Serdica J. Computing **7** (2013), No 1, 13–24

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ORTHOGONAL RESOLUTIONS AND LATIN SQUARES*

Svetlana Topalova, Stela Zhelezova

Abstract. Resolutions which are orthogonal to at least one other resolution (*RORs*) and sets of m mutually orthogonal resolutions (m*-MORs*) of 2-(v, k, λ) designs are considered. A dependence of the number of nonisomorphic RORs and m-MORs of multiple designs on the number of inequivalent sets of $v/k - 1$ mutually orthogonal latin squares (MOLS) of size m is obtained.

1. Introduction.

1.1. Mutually orthogonal resolutions of designs. For the basic concepts and notations concerning combinatorial designs and their resolvability refer, for instance, to [3], [4], [8] or [31].

Let $V = \{P_i\}_{i=1}^{v}$ be a finite set of *points*, and let $\mathcal{B} = \{B_j\}_{j=1}^{b}$ be a finite collection of k-element subsets of V, called *blocks*. If any 2-element subset of V is contained in exactly λ blocks of $\mathcal{B}$, then $D = (V, \mathcal{B})$ is a $2-(v, k, \lambda)$ *design*, or *balanced incomplete block design (BIBD)*. Each point of D is contained in r

ACM Computing Classification System (1998): G.2.1.

Key words: combinatorial design, orthogonal resolution, latin square.

*This work was partially supported by the Bulgarian National Science Fund under Contract No I01/0003.

blocks. We shall call two blocks B_1 and B_2 equal ($B_1 = B_2$) if they contain exactly the same points, and two designs $D_1 = (V_1, \mathcal{B}_1)$ and $D_2 = (V_2, \mathcal{B}_2)$ equal ($D_1 = D_2$) if $V_1 = V_2$ and $\mathcal{B}_1 = \mathcal{B}_2$.

Two designs are *isomorphic* if there exists a bijection from the point and block sets of the first design to respectively the point and block sets of the second design, and if this bijection does not change the point-block incidence. An *automorphism* is an isomorphism of the design to itself, i.e. a permutation of the points that maps the blocks into blocks.

Each 2-(v, k, λ) design determines the existence of 2-$(v, k, m\lambda)$ designs for any integer $m > 1$. The 2-$(v, k, m\lambda)$ designs are called *quasimultiples* of a 2-(v, k, λ) design. A $2-(v, k, m\lambda)$ quasimultiple design is called an *m-fold multiple* of 2-(v, k, λ) designs if there is a partition of its blocks into m subcollections $\mathcal{B}_1$, $\mathcal{B}_2$, $\ldots \mathcal{B}_m$, which form 2-(v, k, λ) designs $D_1, D_2, \ldots, D_m$. If $D_1 = D_2 = \cdots = D_m$ we call the design *a true m-fold multiple* of D_1.

A *parallel class* is a partition of the point set by blocks. A *resolution* of the design is a partition of the collection of blocks by parallel classes. We denote by q the number of blocks in a parallel class ($q = v/k$). We shall call two parallel classes of the resolution $\mathcal{R}$, R_1 and R_2 equal ($R_1 = R_2$) if each block of R_1 is equal to a block of R_2 and vice versa. The design is *resolvable* if it has at least one resolution. Two resolutions are *isomorphic* if there exists an automorphism of the design mapping each parallel class of the first resolution to a parallel class of the second one.

Two resolutions $\mathcal{R}_1$ and $\mathcal{R}_2$ of the same design are *mutually orthogonal* if every parallel class of $\mathcal{R}_1$ shares at most one block with every parallel class of $\mathcal{R}_2$ (blocks are labelled in this case). Orthogonal resolutions may or may not be isomorphic to each other. A *doubly resolvable design (DRD)* is a design which has at least two pairwise orthogonal resolutions. We denote by *ROR* a resolution which is orthogonal to at least one other resolution, and by *m-MOR* a set of m mutually orthogonal resolutions. Two m-MORs are *isomorphic* if there is an automorphism of the design mapping the first one to the second one. The m-MOR is *maximal* if it cannot be extended to an $m+1$-MOR. We call two m-MORs *component equivalent* if there exists a bijection from the first to the second one, such that each resolution of the first m-MOR is mapped to an isomorphic resolution of the second one. This definition is not universally accepted, but gives useful additional information about the m-MORs considered.

1.2. Sets of mutually orthogonal latin squares. For the definitions and notations concerning sets of orthogonal latin squares we follow [9] and [17].

A *latin square of side (order) n* is an $n \times n$ array in which each cell contains a single symbol from an n-element set S, such that each symbol occurs exactly once in each row and exactly once in each column. A latin square exists for any integer side n. An $m \times n$ *latin rectangle* is an $m \times n$ array in which each cell contains a single symbol from an n-element set S, such that each symbol occurs exactly once in each row and at most once in each column. An $m \times n$ latin rectangle can always be completed to a latin square of side n.

Let L be a latin square of side n on a symbol set E_3 with rows indexed by the elements of the n-element set E_1 and columns indexed by the elements of the n-element set E_2. Let $\tau = \{(x_1, x_2, x_3) : L(x_1, x_2) = x_3\}$ and let a, b, and c be three different integers from the set $\{1, 2, 3\}$. The (a, b, c)-conjugate of L, $L_{(a,b,c)}$ has rows indexed by E_a, columns by E_b, and symbols by E_c, and is defined by $L_{(a,b,c)}(x_a, x_b) = x_c$ for each $(x_1, x_2, x_3) \in \tau$.

Two latin squares L_1 and L_2 are *equivalent (isotopic)* if there are three bijections from the rows, columns and symbols of L_1 to the rows, columns and symbols, respectively, of L_2 that map L_1 to L_2. L_1 and L_2 are *main class equivalent* if L_1 is equivalent to any conjugate of L_2.

Consider two latin squares L_1 and L_2 of side n with rows indexed by E_1, and columns by E_2. Let $L_1 = (a_{ij})$ on symbol set E_3 and $L_2 = (b_{ij})$ on symbol set E_4. These latin squares are *mutually orthogonal* if every element in $E_3 \times E_4$ occurs exactly once among the n^2 pairs $(a_{ij}, b_{ij}), i, j = 1, 2, \ldots, n$. A set of m latin squares $L_1, L_2, \ldots, L_m$ such that L_i and L_j are orthogonal for $i, j = 1, 2, \ldots, m, i \neq j$ is called *a set of mutually orthogonal latin squares (a set of MOLS).* A set of m MOLS of side n can have at most $n - 1$ elements, namely $2 \leq m < n$, but formally a set of m MOLS can be defined for $m = 1$ too, which is actually a latin square.

We give below definitions of conjugates and main class equivalence of sets of MOLS similar to the definitions of conjugates and main class equivalence of latin squares. For $m = 1$ they yield the corresponding definitions for latin squares.

Let $\mathcal{M}$ be a set of m MOLS $L_1, L_2, \ldots, L_m$ of side n with rows and columns indexed by the elements of the n-element sets E_1 and E_2 and on symbol sets $E_3, E_4, \ldots, E_{m+2}$ respectively. Let $\tau = \{(x_1, x_2, \ldots, x_{m+2}) : L_i(x_1, x_2) = x_{i+2}, i = 1, 2, \ldots, m\}$ and $\{a_1, a_2, \ldots, a_{m+2}\} = \{1, 2, \ldots, m+2\}$. The $(a_1, a_2, \ldots, a_{m+2})$ conjugate of $\mathcal{M}$, $\mathcal{M}_{(a_1,a_2,\ldots,a_{m+2})}$ contains the latin squares $L_i : L_i(x_{a_1}, x_{a_2}) = x_{a_{i+2}}$, $i = 1, 2, \ldots, m$ for each $(x_1, x_2, \ldots, x_{m+2}) \in \tau$.

Two sets of m MOLS $\mathcal{M}_a$ and $\mathcal{M}_b$ are *equivalent (isotopic)* if there are $m + 2$ bijections from $E_{a1}, E_{a2}, \ldots, E_{am+2}$ of $\mathcal{M}_a$ respectively to $E_{b1}, E_{b2}, \ldots, E_{bm+2}$ of $\mathcal{M}_b$ that map $\mathcal{M}_a$ to $\mathcal{M}_b$. This definition allows reordering of the rows and columns of all squares together and of the symbols of each square individually [17]. Owens and Preece [27] classify complete sets of MOLS of order 9 up to such equivalence.

$\mathcal{M}_a$ and $\mathcal{M}_b$ are *main class equivalent* if $\mathcal{M}_a$ is equivalent to some conjugate of $\mathcal{M}_b$.

1.3. Applications. MORs can be used in cryptography, statistics, etc., see, for instance, [2], [5], [6], [24]. Applications, however, often depend on properties of the underlying design (block intersections for instance), or of the m-MOR (critical sets, etc.), which may not follow from the design parameters. From that point of view, classification results for doubly resolvable designs and orthogonal resolutions might be very useful.

1.4. Previous results. There are many papers devoted to the existence or nonexistence of DRDs with certain parameters and to setting lower bounds on m for the m-MORS with given parameters. The *starter-adder method* [28] is the most often and very successfully used one and many serious results have been obtained in this field. The newest achievements and an extended bibliography and summary of previous works can be found in [1] and [21]. For more details see for instance [10], [11], [12], [15], [19], [20], [22], [23], [33]. Another approach that has been used by some authors is to apply orthogonality tests to the resolutions of the classified designs with certain parameters and sometimes additional properties (automorphisms, etc.), see for instance, [7], [18], [29], [30].

A Room square of side n, $RS(n)$, is equivalent to a 2-MOR of a 2-$(n+1,2,1)$ BIBD. The first classification results that appeared were for Room squares with small parameters [13], [14], [26]. A computer classification of m-MORs with small parameters is presented in our recent paper [32] and the DRDs, RORs and m-MORs themselves can be downloaded from the first author's web page (presently http://www.moi.math.bas.bg/~svetlana).

1.5. The main result of this paper. The present work was inspired by problems, which appeared when we classified by computer search RORs, DRDs and m-MORs with small parameters [32], namely full classification was not possible for some parameters due to the very big number of non-isomorphic m-MORs of true m-fold multiples. We derive the lower bounds in the next section to illustrate the growth of this number with the parameters and to discuss other classification approaches.

The main result is Theorem 3.1, which is followed by useful corollaries.

2. Relation to latin squares.

Proposition 2.1. *Let D be a 2-(v,k,λ) design and $v=2k$ $(q=2)$.*

1) *D is doubly resolvable iff it is resolvable and each set of k points is contained either in no block, or in at least two blocks of the design.*

2) *If D is doubly resolvable and at least one set of k points is contained in m blocks, and the rest in* 0 *or more than m blocks, then D has at least one maximal m-MOR, no μ-MORs for $\mu > m$ and no maximal μ-MORs for $\mu < m$.*

Proof. If $v = 2k$ and one block of a parallel class is known, the point set of the second one of this class is known too. Suppose D has m-MOR $\mathcal{R}_1, \mathcal{R}_2, \dots \mathcal{R}_m$. Consider p equal blocks of the design. Denote by $1, 2, \dots, p$ the parallel classes of $\mathcal{R}_1$, in which these blocks are, the blocks themselves by $1_1, 2_1, \dots, p_1$ and the second blocks in the classes by $1_2, 2_2, \dots, p_2$. Since block i_1 should be with block j_2 $(i, j = 1, 2, \dots, p)$ at most once in a parallel class of the m-MOR, the class numbers of the second blocks form an $m \times p$ latin rectangle (see Figure 1).

Partition the collection of parallel classes of R_1 into subcollections P_1, P_2, $\dots$, P_s, such that two classes are in the same subcollection iff they are equal.

1) Consider two orthogonal resolutions $\mathcal{R}_1$ and $\mathcal{R}_2$ and let B_1 and B_2 form a parallel class of $\mathcal{R}_1$, while B_1 and B_2' and respectively B_1' and B_2 form parallel classes of $\mathcal{R}_2$. Then $B_1 = B_1'$ and $B_2 = B_2'$. As the parallel class containing B_1 and B_2 was arbitrary chosen, any block of D has at least one equal block, i.e. if a set of k points is contained in a block of D, then it is contained in at least 2 blocks.

2) Suppose each block has at least one equal block and D has a resolution $\mathcal{R}_1$. We can construct an orthogonal resolution $\mathcal{R}_2$ such that: the first block of each class is the first block of the corresponding class of $\mathcal{R}_1$ and the second blocks of the classes of P_i form a $2 \times |P_i|$ latin rectangle, $i = 1, 2, \dots, s$.

If D is a DRD, it has at least two orthogonal resolutions $\mathcal{R}_1$ and $\mathcal{R}_2$. The second blocks of P_i form a $2 \times |P_i|$ latin rectangle, $i = 1, 2, \dots, s$. A latin rectangle can be completed to a latin square. Since $|P_i| \geq m$, all $2 \times |P_i|$ latin rectangles can be completed to $m \times |P_i|$ latin rectangles, i.e. μ-MORs with $2 \leq \mu < m$ cannot be maximal, because they are extendable to m-MORs. Since $\exists i, |P_i| = m$, μ-MORs are not possible for $\mu > m$.

4 equal parallel classes of 3 mutually orthogonal resolutions of designs with $v = 2k$ (designs with parameters 2-$(6, 3, 16)$, 2-$(8, 4, 12)$, 2-$(10, 5, 32)$, 2-$(12, 6, 20)$, etc.)

$$\begin{array}{ccccccccccc}
 & 1 & 2 & 3 & 4 & & \multicolumn{4}{c}{\textit{latin rectangle}} \\
\mathcal{R}_1 & 1_1 1_2 & 2_1 2_2 & 3_1 3_2 & 4_1 4_2 & & 1 & 2 & 3 & 4 \\
\mathcal{R}_2 & 1_1 2_2 & 2_1 1_2 & 3_1 4_2 & 4_1 3_2 & \Longrightarrow & 2 & 1 & 4 & 3 \\
\mathcal{R}_3 & 1_1 3_2 & 2_1 4_2 & 3_1 1_2 & 4_1 2_2 & & 3 & 4 & 1 & 2
\end{array}$$

Fig. 1. m-MORs and latin squares

3. Relation to sets of MOLS.

Theorem 3.1. *Let $l_{q-1,m}$ be the number of main class inequivalent sets of $q-1$ MOLS of side m, $m \geq q$. Let the 2-(v,k,mλ) design D be a true m-fold multiple of a resolvable 2-(v,k,λ) design d, and $v = kq$. If $l_{q-1,m} > 0$, then D is doubly resolvable and has at least* $\begin{pmatrix} \frac{(v-1)\lambda}{k-1} + l_{q-1,m} - 1 \\ \frac{(v-1)\lambda}{k-1} \end{pmatrix}$ *m-MORs, which are nonisomorphic, but component equivalent.*

Proof. Consider a resolution $\mathcal{R}_1$ of D, such that each parallel class of $\mathcal{R}_1$ is equal to a parallel class of a resolution of d. Denote by r_d the number of parallel classes of d, $r_d = \dfrac{(v-1)\lambda}{k-1}$. We can partition the collection of blocks of $\mathcal{R}_1$ into subcollections $P_1, P_2, \ldots, P_{r_d}$ of size mq, such that each subcollection contains all q blocks of m equal classes. Consider an arbitrary subcollection P_i. Assign the parallel classes of P_i the numbers $1, 2, \ldots, m$, and the blocks in a parallel class the numbers $1, 2, \ldots, q$. Thus we denote by j the j-th parallel class in P_i, and by j_k its k-th block.

An m-MOR containing resolutions $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_m$ can be constructed as follows: Each resolution contains the same subcollections of equal blocks, but the parallel classes of blocks within these subcollections are different. Namely, the m parallel classes of P_i ($i = 1, \ldots, r_d$) satisfy:

- in each resolution:

  – the first block of the p-th parallel class is the same as the first block of the p-th parallel class of resolution $\mathcal{R}_1$;

  – the number ($1, 2, \ldots, q$) of any block in his parallel class is the same as its number in his parallel class of resolution $\mathcal{R}_1$.

- Blocks $2, \ldots, q$ of the parallel classes of P_i of resolutions $\mathcal{R}_2, \ldots, \mathcal{R}_m$ are chosen in such a way that their parallel class numbers in $\mathcal{R}_1$ form a set $\mathcal{M}_i$ of $q-1$ MOLS of side m $(L_1, L_2, \ldots, L_{q-1})$. The set of MOLS $\mathcal{M}_i$ is defined by $\tau = \{(x_1, x_2, \ldots, x_{q+1}) : L_j(x_1, x_2) = x_{j+2}, j = 1, 2, \ldots, q-1\}$, where x_1 is the number of the resolution of the m-MOR, x_2 the number of the parallel class of P_i, and x_j the class number (in P_i of $\mathcal{R}_1$) of the x_{j-1}-st block in the parallel class, $j = 3, \ldots, q+1$ (see Figure 2a).

The construction is applied to P_i for $i = 1, 2, \ldots, r_d$ and it follows from the definition of MOLS that these m resolutions are mutually orthogonal and form an m-MOR.

Permutation of parallel classes, numbers of equal classes, or resolutions of the m-MOR invokes respectively permutation of columns, symbols and rows of all latin squares in $\mathcal{M}_i$. A nontrivial point automorphism α can map some of the blocks of the classes of P_i to one another and thus invoke mapping of $\mathcal{M}_i$ to one of its conjugates (an example is presented in Fig. 2b), or α can map P_i to P_j for some $i \neq j, i, j = 1, 2, \ldots, r_d$ and thus $\mathcal{M}_i$ to a conjugate of $\mathcal{M}_j$. Therefore there are at least $l_{q-1,m}$ inequivalent ways to fix $\mathcal{M}_i$. To obtain a set of m-MORs we fix i_1 of the MOLS in the first way, i_2 in the second, ..., $i_{l_{q-1,m}}$ in the last, where $i_1 + i_2 + \cdots + i_{l_{q-1,m}} = r_d$.

Denote by $Q(u, w)$ the number of different ways to choose u integers i_1, i_2, ..., i_u, such that $i_1 + i_2 + \cdots + i_u = w$. Fixing i_1 in all the possible ways we get $Q(u, w) = \sum_{i=0}^{w} Q(u-1, w-i) = Q(u, w-1) + Q(u-1, w)$. It can be proved by induction that $Q(u, w) = \binom{u+w-1}{w}$. That is why there are at least $\binom{r_d + l_{q-1,m} - 1}{r_d}$ nonisomorphic m-MORs. Since P_i contains equal classes, all the resolutions of these m-MORs are isomorphic, and thus they are component equivalent. □

The next corollary follows directly from Proposition 2.1 and Theorem 3.1.

Corollary 3.2. *Let l_m be the number of main class inequivalent latin squares of side m. Let $q = 2$ and $m \geq 2$. Let the 2-$(v, k, m\lambda)$ design D be a true m-fold multiple of a resolvable 2-(v, k, λ) design d. Then D is doubly resolvable and has at least* $\left(\begin{array}{c}\frac{(v-1)\lambda}{k-1} + l_m - 1\\ \frac{(v-1)\lambda}{k-1}\end{array}\right)$ *nonisomorphic, but component equivalent m-MORs, no maximal i-MORs for $i < m$, and if d is not doubly resolvable, no i-MORs for $i > m$.*

Corollary 3.3. *Let N_d be the number of nonisomorphic resolvable 2-(v, k, λ) designs, and N_r the number of their nonisomorphic resolutions. The number of nonisomorphic RORs and m-MORs of 2-$(v, k, m\lambda)$ designs with $m \geq q$ is greater or equal to N_r and max$(N_r/m, N_d)$ respectively.*

Proof. Consider resolutions $\mathcal{R}_1$ and $\mathcal{R}_2$ of a 2-(v,k,$m\lambda$) design D, such that each of their parallel classes is equal to a parallel class of the nonisomorphic resolutions $\mathcal{T}_1$ and respectively $\mathcal{T}_2$ of a 2-(v,k,λ) design d. $\mathcal{R}_1$ and $\mathcal{R}_2$ are RORs by Theorem 3.1. Since D and d have the same group of automorphisms, there is no automorphism mapping the classes of $\mathcal{R}_1$ to classes of $\mathcal{R}_2$, so $\mathcal{R}_1$ and $\mathcal{R}_2$ are nonisomorphic.

a subcollection of 4 equal parallel classes of 4 mutually orthogonal resolutions ($m = 4$) and the corresponding set of two MOLS of side 4 for designs with $v = 3k$ ($q = 3$), namely designs with parameters 2-$(9, 3, 4)$, 2-$(12, 4, 12)$, 2-$(27, 9, 16)$, etc.

a) relation to a set $\mathcal{M}$ of two MOLS of side 4

$$\begin{array}{ccccc} & 1 & 2 & 3 & 4 \\ \mathcal{R}_1 & 1_1 1_2 1_3 & 2_1 2_2 2_3 & 3_1 3_2 3_3 & 4_1 4_2 4_3 \\ \mathcal{R}_2 & 1_1 2_2 3_3 & 2_1 1_2 4_3 & 3_1 4_2 1_3 & 4_1 3_2 2_3 \\ \mathcal{R}_3 & 1_1 3_2 4_3 & 2_1 4_2 3_3 & 3_1 1_2 2_3 & 4_1 2_2 1_3 \\ \mathcal{R}_4 & 1_1 4_2 2_3 & 2_1 3_2 1_3 & 3_1 2_2 4_3 & 4_1 1_2 3_3 \end{array} \Longrightarrow \begin{array}{ccccccccc} \multicolumn{9}{c}{\mathcal{M} = \mathcal{M}_{(1,2,3,4)}} \\ 1 & 2 & 3 & 4 & & 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 & & 3 & 4 & 1 & 2 \\ 3 & 4 & 1 & 2 & & 4 & 3 & 2 & 1 \\ 4 & 3 & 2 & 1 & & 2 & 1 & 4 & 3 \end{array}$$

$$\tau =$$
$$\{(1,1,1,1),(1,2,2,2),(1,3,3,3),(1,4,4,4),(2,1,2,3),(2,2,1,4),(2,3,4,1),(2,4,3,2),$$
$$(3,1,3,4),(3,2,4,3),(3,3,1,2),(3,4,2,1),(4,1,4,2),(4,2,3,1),(4,3,2,4),(4,4,1,3)\}$$

b) automorphism α mapping to one another the first and the second block of each parallel class of $\mathcal{R}_1$

$$\begin{array}{ccccc} & 1 & 2 & 3 & 4 \\ \mathcal{R}_1 & 1_2 1_1 1_3 & 2_2 2_1 2_3 & 3_2 3_1 3_3 & 4_2 4_1 4_3 \\ \mathcal{R}_2 & 1_2 2_1 3_3 & 2_2 1_1 4_3 & 3_2 4_1 1_3 & 4_2 3_1 2_3 \\ \mathcal{R}_3 & 1_2 3_1 4_3 & 2_2 4_1 3_3 & 3_2 1_1 2_3 & 4_2 2_1 1_3 \\ \mathcal{R}_4 & 1_2 4_1 2_3 & 2_2 3_1 1_3 & 3_2 2_1 4_3 & 4_2 1_1 3_3 \end{array}$$

Since parallel classes are sets (unordered) of blocks, this can be written as:

$$\begin{array}{ccccc} & 1 & 2 & 3 & 4 \\ \mathcal{R}_1 & 1_1 1_2 1_3 & 2_1 2_2 2_3 & 3_1 3_2 3_3 & 4_1 4_2 4_3 \\ \mathcal{R}_2 & 2_1 1_2 3_3 & 1_1 2_2 4_3 & 4_1 3_2 1_3 & 3_1 4_2 2_3 \\ \mathcal{R}_3 & 3_1 1_2 4_3 & 4_1 2_2 3_3 & 1_1 3_2 2_3 & 2_1 4_2 1_3 \\ \mathcal{R}_4 & 4_1 1_2 2_3 & 3_1 2_2 1_3 & 2_1 3_2 4_3 & 1_1 4_2 3_3 \end{array}$$

Since resolutions are collections (unordered) of parallel classes, this can be written as:

$$\begin{array}{ccccc} & 1 & 2 & 3 & 4 \\ \mathcal{R}_1 & 1_1 1_2 1_3 & 2_1 2_2 2_3 & 3_1 3_2 3_3 & 4_1 4_2 4_3 \\ \mathcal{R}_2 & 1_1 2_2 4_3 & 2_1 1_2 3_3 & 3_1 4_2 2_3 & 4_1 3_2 1_3 \\ \mathcal{R}_3 & 1_1 3_2 2_3 & 2_1 4_2 1_3 & 3_1 1_2 4_3 & 4_1 2_2 3_3 \\ \mathcal{R}_4 & 1_1 4_2 3_3 & 2_1 3_2 4_3 & 3_1 2_2 1_3 & 4_1 1_2 2_3 \end{array} \Longrightarrow \begin{array}{ccccccccc} \multicolumn{9}{c}{\mathcal{M}_{(1,3,2,4)}} \\ 1 & 2 & 3 & 4 & & 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 & & 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 2 & & 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 & & 3 & 4 & 1 & 2 \end{array}$$

$\mathcal{M}_{(1,3,2,4)}$ – the $(1, 3, 2, 4)$ conjugate of $\mathcal{M}$

α maps $(x_1, x_2, x_3, x_4) \in \tau$ to (x_1, x_3, x_2, x_4)

Fig. 2. m-MORs and MOLs

The m-MOR has m RORs. If all the RORs in each m-MOR are nonisomorphic, the number of m-MORs is N_r/m. The resolutions in the m-MOR are of one and the same design. That is why the number of m-MORs is at least N_d. □

4. Lower bounds. Unfortunately we do not know any results on the exact values of $l_{q-1,m}$ for $q > 2$, but useful lower bounds can be obtained in the following three cases.

4.1. Existence results. Research has been carried out [17] on the existence of sets of n MOLS of side m, i.e. for many parameters it is known whether $l_{q-1,m} > 0$. This can be used to establish existence of m-MORs for some parameters.

4.2. Lower bounds on the number of m-MORs with $q = 2$. The number of main class inequivalent latin squares of side m is known for many values of m, and thus for $q = 2$ lower bounds can be set using Corollary 3.2.

The growth of the number of m-MORs for higher m is illustrated by some lower bounds calculated by Corollary 3.2 and presented in Table 1.

Table 1. Lower bounds on the number of some m-MORs with $q = 2$ by Corollary 3.2.

v	k	λ	r_d	m	l_m	at least $\binom{r_d + l_m - 1}{r_d}$ m-MORs
6	3	16	10	4	2	11
6	3	20	10	5	2	11
6	3	24	10	6	12	352716
6	3	28	10	7	147	2.10^{15}
6	3	32	10	8	283657	3.10^{42}
6	3	36	10	9	19270853541	2.10^{96}
8	4	12	7	4	2	8
8	4	15	7	5	2	8
8	4	18	7	6	12	31824
8	4	21	7	7	147	33.10^{10}
8	4	24	7	8	283657	29.10^{33}
8	4	27	7	9	19270853541	19.10^{67}

The bound is rather rough, because it only counts a minimum of the m-MORS of the true multiple design. Computer results [32] establish that there are, for instance, 60 4-MORs of 2-(8,4,12) designs and at least 485 4-MORs of 2-(6,3,16).

4.3. Lower bounds on the number of RORs of quasimultiple designs. By Corollary 3.3 we can calculate lower bounds on the number of RORs for some parameters. If the designs with some parameters have many resolutions, the number of RORs of their multiples grows very fast with the parameters. For instance, computer results [32] show that there are no doubly resolvable 2-(10,5,8) designs, 5 RORs of 2-(10,5,16) and 6 RORs of 2-(10,5,24) designs. But 2-(10,5,16) designs have 27121734 resolutions, and thus by Corollary 3.3 there are at least

27121734 RORs of 2-(10,5,32) designs, and the classification of m-MORs for such a great number of RORs is impossible in reasonable time.

5. An open problem and some approaches. The very big number of nonisomorphic, but component equivalent m-MORs of true m-fold multiples is an obstacle for the classification even of m-MORs of quasimultiple designs with relatively small parameters.

Open problem. *To find classification criteria which will make it possible to obtain all* useful *(with respect to possible applications) m-MORs of quasimultiple designs for somewhat higher parameters.*

One of the approaches might be to classify only m-MORs of simple designs (without equal blocks), or only m-MORs of designs within some upper bound on the number of points, in which two blocks might intersect. Yet m-MORs of designs with several repeated blocks, or with several blocks intersecting in a great number of points, will not be considered then, but they can have m-MORs, which are interesting from application point of view.

Classification up to component equivalence might be another possible approach. Yet if two equivalent m-MORs are nonisomorphic, one of them might be extendable to an $m+1$-MOR, while the other might not be. That is why if the construction process implies backtrack search of i-MORs, and next of the $i+1$-MORs that contain each i-MOR (i=2,3,...), partial solutions cannot be eliminated effectively. Classification up to component equivalence will therefore be not much faster than the classification up to isomorphism.

REFERENCES

[1] Abel R., E. Lamken, J. Wang. A few more Kirkman squares and doubly near resolvable BIBDS with block size 3. *Discrete Math*, **308** (2008), 1102–1123.

[2] Archbold J., N. Johnson. A Construction for Room's Squares and an Application in Experimental Design. *Ann. Math. Statist,* **29** (1958), No 1, 219–225.

[3] Assmus E., J. Key. Designs and their Codes. Cambridge Tracts in Mathematics, Vol. **103**, Cambridge University Press, 1992.

[4] Beth Th., D. Jungnickel, H. Lenz. Design Theory. Cambridge University Press, 1993.

[5] Chaudhry G., J. Seberry. Secret sharing schemes based on Room squares, Combinatorics, Complexity and Logic. In: Proceedings of the DMTCS'96, Springer–Verlag, Singapore, 1996, 158–167.

[6] Chaudhry G., H. Ghodosi, J. Seberry. Perfect secret sharing schemes from Room squares. *J. Combin. Math. Combin. Comput.*, **28** (1998), 55–61.

[7] Cohen M., C. Colbourn, L.I ves, A. Ling. Kirkman triple systems of order 21 with nontrivial automorphism group. *Math. Comp.*, **71** (2002), No 238, 873–881.

[8] Colbourn C., J. Dinitz (Eds). The CRC Handbook of Combinatorial Designs. CRC Press, Boca Raton, FL, 2007.

[9] Colbourn C., J. Dinitz, I. Wanless. Latin squares. In: The CRC Handbook of Combinatorial Designs (Eds C. Colbourn, J. Dinitz), Boca Raton, FL, 2007, 135–151.

[10] Colbourn C., E. Lamken, A. Ling, W. Mills. The existence of Kirkman squares – doubly resolvable (v,3,1)-BIBDs. *Des Codes Cryptogr.*, **26** (2002), 169–196.

[11] Colbourn C., A. Rosa. Orthogonal resolutions of triple system. *Australas. J. Combin.*, **12** (1995), 259–269.

[12] Deza M., R. Mullin, S. Vanstone. Orthogonal systems. *Aequationes Math.*, **17** (1978), 322–330.

[13] Dinitz J. Room squares. In: The CRC Handbook of Combinatorial Designs (Eds C. Colbourn, J. Dinitz), Boca Raton, FL, 2007, 584–590.

[14] Dinitz J., D. Stinson. Room squares and related designs. In: Contemporary Design Theory: A Collection of Surveys (Eds J. Dinitz, D. Stinson), Wiley, 1992.

[15] Fuji-Hara R., S. Vanstone. On the spectrum of doubly resolvable designs. *Congr. Numer.*, **28** (1980), 399–407.

[16] Gelling E., R. Odeh. On 1-factorizations of the complete graph and the relationship to round-robin schedules. *Congr. Numer.*, **9** (1974), 213–221.

[17] Julian R., R. Abel, C. Colbourn, J. Dinitz. Mutually orthogonal latin squares (MOLS). In: The CRC Handbook of Combinatorial Designs (Eds C. Colbourn, J. Dinitz), Boca Raton, FL, 2007, 160–192.

[18] Kaski P., P. Östergård, S. Topalova, R. Zlatarski. Steiner Triple Systems of Order 19 and 21 with Subsystems of Order 7. *Discrete Math.*, **308** (2008), 2732–2741.

[19] Lamken E. Coverings, orthogonally resolvable designs and related combinatorial configurations. Ph.D. Thesis, Univ. of Michigan, 1983.

[20] Lamken E. Constructions for resolvable and near resolvable (v,k,$k-1$)-BIBDs. In: Coding Theory and Design Theory. Part II. Design Theory (Ed. D. Ray-Chaudhuri), Springer, 1990, 236–250.

[21] Lamken E. Designs with Mutually Orthogonal Resolutions and Decompositions of Edge-Colored Graphs. *J. Combin. Des.*, **17**(2009), No 6, 425-447.

[22] Lamken E., S. Vanstone. Designs with mutually orthogonal resolutions. *European J. Combin.*, **7** (1986), 249–257.

[23] Lamken E., S. Vanstone. The existence of a class of Kirkman squares of index 2. *J. Austral. Math. Soc.*, Ser. **A 44** (1988), 33–41.

[24] Martin W. Designs in product association schemes. *Des. Codes. Cryptogr.*, **16** (1999), No 3, 271–289.

[25] Mathon R., A. Rosa. 2-(v,k,λ) designs of small order. In: The CRC Handbook of Combinatorial Designs (Eds C. Colbourn, J. Dinitz), Boca Raton, FL, 2007, 25–57.

[26] Mullin R., W. Wallis. The existence of Room squares. *Aequationes Math.*, **13** (1975), 1–7.

[27] Owens P., D. Preece. Aspects of complete sets of 9 x 9 pairwise orthogonal latin squares. *Discrete Math.*, **167/168** (1997), 519–525.

[28] Rosa A., S. Vanstone. Starter-adder techniques for Kirkman squares and Kirkman cubes of small sides. *Ars Combin.*, **14** (1982), 199–212.

[29] Stinson D., S. Vanstone. Orthogonal packings in PG(5,2). *Aequationes Math.*, **31** (1986), 159–168.

[30] Tonchev V. Steiner triple systems of order 21 with automorphisms of order 7. *Ars Combin.*, **23** (1987), 93–96.

[31] Tonchev V. Combinatorial configurations. Longman Scientific and Technical, New York, 1988.

[32] Topalova S., S. Zhelezova. Doubly resolvable designs with small parameters. *Ars Combin.* (In print)

[33] Vanstone S. Doubly resolvable designs. *Discrete Math.*, **29** (1980), 77–86.

Svetlana Topalova, Stela Zhelezova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O.Box 323
5000 Veliko Tarnovo, Bulgaria
e-mail: `svetlana@math.bas.bg`
`stela@math.bas.bg`

Received November 5, 2012
Final Accepted April 16, 2013