Journal of Combinatorial Mathematics and Combinatorial Computing, 120: 231–239
DOI:10.61091/jcmcc120-020
http://www.combinatorialpress.com/jcmcc
Received 17 April 2024, Accepted 06 June 2024, Published 30 June 2024

Article

(2, w)-Threshold Schemes Constructed from Orthogonal Resolutions

Shyam Saurabh[1,*], **and Kishore Sinha**[2]

[1] Department of Mathematics, Tata College, Kolhan University, Chaibasa, India
[2] Formerly at Birsa Agricultural University, Ranchi, India and Presently at D201, Oceanus Tranquil, Ambedkar Road, Bangalore–560036

* **Correspondence:** vishal.deep1@bhu.ac.in

Abstract: A brief survey on mutually orthogonal resolutions of some combinatorial designs is presented. Some $(2, w)-$threshold schemes from mutually orthogonal resolutions of these designs are also obtained.

Keywords: Doubly resolvable designs, Mutually orthogonal resolutions, Threshold schemes, Combinatorial designs

1. Introduction

Definition 1. *(Balanced incomplete block design) A block design $D(v, b, r, k)$ is* resolvable *if the b blocks each of size k can be grouped into r resolution (or parallel) classes such that*

1. *Each resolution class contains $\frac{b}{r}$ blocks;*
2. *Every element is replicated exactly once in each resolution class.*

A balanced incomplete block design (BIBD) or a $2-(v,\ k,\ \lambda)$ design is an arrangement of v elements into $b = \frac{\lambda(v^2-v)}{(k^2-k)}$ blocks, each of size $k(< v)$ such that each element appears r times and each pair of distinct elements occurs λ times. We also denote such design as $(v,\ k,\ \lambda)-$BIBD. The integers v, b, r, k, λ are called parameters of the $(v,\ k,\ \lambda)-$BIBD and they satisfy the relations: $bk = vr,\ r(k-1) = \lambda(v-1)$.

A BIBD with $k = 3$ and $\lambda = 1$ is usually known as Steiner triple system (STS) or Steiner 2–design and a resolvable Steiner triple system is known as Kirkman triple system (KTS), see [1–3].

Example 1. *Consider a resolvable BIBD with parameters: $v = 9, b = 12, r = 4, k = 3, \lambda = 1$ whose resolution classes are:*

RI: [(1 2 3) (4 5 6) (7 8 9)]; RII: [(1 4 7) (2 5 8) (3 6 9)]; RIII: [(1 5 9) (2 6 7) (3 4 8)];
RIV: [(1 6 8) (2 4 9) (3 5 7)].

Definition 2. *(Group divisible design, frames and their orthogonal resolutions)*

A group divisible *(GD)* design *is an arrangement of $v = mn$ elements in b blocks such that*

1. *Each block contains $k(< v)$ distinct elements;*
2. *Each element occurs r times;*

3. *The elements can be divided into m groups each of size n such that any two distinct elements occur together in λ_1 blocks if they belong to the same group and in λ_2 blocks if they belong to different groups.*

The integers: $v = mn, b, r, k, \lambda_1$and λ_2 are known as parameters of the GD design and they satisfy the relations: $bk = vr; (n-1)\lambda_1 + n(m-1)\lambda_2 = r(k-1)$. Furthermore, if $r - \lambda_1 = 0$ then the GD design is singular (S); if $r - \lambda_1 > 0; rk - v\lambda_2 = 0$ then it is semi–regular (SR); and if $r - \lambda_1 > 0; rk - v\lambda_2 > 0$, then the design is regular (R). A GD design with parameters: $v = mn, b, r, k, \lambda_1 = 0, \lambda_2 = \lambda$ is also known as $(k, \lambda)-$GD design of type n^m for some positive integer m [4].

Example 2. *Consider the following resolvable solution of an SRGD design SR9 with parameters: $v = 8, b = 16, r = 4, k = 2, \lambda_1 = 0, \lambda_2 = 1, m = 2, n = 4$ as given in [5]:*

RI: [(1 5) (2 6) (3 7) (4 8)]; RII: [(2 7) (1 8) (4 5) (3 6)]; RIII: [(4 6) (3 5) (2 8) (1 7)];
RIV: [(3 8) (4 7) (1 6) (2 5)].

The arrangement of $v = 8$ elements in 2×4 array is given as: $\begin{matrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{matrix}.$

A holey or partial resolution class is a collection of blocks such that every element of $\mathcal{V} \backslash G, G \in \mathcal{G}$ occurs exactly once and the elements of G do not occur where $\mathcal{G}$ is a set of $'m'$ groups each of size n of the GD design. A uniform $(k, \lambda)-$frame of type n^m and index λ is a GD design with parameters: $v = mn, b, r, k, \lambda_1 = 0, \lambda_2 = \lambda$ such that

1. The block set $\mathcal{B}$ can be partitioned into a family $\mathcal{R} : R_1, R_2, \ldots, R_m$ of partial resolution classes;
2. Each $R_i \in \mathcal{R}$ can be associated with a group $G \in \mathcal{G}$ so that $R_i (1 \leq i \leq m)$ contains every element of $\mathcal{V} \backslash G$ exactly once.

Example 3. *Consider a (3; 1)–frame of type 2^4 given in [6] whose holey resolution classes are given below. This GD design is listed as R54 : $v = b = 8, r = k = 3, \lambda_1 = 0, \lambda_2 = 1, m = 4, n = 2$ in [5].*

Holey Resolution Classes	R^1	R^2	R^3	R^4
groups	{1, 5}	{2, 4}	{3, 6}	{7, 8}
blocks	{2, 6, 7}	{1, 6, 8}	{1, 4, 7}	{1, 2, 3}
	{3, 4, 8}	{3, 5, 7}	{2, 5, 8}	{4, 5, 6}

Example 4. *The following solution of a (3; 1) –frame of type 4^4 may be found in [7]. This GD design is listed as R86 : $v = 16, b = 32, r = 6, k = 3, \lambda_1 = 0, \lambda_2 = 1, m = n = 4$ in [5].*

Groups: {1, 2, 3, 4}; {7, 8, 9, 10}; {13, 14, 15, 16}; {19, 20, 21, 22}

Holey Resolution Classes

1 2 3 4		***7 8 9 10***	
7 13 20	*7 15 21*	*1 13 21*	*1 14 22*
8 16 22	*8 14 19*	*2 15 22*	*2 16 21*
9 14 21	*9 16 20*	*3 16 19*	*3 15 20*
10 15 19	*10 13 22*	*4 14 20*	*4 13 19*
13 14 15 16		***19 20 21 22***	
1 7 19	*1 8 20*	*1 9 15*	*1 10 16*
2 10 20	*2 9 19*	*2 8 13*	*2 7 14*
3 8 21	*3 7 22*	*3 10 14*	*3 9 13*
4 9 22	*4 10 21*	*4 7 16*	*4 8 15*

A uniform $(k, \lambda)-$frame of type n^m and index λ has a pair of orthogonal resolutions *if it admits $R = R_1, R_2, \ldots, R_m$ and $S = S_1, S_2, \ldots, S_m$ as different frame resolutions such that*

1. *For any group $G \in \mathcal{G}$, for any partial parallel class R_i associated with G in R and any partial parallel class S_j associated with G in S, $R_i \cap S_j = \varphi$;*
2. *For any different groups G_1 and G_2 of $\mathcal{G}$, for any partial parallel class R_i associated with G_1 in R and any partial parallel class S_j associated with G_2 in S, $\left|R_i \cap S_j\right| \leq 1$..*

For details on frames, their orthogonal resolutions and applications we refer to Furino et al. [8], Lamken [9] and Wang et al. [10].

A *triangular association scheme* is an arrangement of $v = \frac{n(n-1)}{2}$ elements in an $n \times n$ array such that the positions on the principal diagonal are left blank, the $\frac{n(n-1)}{2}$ positions above and below the principal diagonal are filled with the v elements in such a way that the resultant arrangement is symmetric about the principal diagonal. Then any two elements which occur in the same row or same column are first associates; otherwise, they are second associates. A partially balanced incomplete block (PBIB) design based on triangular association scheme is called a triangular design.

The integers $v = \frac{n(n-1)}{2}, b, r, k, \lambda_1$and λ_2 are known as parameters of the triangular design and they satisfy the relations: $bk = vr; 2(n-2)\lambda_1 + \frac{(n-2)(n-3)}{2}\lambda_2 = r(k-1)$.

Example 5. *Consider a triangular design* T9 *given in Clatworthy [5] with parameters:* $v = b = 10, r = k = 3, \lambda_1 = 1, \lambda_2 = 0$ *whose blocks are given as: (1 2 5); (8 9 10); (2 3 8); (5 7 9); (2 4 9); (5 6 8); (3 4 10); (6 7 10); (1 4 7); (1 3 6)*

The arrangement of 10 elements in 5×5 *array is given as:*
$$\begin{array}{ccccc} * & 1 & 2 & 3 & 4 \\ 1 & * & 5 & 6 & 7 \\ 2 & 5 & * & 8 & 9 \\ 3 & 6 & 8 & * & 10 \\ 4 & 7 & 9 & 10 & * \end{array}.$$

An (r, λ)−design is a collection $\mathcal{B}$ of subsets (blocks) from a finite set V of elements such that every element of V is contained in r blocks of $\mathcal{B}$ and every pair of distinct elements is contained in exactly λ blocks.

Suppose b blocks of a block design $D(v, b, r, k)$ can be divided into t $(= \frac{r}{\mu})$ classes, each of size $\beta = \frac{v\mu}{k}$ such that in each class of β blocks every element of D is replicated μ times. Then these t classes are known as μ−resolution (or parallel) classes and the design is called μ−resolvable design [11]. When $\mu = 1$ the design is said to be resolvable and the classes are called resolution classes.

Any two resolutions $R = R_1, R_2, \ldots, R_r$ and $S = S_1, S_2, \ldots, S_r$ of a resolvable block design $D(v, b, r, k)$ are orthogonal if $\left|R_i \bigcap S_j\right| \leq 1,\ 1 \leq i, j \leq r$. Further $D(v, b, r, k)$ is doubly resolvable if it has a pair of orthogonal resolutions. It should be noted that the blocks of the design are considered as labeled so that repeated blocks are treated as distinct. We write $m-$ MORs if $D(v, b, r, k)$ has a set of m mutually orthogonal resolutions.

Corresponding to a doubly resolvable design: $D(v, b, r, k)$, an $r \times r$ array $A = (A_{\mathrm{ij}})_{1 \leq i, j \leq r} = R_i \bigcap S_j; R_i \in R, S_j \in S$ can be formed such that the rows are indexed by the elements of R and columns by the elements of S. Hence any cell of A will either be empty or contain a block of D. Clearly A is row–wise as well as column–wise resolvable.

If the $r \times r$ array A is based on a $(v,\ 2,\ 1)$−BIBD, then it is known as a Room square or Kirkman square $\mathrm{KS}_2(v; 1, 1)$ of side $v - 1$ otherwise it is called a generalized Room square. Further when a doubly resolvable design is based on μ−resolvable BIBD, it is called doubly $\mu-$ resolvable and the corresponding $t \times t$ $(t = \frac{r}{\mu})$ array based on it is known as a Kirkman square, $\mathrm{KS}_k(v; \mu, \lambda)$ Stinson [12] and Abel et al. [13].

Example 6. *A Kirkman square* $KS_4(8; 3,\ 9)/$ *doubly 3– resolvable design based on a BIBD with parameters* $v = 8,\ b = 42,\ r = 21,\ k = 4,\ \lambda = 9$ *with empty diagonals is presented Table 1.*

A $(v,\ k,\ \lambda)$−BIBD is said to be near resolvable if its blocks can be partitioned into $'v'$ near or holey resolvable classes: $R_1, R_2, \ldots, R_v$ such that such that for each element x of the design there is precisely

–	1, 2, 7, 8	5, 6, 7, 8	3, 4, 5, 6	1, 2, 3, 4	1, 2, 5, 6	3, 4, 7, 8
1, 3, 5, 7	–	1, 2, 3, 4	1, 3, 6, 8	2, 4, 5, 7	2, 4, 6, 8	5, 6, 7, 8
1, 4, 6, 7	1, 4, 5, 8	–	2, 3, 5, 8	5, 6, 7, 8	2, 3, 6, 7	1, 2, 3, 4
1, 4, 5, 8	2, 3, 6, 7	3, 4, 7, 8	–	2, 4, 6, 8	1, 3, 5, 7	1, 2, 5, 6
2, 3, 5, 8	1, 3, 6, 8	1, 2, 5, 6	2, 4, 5, 7	–	3, 4, 7, 8	1, 4, 6, 7
2, 4, 6, 8	3, 4, 5, 6	1, 2, 7, 8	1, 4, 6, 7	1, 3, 5, 7	–	2, 3, 5, 8
2, 3, 6, 7	2, 4, 5, 7	3, 4, 5, 6	1, 2, 7, 8	1, 3, 6, 8	1, 4, 5, 8	–

Table 1. 7×7 KS$_4(8; 3,\ 9)$ with Empty Diagonals

one class which does not contain x in any of its blocks and each class contains $v-1$ distinct elements of the design. If D has a pair of near orthogonal resolutions then the design is known as doubly near resolvable, DNR$(v,\ k,\ \lambda)$−BIBD [14].

Corresponding to a DNR$(v,\ k,\ \lambda)$−BIBD, a $v \times v$ array $A = (A_{\text{ij}})_{1 \le i,j \le v} = R_i \bigcap S_j; R_i \in R, S_j \in S$ can be formed such that the rows are indexed by the elements of R and columns by the elements of S where $R = R_1, R_2, \ldots, R_v$ and $S = S_1, S_2, \ldots, S_v$ are near orthogonal resolutions of the design. Hence any cell of A will either be empty or contain a block of the design. Clearly A is row–wise as well as column–wise near resolvable. We write m−MNORs if a $(v,\ k,\ \lambda)$− BIBD has a set of m mutually near orthogonal resolutions.

Example 7. *The following example may be found in Abel et al. [13]. Rows and columns form orthogonal near resolutions (Table 2).*

–	–	3, 4, 8	1, 6, 7	–	–	–	2, 5, 9	–	–
–	–	–	0, 4, 9	2, 7, 8	–	–	–	3, 5, 6	–
3, 8, 9	–	–	–	0, 1, 5	–	–	–	–	4, 6, 7
1, 2, 6	4, 5, 9	–	–	–	0, 7, 8	–	–	–	–
–	2, 3, 7	0, 5, 6	–	–	–	1, 8, 9	–	–	–
–	–	1, 7, 9	–	–	–	–	4, 6, 8	–	0, 2, 3
–	–	–	2, 5, 8	–	1, 3, 4	–	–	0, 7, 9	–
–	–	–	–	3, 6, 9	–	0, 4, 2	–	–	1, 5, 8
4, 5, 7	–	–	–	–	2, 6, 9	–	0, 1, 3	–	–
–	0, 6, 8	–	–	–	–	3, 5, 7	–	1, 2, 4	–

Table 2. A Doubly Near Resolvable (10,3,2)-BIBD

Let $\mathcal{K}$ be a finite key space and P be a finite set of participants. In a secret sharing scheme, a special participant $D \notin P$, called the dealer, secretly chooses a key $K \in \mathcal{K}$ and distributes one share or shadow from the share set S to each participant in a secure manner, so that no participant knows the shares given to other participants. A $(t,\ w)$−threshold scheme is a secret sharing scheme in which if any $t(\le w)$ or more participants pool their shares, where $w = |P|$, then they can reconstruct the secret key $K \in \mathcal{K}$, but any $t-1$ or fewer participants can gain no information about it.

According to *Time Magazine* (May 4, 1992, p. 13), control of nuclear weapons in Russia in early 1990s depended upon "two–out–of–three" access mechanism. The three parties involved were the President, the Defense–minister and the Defense Ministry. This would correspond to a threshold scheme with $w = 3$ and $t = 2$, op. cit. Stinson and Vanstone [15], Stinson [16].

2. $(2, w)$ −threshold Schemes from Orthogonal Resolutions

Mutually orthogonal resolutions (m-MORs) of certain series of (v, k, λ)-BIBDs can be found in the works of Mathon and Vanstone [17], Abel et al. [13], and Topalova and Zhelezova [18–20].

Additionally, MORs of GD designs and (r, λ)-designs are discussed by Fuji-Hara and Vanstone [21], Vanstone [22], Lamken and Vanstone [23,24], Chang and Miao [25], and Dong and Wang [26]. Some key existence theorems on orthogonal resolutions are presented below:

Theorem 1. [9] *For any integer $k > 2$, there exists m_0 such that a $(k; k-1)$-frame of type k^m with a pair of orthogonal frame resolutions exists for any integer $m \geq m_0$.*

Theorem 2. [27] *Given any integers $k \geq 2$, $\lambda \geq 1$, and $n \geq 1$ such that $\lambda n \equiv 0 \pmod{k-1}$, there exists m_0 such that a $(k; \lambda)$-frame of type n^m with a pair of orthogonal frame resolutions exists for any integer $m \geq m_0$ that satisfies $n(m-1) \equiv 0 \pmod{k}$.*

Theorem 3. [14] *A DNR$(v, 4, 3)$-BIBD exists for all $v \equiv 1 \pmod{4}$ except for $v = 9$ and possibly for $v \in \{17, 213\}$.*

Theorem 4. [28] *There exist DNR$(3 \cdot 19^i + 1, 3, 2)$-BIBDs and DNR$(3 \cdot 31^i + 1, 3, 2)$-BIBDs for any positive integer i.*

Theorem 5. [29] *Let $q = 3t + 1$ be a prime power and $(3, t) = 1$. If 2 is a cube in the Galois field $GF(q)$, then there exists a set of four MNORs for a cyclically generated $(q, 3, 2)$-BIBD over $GF(q)$.*

Vanstone [29] also constructed a $(31, 3, 2)$-BIBD with seven MNORs; $(29, 4, 3)$-, $(19, 3, 2)$-, and $(37, 3, 2)$-BIBDs with five MNORs.

A 2-MOR of an $(n + 1, 2, 1)$-BIBD is equivalent to a Room square of side n, see Topalova and Zhelezova [19]. Chaudhry et al. [30] used the critical set of a Room square of side n or equivalently orthogonal resolutions of an $(n + 1, 2, 1)$-BIBD in constructing perfect secret sharing schemes, while Saurabh and Sinha [31] used critical sets of group divisible Room squares for the same purpose. Pieprzyk and Zhang [32] derived ideal (t, w)-threshold schemes from a $b^t \times (n + 1)$ orthogonal array $OA(b^t, n + 1, b, t)$ by considering $OA(i, j)$ as the shares of participants P_j (where $1 \leq j \leq n$) and $OA(i, 0)$ as a secret key (where $1 \leq i \leq b^t$), with $OA(i, j)$ denoting the entry in the ith row and jth column of $OA(b^t, n + 1, b, t)$. Stinson and Vanstone [15] obtained perfect threshold schemes from Steiner systems $S(t, w, v)$. Adachi and Lu [33] constructed $(3, 3)$-threshold schemes from magic cubes by considering the magic cube as a secret key and the corresponding three cubes as the shadows.

Although various secret sharing schemes exist in the literature, more schemes are desirable from the perspectives of secrecy and security. It is suggested to consider each of the w resolutions of a block design as shares and a combination of any two orthogonal resolutions or the corresponding Room square as a secret key of a $(2, w)$-threshold scheme. By considering w-MORs or w-MNORs of (v, k, λ)-BIBDs, GD designs, (r, λ)-designs, triangular designs, or any combinatorial designs and 2-MORs of frames, we may obtain $(2, w)$-threshold schemes. Tables 3-5 present $(2, w)$-threshold schemes derived from some combinatorial designs.

No.	(v, k, λ)**-BIBD**	**Source**	w**-MORs**
1	$(p^n, p, 1)$ - BIBD; $n \geq 2$	LV (1986)	$w = 2$
2	$(p + 1, 2, 1)$ - BIBD; $p = 2^k t + 1$	LV (1986)	$w = t$
No.	(r, λ)**-design**	**Source**	w**-MORs**
1	$\left(p^2 + p + 1, 1\right)$ - design	FV (1980)	$w = 2$
No.	**GD design:** $(v, r, k, \lambda_1, \lambda_2, m, n)$	**Source**	w**-MORs**
1	$\left(p^2 - ps, p, p - s, 0, 1, p - s, p\right)$	LV (1986)	$w = s + 1, 1 \leq s \leq p - 2$
2	$\left(2^n + 2, 2^n, 2, 0, 1, 2^{n-1} + 1, 2\right)$	LV (1986)	$w = 2^{n-1}; n \geq 2$
3	$\left(p^3 - p, p^2, p, 0, 1, p + 1, p^2 - p\right)$	LV (1988)	$w = p^2 - p$

Table 3. $(2, w)$-threshold Schemes from w-MORs of Designs

No.	Near resolvable (v, k, λ) - BIBDs	Source	w-MNORs
1	$(v, 4, 3)$ - BIBD; $v \equiv 1 \mod 4$; except for $v = 9$ and possibly for $v \in \{17, 213\}$	Abel and Chan [14]	2-MNORs
2	$\left(3 \cdot 19^i + 1, 3, 2\right)$ - and $\left(3 \cdot 31^i + 1, 3, 2\right)$ - BIBDs; i a positive integer	Lamken and Vanstone [28]	2-MNORs
3	$(q, 3, 2)$ - BIBD; $q = 3t + 1$ a prime power and $(3, t) = 1$	Vanstone [29]	4-MNORs
4	$(31, 3, 2)$ - BIBD	Stinson [29]	7-MNORs
5	$(29, 4, 3)$ -, $(19, 3, 2)$ -, and $(37, 3, 2)$ - BIBDs	Vanstone [29]	5-MNORs

Table 4. (2, w) - threshold Schemes from w-MNORs of Near Resolvable Designs

Abbreviations

p is a prime or prime power, FV stands for Fuji-Hara and Vanstone [21], and LV stands for Lamken and Vanstone, [28].

Given below are examples of mutually orthogonal resolutions of GD and triangular designs:

Example 8. *For $p = 5, s = 2$ in Series No. 1 of GD designs given in Table 3, we obtain 3– MORs of a GD design with parameters: $v = 15, r = 5, k = 3, b = 25, \lambda_1 = 0, \lambda_2 = 1, m = 3, n = 5$ which are presented below. This GD design is listed as SR28 in Clatworthy [5].*

I
(1, 2, 3); (6, 13, 14); (4, 9, 11); (5, 7, 15); (8, 10, 12)
(4, 5, 12); (6, 10, 11); (1, 14, 15); (3, 8, 13); (2, 7, 9)
(2, 10, 15); (5, 9, 13); (6, 7, 8); (1, 11, 12); (3, 4, 14)
(3, 7, 11); (4, 8, 15); (2, 12, 13); (9, 10, 14); (1, 5, 6)
(1, 8, 9); (7, 12, 14); (3, 5, 10); (2, 4, 6); (11, 13, 15)

II
(1, 2, 3); (6, 7, 8); (4, 5, 12); (9, 10, 14); (11, 13, 15)
(1, 8, 9); (2, 12, 13); (3, 4, 14); (6, 10, 11); (5, 7, 15)
(1, 5, 6); (3, 8, 13); (2, 10, 15); (4, 9, 11); (7, 12, 14)
(1, 11, 12); (4, 8, 15); (3, 5, 10); (6, 13, 14); (2, 7, 9)
(1, 14, 15); (2, 4, 6); (3, 7, 11); (5, 9, 13); (8, 10, 12)

III
(6, 13, 14), (4, 5, 12); (2, 10, 15); (3, 7, 11); (1, 8, 9)
(1, 2, 3); (6, 10, 11); (5, 9, 13); (4, 8, 15); (7, 12, 14)
(4, 9, 11); (1, 14, 15); (6, 7, 8); (2, 12, 13); (3, 5, 10)
(5, 7, 15); (3, 8, 13); (1, 11, 12); (9, 10, 14); (2, 4, 6)
(8, 10, 12); (2, 7, 9); (3, 4, 14); (1, 5, 6); (11, 13, 15)

The arrangement of $v = 15$ elements in 3×5 array is given as: $\begin{array}{ccccc} 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14. \\ 3 & 6 & 9 & 12 & 15 \end{array}$

Considering each of three resolutions as shares and a combination of any two orthogonal resolutions as secret key of the above GD design, we obtain a (2, 3) –threshold scheme.

Example 9. *2 –MOR of a triangular design with parameters: $v = 15, r = 6, k = 3, b = 30, \lambda_1 = 0, \lambda_2 = 2$ are presented below. Rows and columns form two different resolutions. This design is listed as T17 in Clatworthy [5].*

–	1, 10, 15	4, 7, 12	5, 6, 13	3, 9, 11	2, 8, 14
1, 10, 15	–	2, 9, 13	3, 8, 12	4, 6, 14	5, 7, 11
3, 8, 12	5, 6, 13	–	1, 11, 14	2, 7, 15	4, 9, 10
2, 9, 13	4, 7, 12	1, 11, 14	–	5, 8, 10	3, 6, 15
5, 7, 11	2, 8, 14	3, 6, 15	4, 9, 10	–	1, 12, 13
4, 6, 14	3, 9, 11	5, 8, 10	2, 7, 15	1, 12, 13	–

Table 5. Doubly Resolvable Triangular Design

This arrangement may be found in Sinha [34]. Considering each of two resolutions as shares and a combination of two orthogonal resolutions as secret key of the above triangular design, we obtain a (2, 2) –threshold scheme.

3. Conclusion

Here, a brief survey on mutually orthogonal resolutions of some combinatorial designs is presented and some $(2, w)-$threshold schemes are obtained from these mutually orthogonal resolutions. Two orthogonal resolutions have been used to coordinatize a two–dimensional square, called Room square however we could use $t-$MORs to coordinatize a $t-$dimensional hypercube. These $t-$MORs can also be used in secret sharing schemes. When $t = 3, k = 2, \lambda = 1$, a set of 3−MORs is commonly called a Room cube of side $v - 1$ based on D [29, 35]. Further considering each resolution as a share and a secret as Room cube obtained from 3−MORs of a block design, we can obtain $(3, w)-$threshold schemes. Some constructions and existence results of some other doubly resolvable combinatorial designs namely $H-$designs and Canonical Kirkman packing designs can be found in Meng [36], Wang [10] and Meng et al. [37]. The orthogonal resolutions of these designs can also be used to obtain (2, 2) –threshold schemes. Some examples of doubly near resolvable designs which are not frames can be found in Lamken and Vanstone [28] and Abel et al. [13].

An example of a doubly 3–resolvable BIBD is given below which is duplicate of an unreduced BIBD. It seems that there is a possibility of presenting a construction rule of a doubly $\mu-$resolvable BIBD with parameters: $v,\ b = 2\binom{v}{k}, r = 2\binom{v-1}{k-1}, k, \lambda = 2\binom{v-2}{k-2}; \mu = k$, obtained by the duplicate of an unreduced BIBD with parameters: $v,\ b = \binom{v}{k}, r = \binom{v-1}{k-1}, k, \lambda = \binom{v-2}{k-2}$, provided that v divides b.

Example 10. *Sinha and Kageyama [38] obtained a 3–resolvable BIBD with parameters:* $v = 7,\ b = 70,\ r = 30,\ k = 3,\ \lambda = 10$ *which is duplicate of an unreduced BIBD with parameters:* $v = 7,\ b = 35,\ r = 15,\ k = 3,\ \lambda = 5$. *A Kirkman square* $KS_3(7; 3,\ 10)$ *(or a doubly 3–resolvable design) as a* 10×10 *array with empty diagonals is presented in Table 6.*

–	–	2, 4, 5	3, 5, 6	2, 6, 7	–	1, 2, 3	1, 4, 6	1, 5, 7	3, 4, 7
3, 6, 7	–	1, 4, 6	1, 5, 7	1, 2, 3	3, 4, 5	–	–	2, 4, 7	2, 5, 6
1, 3, 5	3, 4, 6	–	2, 5, 6	–	2, 3, 7	1, 2, 4	4, 5, 7	–	1, 6, 7
4, 5, 6	1, 3, 5	2, 5, 7	–	–	1, 6, 7	3, 4, 7	–	2, 3, 6	1, 2, 4
1, 4, 7	1, 3, 6	–	2, 3, 4	–	–	4, 5, 6	2, 6, 7	1, 2, 5	3, 5, 7
2, 4, 6	1, 2, 5	3, 4, 5	–	1, 4, 7	–	2, 3, 7	1, 3, 6	5, 6, 7	–
–	2, 5, 7	1, 2, 6	4, 6, 7	3, 5, 6	1, 4, 5	–	1, 3, 7	–	2, 3, 4
2, 3, 5	2, 4, 7	1, 3, 7	–	1, 4, 5	1, 2, 6	5, 6, 7	–	3, 4, 6	–
1, 2, 7	–	3, 6, 7	1, 3, 4	2, 4, 6	4, 5, 7	–	2, 3, 5	–	1, 5, 6
–	4, 6, 7	–	1, 2, 7	3, 5, 7	2, 3, 6	1, 5, 6	2, 4, 5	1, 3, 4	–

Table 6. 10×10 $\mathrm{KS}_3(7; 3,\ 10)$ with Empty Diagonal

Conflict of Interest

The authors declare no conflict of interest.

References

1. Raghavarao, D., 1971. *Constructions and Combinatorial Problems in Design of Experiments* (Vol. 4). New York: Wiley.
2. Ray-Chaudhuri, D.K. and Wilson, R.M., 1971. Solution of Kirkman's schoolgirl problem. In *Proc. Symp. Pure Math* (Vol. 19, pp. 187-203).
3. Johnson, S.J. and Weller, S.R., 2001, November. Construction of low-density parity-check codes from Kirkman triple systems. In GLOBECOM'01. *IEEE Global Telecommunications Conference* (Cat. No. 01CH37270) (Vol. 2, pp. 970-974). IEEE.
4. Saurabh, S. and Sinha, K., 2023. Matrix approaches to constructions of group divisible designs. *Bull. ICA, 97*, pp.83-105.
5. Clatworthy, W.H., 1973. *Tables of Two-Associate-Class Partially Balanced Designs* (Vol. 63). US Government Printing Office.
6. Ge, G. and Miao, Y., 2006. PBDs, frames, and resolvability. In *Handbook of Combinatorial Designs* (pp. 287-291). Chapman and Hall/CRC.
7. Stinson, D.R., 1991. A survey of Kirkman triple systems and related designs. *Discrete Mathematics, 92*(1-3), pp.371-393.
8. Furino, S., Ying, M. and Jianxing, Y., 1996. *Frames and Resolvable Designs: Uses, Constructions and Existence* (Vol. 3). CRC press.
9. Lamken, E.R., 2015. The asymptotic existence of DR$(v, k, k-1)-$BIBDs. *Designs, Codes and Cryptography, 77*, pp.553-562.
10. Wang, S., 2019. Doubly Resolvable Canonical Kirkman Packing Designs and its Applications. *Graphs and Combinatorics, 35*, pp.1239-1251.
11. Kageyama, S. and Mohan, R.N., 1983. On μ-resolvable BIB designs. *Discrete Mathematics, 45*(1), pp.113-121.
12. Stinson, D.R., 2008. Combinatorial designs: constructions and analysis. *ACM SIGACT News, 39*(4), pp.17-21.
13. Abel, R.J.R., Lamken, E.R. and Wang, J., 2008. A few more Kirkman squares and doubly near resolvable BIBDs with block size 3. *Discrete Mathematics, 308*(7), pp.1102-1123.
14. Abel, R.J.R. and Chan, N.H., 2010. Existence of doubly near resolvable (v, 4, 3) BIBDs. *Australas. J Comb., 47*, pp.109-124.
15. Stinson, D.R. and Vanstone, S.A., 1988. A combinatorial approach to threshold schemes. *SIAM Journal on Discrete Mathematics, 1*(2), pp.230-236.
16. Stinson, D.R., 2005. *Cryptography: Theory and Practice.* Chapman and Hall/CRC.
17. Mathon, R. and Vanstone, S.A., 1980. On the existence of doubly resolvable Kirkman systems and equidistant permutation arrays. *Discrete Mathematics, 30*(2), pp.157-172.
18. Topalova, S. and Zhelezova, S., 2008. Sets of mutually orthogonal resolutions of BIBDs. In Proc. XI Intern. *Workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria* (pp. 280-285).
19. Topalova, S. and Zhelezova, S., 2013. Orthogonal resolutions and Latin squares. *Serdica Journal of Computing, 7*(1), pp.13-24.

20. Topalova, S. and Zhelezova, S., 2014. Doubly resolvable designs with small parameters. *Ars Comb., 117*, pp.289-302.

21. Fuji-Hara, R. and Vanstone, S.A., 1980. Transversal designs and doubly-resolvable designs. *European Journal of Combinatorics, 1*(3), pp.219-223.

22. Vanstone, S.A., 1980. Doubly resolvable designs. *Discrete Mathematics, 29*(1), pp.77-86.

23. Lamken, E.R. and Vanstone, S.A., 1986. Designs with mutually orthogonal resolutions. *European Journal of Combinatorics, 7*(3), pp.249-257.

24. Lamken, E.R. and Vanstone, S.A., 1986. Designs with mutually orthogonal resolutions. *European Journal of Combinatorics, 7*(3), pp.249-257.

25. Chang, Y. and Miao, Y., 2002. General constructions for double group divisible designs and double frames. *Designs, Codes and Cryptography, 26*, pp.155-168.

26. Dong, X. and Wang, J., 2023. Frames and Doubly Resolvable Group Divisible Designs with Block Size Three and Index Two. *Graphs and Combinatorics, 39*(5), p.109.

27. Wang, C., Chang, Y. and Feng, T., 2019. The asymptotic existence of frames with a pair of orthogonal frame resolutions. *Science China Mathematics, 62*, pp.1839-1850.

28. Lamken, E.R. and Vanstone, S.A., 1993. Existence results for doubly near resolvable (v, 3, 2)-BIBDs. *Discrete mathematics, 120*(1-3), pp.135-148.

29. Vanstone, S. A. (1982). On mutually orthogonal resolutions and near resolutions. *Annals of Discrete Mathematics, 15*, 357-369.

30. Chaudhry, G.R., Ghodosi, H. and Seberry, J., 1998. Perfect secret sharing schemes from Room squares. *Journal of Combinatorial Mathematics and Combinatorial Computing, 28*, pp.55-61.

31. Saurabh, S. and Sinha, K., 2022. Perfect secret sharing schemes from combinatorial squares. *Security and Privacy, 5*(6), p.e262.

32. Pieprzyk, J. and Zhang, X.M., 2002. Ideal threshold schemes from orthogonal arrays. In Information and Communications Security: 4th International Conference, ICICS 2002 Singapore, December 9–12, 2002 *Proceedings* 4 (pp. 469-479). Springer Berlin Heidelberg.

33. Adachi, T. and Lu, X.N., 2018. Magic Cubes and Secret Sharing Schemes (Algebras, Logics, Languages, and Related Areas). *Research Institute of Mathematical Sciences, Kokyuroku, 2096*, pp.115-118.

34. Sinha, K., 2019. A combinatorial arrangement of six elements. *Statistics & Applications, 17*, pp.7-9.

35. Dinitz, J.H. and Stinson, D.R., 1981. The spectrum of Room cubes. *European Journal of Combinatorics, 2*(3), pp.221-230.

36. Meng, Z., 2016. Doubly resolvable H designs. *Graphs and Combinatorics, 32*(6), pp.2563-2574.

37. Meng, Z., Zhang, B. and Wu, Z., 2021. Constructions of doubly resolvable Steiner quadruple systems. *Designs, Codes and Cryptography, 89*, pp.781-795.

38. Sinha, K. and Kageyama, S., 1990. On resolvability of duplicate designs. *Journal of Statistical Computation and Simulation, 36*, pp.40-42.