$ that contains the point $g_{c(-\omega)}$.

The definition of α_c ensures that $\{x, ax\} = \alpha_c + \{z, cz\}$ for some $z \in R$; again, the block B_x contain the point $g_{c\alpha_c}$. Let B_y $(y \in R)$ be another block from the Mullin-Nemeth starter T_a. Since x and y are both quadratic residues, there exists another residue $r \in R$ where $xr = y$. So $\{y, ay\} = \{xr, axr\} = r\alpha_c + \{rz, crz\}$. Since $r\alpha_c$ is in the same residue class as α_c, the points in group c that are contained in blocks from $\mathcal{B}_{T_a}$ are precisely either the set of residues or the set of nonresidues. In either case, (since -1 is not a residue) if a block $B_x \in \mathcal{B}_{T_a}$ contains the point $g_{c\omega}$, then there is no block in $\mathcal{B}_{T_a}$ that contains the point $g_{c(-\omega)}$. The proof is complete when the conditions on groups 1 and 2 are checked. This is straightforward and is omitted here. $\Box$

It can be shown further that the idempotent TD$((q+3)/2, q)$ constructed in Theorem 5.3 can itself be extended to an idempotent TD(q, q) — an affine plane of order q. The $q-2$ idempotent MOLS that correspond to this plane can each be described by the equation $L_a(x, y) = ax + (1-a)y$ where the square L_a corresponds to the the ath group of the transversal design. The original villa design and its negative are embedded in the rows indexed by the nonresidues of $GF(q)$.

The basic motivation for the study of EVDs or STDs is to develop a general machinery which can, for example, apply standard recursive constructions for TDs to generate STDs, and hence to obtain new VDs and Room cubes. Indeed, the following theorem is a variant of Wilson's celebrated recursive construction for transversal designs. In this case, however, when certain ingredient TDs are splittable, so is the resulting design. In this way, we translate theorems on TDs into theorems on Room cubes.

Again we need some definitions in order to proceed. We must define the notion of holes in both TDs and VDs. For transversal designs it has been well studied; see [8]. A TD$(k, n+u; u)$ is a triple $(V, \mathcal{G}, \mathcal{B})$, where

1. V is a set of $k(n+u)$ elements;

2. $\mathcal{G}$ is a partition of V into k classes (called *groups*); each of size $n+u$ (in each group the elements are labeled $1, \ldots, n, \infty_1, \ldots \infty_u$);

3. $\mathcal{B}$ is a collection of k-subsets of V (called *blocks*);

4. every unordered pair of non-infinity elements from V is either contained in exactly one group, or is contained in exactly one block, but not both;

5. every infinity element and every non-infinity element from different groups are in exactly one block;

6. no block contains two infinity elements.

A VD$(k, n+u; u)$ is defined similarly. Essentially it has the same properties as a VD, except that two infinity type elements occur together in no blocks. The meaning of STD$(k, n+u; u)$ and EVA$(k, n+u; u)$ is also clear.

Theorem 5.4 *(a) If there exists a $STD(k+1, n)$, a $STD(k, m+u_i; u_i)$ for $1 \leq i \leq n$, and a $STD(k, u)$ where $u = \sum u_i$, then there exists a $STD(k, mn+u)$.*
(b) If there exists a $EVD(k+1, n)$, a $EVD(k, m+u_i; u_i)$ for $1 \leq i \leq n$, and a $EVD(k, u)$ where $u = \sum u_i$, then there exists a $EVD(k, mn+u)$.

Proof: Obviously these two statements are equivalent. We prove (a). Without the requirement that the TD be splittable, this statement is the simplest variant of Wilson's theorem beyond simple multiplication. A proof of Wilson's theorem is given in [6]; the statement here employs the $STD(k+1, n)$ as the master design, the $STD(k, m+u_i; u_i)$ for $1 \leq i \leq n$ as ingredient designs in the inflation, and the $STD(k, u)$ to fill the hole which results.

Now the split of the $STD(k+1, n)$ partitions the transversal design into $\mathcal{B}_1$, $\mathcal{B}_2$, and $\mathcal{B}_3$ where $\mathcal{B}_1$ and $\mathcal{B}_2$ are $VD(k+1, n)$s and $\mathcal{B}_3$ is the set of idempotent blocks. To split the final design, we find the $EVD(k, mn+u)$ which it contains. First, for each block in $\mathcal{B}_2$, erase all blocks which arise from the inflation of the block. Second, for each block in $\mathcal{B}_3$, employ the fact that the $STD(k, m+u_i; u_i)$ is splittable to retain only an $EVD(k, m+u_i; u_i)$ from the blocks obtained in the inflation. Finally, employ the fact that the $STD(k, u)$ is splittable to retain only an $EVD(k, u)$ from the blocks obtained in the inflation. All blocks obtained in the inflation of blocks from $\mathcal{B}_1$ are retained. It is now easy to verify that this is a $VD(k, mn+u)$, and that interchanging the roles of $\mathcal{B}_1$ and $\mathcal{B}_2$, and retaining the alternate $EVD(k, m+u_i; u_i)$ and $EVD(k, u)$, we obtain a disjoint $VD(k, mn+u)$ which supplies the embedding. □

In the previous theorem, it is not necessary that the VDs be embeddable. Of course, if the ingredients are not embeddable then neither is the resulting design. The following is a Wilson-type construction for VDs.

Theorem 5.5 *If there exists a $VD(k+1, n)$, a $VD(k, m+u_i; u_i)$ for $1 \leq i \leq n$, a $TD(k, m+u_i; u_i)$ for $1 \leq i \leq n$, and a $VD(k, u)$ where $u = \sum u_i$, then there exists a $VD(k, mn+u)$.*

Naturally, the previous two theorems extend to more sophisticated applications of Wilson's theorem. However, we content ourselves here with this basic one.

6 Conclusion

MOLS and transversal designs have been extensively explored, and difficult and elegant construction techniques have been found. POSLS and Room cubes have not been attacked with the same success, or with the same diligence. We believe that one reason for this is the difficulty of exploiting results on transversal designs in the symmetric case. For this reason, we have introduced villa designs (designs with many "rooms"), and shown that one of the more powerful recursive techniques for MOLS, Wilson's theorem, can now be employed for a restricted class of sets of POSLS. The eventual value of this "translation", by embedding villa designs into transversal designs, remains very much to be seen. Nevertheless, since examples of embeddable villa designs, and a powerful recursive construction, have both been found here, we expect that a study of Room cubes via this embedding approach will prove fruitful.

Acknowledgments

Thanks to Alan Ling and Dan Archdeacon for valuable observations on this research.

References

[1] R.J.R. Abel, A.E. Brouwer, C.J. Colbourn, and J.H. Dinitz, Mutually orthogonal latin squares, in: *CRC Handbook of Combinatorial Designs* (C.J. Colbourn, J.H. Dinitz; eds.), CRC Press, Boca Raton FL, 1996, pp. 111-142.

[2] R.J.R. Abel and Y.W. Cheng, Some new MOLS of order $2^n p$ for p a prime power, *Austral. J. Combin.* 10 (1994), 175-186.

[3] R.J.R. Abel and D.T. Todorov, Four MOLS of order 20, 30, 38 and 44, *J. Combinat. Theory (A)* 64 (1993), 144-148.

[4] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1986.

[5] R.C. Bose, S.S. Shrikhande and E.T. Parker, Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture, *Canad. J. Math.* 12 (1960), 189-203.

[6] A.E. Brouwer and G.H.J. van Rees, More mutually orthogonal latin squares, *Discrete Math.* 39 (1982), 263-281.

[7] C.J. Colbourn, Four MOLS of order 26, *J. Comb. Math. Comb. Comput.* 17 (1995), 147-148.

[8] C.J. Colbourn and J.H. Dinitz, Making the MOLS table, in: *Computational and Constructive Design Theory*, (W.D. Wallis, ed), Kluwer Academic Publishers, Boston, 1996, 67-134.

[9] J. Dénes and A.D. Keedwell, *Latin Squares: New Developments in the Theory and Applications*, North-Holland, Amsterdam, 1991.

[10] J.H. Dinitz, Room $n-$cubes of low order, *J. Austral. Math. Soc. (A)* 36 (1984), 237-252.

[11] J.H. Dinitz, The existence of Room 5-cubes, *J. Combinat. Theory (A)* 45 (1987), 125-138.

[12] J.H. Dinitz, Room Squares, in: *CRC Handbook of Combinatorial Designs* (C.J. Colbourn, J.H. Dinitz; eds.), CRC Press, Boca Raton FL, 1996, pp. 437-442.

[13] J.H. Dinitz and D.R. Stinson, Room squares and related designs, in: *Contemporary Design Theory: A Collection of Surveys* (J.H. Dinitz and D.R. Stinson, eds), John Wiley & Sons, New York, 1992, 137-204.

[14] L. Euler, Recherches sur une nouvelle espèce de quarrés magiques, *Verh. Zeeuw. Gen. Weten. Vlissengen* 9 (1782), 85-239.

[15] K.B. Gross, R.C. Mullin and W.D. Wallis, The number of pairwise orthogonal symmetric latin squares, *Utilitas Math.* 4 (1973), 239-251.

[16] T.P. Kirkman, On the perfect r-partitions of $r^2 - r + 1$, *Transactions of the Historic Society of Lancashire and Cheshire* (1850), 127-142.

[17] D.M. Johnson, A.L. Dulmage and N.S. Mendelsohn, Orthomorphisms of groups of orthogonal latin squares, *Canad. J. Math.* 13 (1961), 356-372.

[18] W.H. Mills, Some mutually orthogonal latin squares, *Proc. Eighth S.E. Conf. Combin. Graph Theory Computing*, 1977, pp. 473-487.

[19] R. C. Mullin and E. Nemeth, An existence theorem for Room squares, *Canad. Math. Bull* 12 (1969), 493-497.

[20] A.V. Nazarok, Five pairwise orthogonal latin squares of order 21, *Issled. oper. i ASU*, 1991, pp. 54-56.

[21] D. Raghavarao, *Constructions and Combinatorial Problems in Design of Experiments*, John Wiley & Sons, New York, 1971.

[22] C.E. Roberts Jr., Sets of mutually orthogonal latin squares with 'like subsquares', *J. Combinat. Theory (A)* 61 (1992) 50-63.

[23] C.E. Roberts Jr., Sets of mutually orthogonal latin squares with 'like subsquares' II, preprint.

[24] P.J. Schellenberg, G.H.J. van Rees and S.A. Vanstone, Four pairwise orthogonal latin squares of order 15, *Ars Combinat.* 6 (1978), 141-150.

[25] G. Tarry, Le problème de 36 officiers, *Ass. Franc. Av. Sci.* 29 (1900), 170-203.

[26] L. Teirlinck, Orthogonal one-factorizations, ordered designs and related structures, in: *Coding Theory, Design Theory, Group Theory*, (D. Jungnickel, S.A. Vanstone, et al, eds.), John Wiley & Sons, New York, 1993, 77-106.

[27] D.T. Todorov, Three mutually orthogonal latin squares of order 14, *Ars Combinat.* 20 (1985), 45-48.

[28] D.T. Todorov, Four mutually orthogonal latin squares of order 20, *Ars Combinat.* 27 (1989), 63-65.

[29] W.D. Wallis, A.P. Street and J.S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Springer-Verlag, Berlin, 1972.

[30] S.P. Wang, *On self-orthogonal latin squares and partial transversals of latin squares*, Ph.D. thesis, Ohio State University, 1978.

[31] R.M. Wilson, A few more squares, *Proc. Fifth Southeastern Conf. Combin. Graph Theory Computing* (1974), pp. 675-680.

[32] M. Wojtas, Five mutually orthogonal latin squares of order 35, *J. Combin. Designs* 4 (1996), 153-154.

[33] M. Wojtas, Six Mutually Orthogonal Latin Squares of Order 48, preprint, 1996.