UTILITAS MATHEMATICA 122 (2025) 109–116

Utilitas Mathematica
www.combinatorialpress.com/um

Combinatorial Press

Tactical decomposable regular group divisible designs and their threshold schemes

Shyam Saurabh[1,✉]

[1] *Department of Mathematics, Tata College, Kolhan University, Chaibasa, India*

ABSTRACT

Some methods of decomposing $v(=mn)\times b$ incidence matrix of regular group divisible (RGD) designs into square submatrices of order m are described. Such designs are known as tactical decomposable designs. As a by–product, resolvable solutions of some RGD designs are obtained. A relationship between tactical decomposable designs and $(2,\ n)$ −threshold schemes is also given.

Keywords: regular group divisible design, tactical decomposable design, resolvability, partial cyclic solution, $(2,\ n)$ −threshold scheme

2020 Mathematics Subject Classification: 62K10, 05B05, 05B15, 94A62.

1. Introduction

A balanced incomplete block (BIB) design or a $2-(v,k,\lambda)$ design is an arrangement of v elements into $b=\lambda(v^2-v)/(k^2-k)$ blocks, each of size $k(<v)$ such that every element occurs in exactly r blocks and any two distinct elements occur together in λ blocks. Further a BIB design is symmetric if $v=b$ and is self –complementary if $v=2k$.

1.1. *Tactical decomposable design*

Let a (0, 1) – matrix N have a decomposition $N=[N_{ij}]_{i=1,2,\ldots,s;\ j=1,2,\ldots,t}$ where N_{ij} are submatrices of N of suitable sizes. The decomposition is called row tactical if row sum of N_{ij} is r_{ij} and column tactical if the column sum of N_{ij} is k_{ij} and tactical if it is row as well as column tactical. If N is the incidence matrix of a block design $D(v,b,r,k)$, D is called row (column) tactical decomposable. D is called uniform row (column) tactical decomposable if $r_{ij}=\alpha\,(k_{ij}=\beta)\,\forall i,j$. If each N_{ij} is an $m\times m$ matrix, D is called square tactical decomposable design, STD (m).

✉ Corresponding author.
E-mail address: shyamsaurabh785@gmail.com (S. Saurabh).

Received 24 January 2025; Accepted 21 March 2025; Published 28 March 2025.

DOI: 10.61091/um122-08

Several methods of constructions of tactical decomposable rectangular, group divisible and L_2-type designs may be found in Bekar et al. [2], Singh and Saurabh [19], Saurabh and Sinha [16, 17] and Saurabh [14], among others.

1.2. *Group divisible design*

Let $v = mn$ elements be arranged in an $m \times n$ array. A *regular group divisible* (*RGD*) *design* is an arrangement of the $v = mn$ elements in b blocks each of size k such that:

1. Every element occurs at most once in a block;
2. Every element occurs in r blocks;
3. Every pair of elements, which are in the same row of the $m \times n$ array, occur together in λ_1 blocks whereas remaining pair of elements occur together in λ_2 blocks; and
4. $r - \lambda_1 > 0,\ rk - v\lambda_2 > 0$.

Further let N be $v \times b$ incidence matrix of a block design such that $J_v N = kJ_{v\times b}$ and satisfies the following conditions (1) or (2):

(i)

$$NN' = (r - \lambda_1)(I_m \otimes I_n) + (\lambda_1 - \lambda_2)(I_m \otimes J_n) + \lambda_2 (J_m \otimes J_n). \tag{1}$$

Let R_i and R_j be any two rows of blocks of N. Then from (1), their inner product is

$$R_i \bullet R_j = \begin{cases} rI_n + \lambda_1 (J - I)_n, & i = j \\ \lambda_2 J_n, & i \neq j \end{cases}$$
$$= \begin{cases} (r - \lambda_1) I_n + \lambda_1 J_n, & i = j, \\ \lambda_2 J_n, & i \neq j. \end{cases}$$

(ii)

$$NN' = (r - \lambda_2)(I_n \otimes I_m) + \lambda_2 (J_n \otimes J_m) + (\lambda_1 - \lambda_2)\{(J_n - I_n) \otimes I_m\}. \tag{2}$$

Then (2)$\Rightarrow$

$$R_i \bullet R_j = \begin{cases} rI_m + \lambda_2 (J - I)_m, & i = j, \\ \lambda_1 I_m + \lambda_2 (J - I)_m, & i \neq j, \end{cases}$$
$$= \begin{cases} (r - \lambda_2) I_m + \lambda_2 J_m, & i = j, \\ (\lambda_1 - \lambda_2) I_m + \lambda_2 J_m, & i \neq j. \end{cases}$$

Then N represents a GD design with parameters: $v = mn, r, k, b, \lambda_1, \lambda_2, m, n$. For GD schemes, we refer to Saurabh [14]. A GD design will be called STD(n) or STD(m) with orthogonal rows if its incidence matrix satisfies the conditions (1) or (2) respectively.

1.3. $(\mu_1, \mu_2, \ldots, \mu_t)$ *−resolvable design*

Let the incidence matrix N of a block design $D(v,\ r,\ k,\ b)$ may be decomposed into submatrices as $N = (N_1 \mid N_2 \mid \cdots \mid N_t)$ such that each row sum of $N_i\,(1 \le i \le t)$ is μ_i. Then the design is $(\mu_1, \mu_2, \ldots, \mu_t)-$resolvable [see Kageyama [8], Saurabh [13]]. If $\mu_1 = \mu_2 = \cdots = \mu_t = \mu$ then the design is $\mu-$resolvable. Such designs are also denoted as $A-$resolvable designs in combinatorial design theory [see Ge and Miao [7]]. A practical application of $(\mu_1, \mu_2, \ldots, \mu_t)-$resolvable designs may be found in Kageyama [8]. These designs may also have potential applications in coding theory and cryptography.

1.4. *Cyclic and partial cyclic designs*

A block design $D(v,b,r,k)$ is cyclic if its solution may be obtained by adding the elements of a cyclic group $Z_v = \{0,1,2,\dots,v\}$ $mod v$ to the initial blocks of the design whereas a design is partial cyclic if its solution may be obtained by developing the initial blocks under a partial cycle: $1 \longleftrightarrow q, q+1 \longleftrightarrow 2q, \ \dots, [q(p-1)+1] \longleftrightarrow v = pq$ of length q where $(1 \leftrightarrow q) \iff 1 \to 2, \ 2 \to 3, \ \dots, (q-1) \to q, \ q \to 1$ [see Saurabh [12]].

Some constructions of partial cyclic GD designs can be found in Dey and Nigam [6], Mukerjee *et al.* [10], Dey and Balasubramanian [5], Midha and Dey [9], among others.

Example 1.1. A partial cyclic solution the GD design $R80 : v = 14, \ r = 9, k = 3, b = 42, \lambda_1 = 6, \lambda_2 = 1, m = 7, n = 2$ may be obtained by developing the initial blocks: (1, 2, 8) ; (1, 8, 9) ; (1, 3, 8) ; (1, 8, 10) ; (1, 4, 8) ; (1, 8, 11) under a partial cycle $1 \longleftrightarrow 7, 8 \longleftrightarrow 14$ of length 7 [see Clatworthy [4]].

Notation 1.2. I_n is the identity matrix of order n, $J_{v\times b}$ is the $v\times b$ matrix all of whose entries are 1 and $J_{v\times v} = J_v$, A' is the transpose of matrix A, $A \otimes B$ is the Kronecker product of two matrices A and B, 0_n is a zero matrix of order $n \times n$ and a $(0,1)$ −matrix: $\alpha = circ\,(0\,1\,0\dots0)$ is a permutation circulant matrix of order m such that $\alpha^m = I_m$. RX numbers are from Clatworthy [4].

2. Tactical decomposable RGD designs

2.1. *From partial cyclic RGD designs*

Theorem 2.1. *There always exists a square tactical decomposition of a partial cyclic RGD design with parameters:* $v = mn, r, k, b, \lambda_1, \lambda_2, m, n$ *where* m *is length of the partial cycle.*

Proof. Let N be the incidence matrix of a RGD design D having partial cyclic solution of length m. Then the number of initial blocks is $t = b/m$. Our aim to decompose N as $N = [N_{ij}]_{i=1,2,\dots,n;\ j=1,2,\dots,t}$ where each N_{ij} is a square matrix of order m. Then corresponding to each initial block $B_i (1 \le i \le t)$ of D, we obtain i^{th}−column of blocks of N as follows:

Step I: Break the interval $[1, \ mn]$ in to n subintervals as: $[1, m], [m+1, 2m], \dots, [m(n-1)+1, mn]$ such that each subinterval contains m elements which is the length of partial cycle.

Step II: Let $\alpha = circ\,(0\,1\,0\dots0)$ be a permutation circulant matrix of order m. Then corresponding to initial block whose elements belong to above subintervals, we obtain following $m\times m$ block matrices:

$$N_{1i} = I_m + \alpha + \alpha^2 + \cdots + \alpha^{m-1},$$
$$N_{2i} = I_m + \alpha^{m+1} + \alpha^{m+2} + \cdots + \alpha^{2m-1}\,(modm) = I_m + \alpha + \alpha^2 + \cdots + \alpha^{m-1},$$
$$\vdots$$
$$N_{ni} = I_m + \alpha^{m(n-1)+1} + \alpha^{m(n-1)+2} + \cdots + \alpha^{mn-1}\,(modm) = I_m + \alpha + \alpha^2 + \cdots + \alpha^{m-1}.$$

Hence we obtain a STD (m) RGD design corresponding to its partial cyclic solution. □

2.2. *From self–complementary BIB design*

Theorem 2.2. *The existence of a self–complementary BIB design with parameters:* $v = 2k, r, \ k, \ b = 2r, \ \lambda$ *implies the existence of a 3–resolvable STD* (2) *RGD design with parameters:* $v^* = 4k, \ r^* =$

$3r,\ k^* = 3k,\ b^* = 4r,\ \lambda_1 = \lambda + 2r,\ \lambda_2 = 2r,\ m = 2,\ n = 2k.$

Proof. Let M be the incidence matrix of a self–complementary BIB design. Then replacing $0 \to I_2$ and $1 \to J_2$ in M, we obtain a $(0,\ 1)-$matrix N such that $NN' = r\,(I_{2k} \otimes I_2) + 2r\,(J_{2k} \otimes J_2) + \lambda \left\{(J-I)_{2k} \otimes I_2\right\}$. Also each column sum of N is $3k$. Hence N represents the incidence matrix of a STD (2) RGD design with above mentioned parameters.

Since the BIB design is self–complementary, we obtain $'r'$ pairs of columns C_i and C_j such that $C_i + C_j = J_{2k\times 1}$. Such columns will be called a pair of self–complementary columns. Further replacement of $0 \to I_2$ and $1 \to J_2$ in each pair of self–complementary columns yields $'r'$ resolution classes such that each element occurs exactly three times in every class. Hence the design is 3–resolvable. □

Example 2.3. Consider a self–complementary BIB design with parameters: $v = 4, r = 3,\ k = 2,\ b = 6,\ \lambda = 1$ whose incidence matrix is:

$$M = \left[\begin{array}{cc|cc|cc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right].$$

Then replacing in M, we obtain a STD (2) RGD design R164: $v = 8, r = 9, k = 6, b = 12, \lambda_1 = 7, \lambda_2 = 6, m = 2, n = 4$ with incidence matrix N as given below:

$$N = [N_1 \mid N_2 \mid N_3] = \left[\begin{array}{cc|cc|cc} J_2 & I_2 & J_2 & I_2 & I_2 & J_2 \\ J_2 & I_2 & I_2 & J_2 & J_2 & I_2 \\ I_2 & J_2 & J_2 & I_2 & J_2 & I_2 \\ I_2 & J_2 & I_2 & J_2 & I_2 & J_2 \end{array}\right].$$

Further since each row sum of N_1, N_2 and N_3 is 3, the design is $3-$resolvable.

3. Illustrative examples

Here, some RGD designs of Clatworthy [4] are identified as STD (m) using Theorem 2.1 where $\alpha = circ\ (0\ 1\ 0 \ldots 0)$ is a permutation circulant matrix of order m. The arrangement of $v = mn$ elements into $m \times n$ array for following RGD designs is as follows:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)\,m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)\,m+2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & 2m & 3m & \cdots & mn \end{array}$$

1) $R80 : v = 14, r = 9, k = 3, b = 42, \lambda_1 = 6, \lambda_2 = 1, m = 7, n = 2.$

Initial blocks are [(1, 2, 8), (1, 8, 9), (1, 3, 8), (1, 8, 10), (1, 4, 8), (1, 8, 11)] under the partial cycles $1 \to 7,\ 8 \to 14$ of length 7. Using Theorem 2.1, we have

$$N = [N_1 \mid N_2 \mid N_3] = \left[\begin{array}{cc|cc|cc} \alpha & \alpha+\alpha^2 & \alpha & \alpha+\alpha^3 & \alpha & \alpha+\alpha^4 \\ \alpha+\alpha^2 & \alpha & \alpha+\alpha^3 & \alpha & \alpha+\alpha^4 & \alpha \end{array}\right].$$

Then $NN' = 8\left(I_2 \otimes I_7\right) + \left(J_2 \otimes J_7\right) + 5\left\{\left(J_2 - I_2\right) \otimes I_7\right\}$. Hence N represents the incidence matrix of $R80$. Further since each row sum of N_1, N_2 and N_3 is 3, the design is 3−resolvable.

The initial blocks of the remaining RGD designs listed below may be found in Clatworthy [4].

2) $R89 : v = 18, r = 9, k = 3, b = 54, \lambda_1 = 2, \lambda_2 = 1, m = 9, n = 2$.

$$N = [N_1 \mid N_2] = \left[\begin{array}{cc|cccc} \alpha & \alpha + \alpha^3 & \alpha & \alpha & \alpha & \alpha + \alpha^2 + \alpha^5 \\ \alpha^7 + \alpha^8 & \alpha^3 & \alpha^2 + \alpha^4 & \alpha + \alpha^5 & I_7 + \alpha^6 & 0_7 \end{array}\right].$$

Since each row sum of N_1 and N_2 is 3 and 6 respectively, the design is $(3,\ 6)$ −resolvable.

3) $R115 : v = 15, r = 8, k = 4, b = 30, \lambda_1 = 6, \lambda_2 = 1, m = 5, n = 3$.

$$N = [N_1 \mid N_2] = \left[\begin{array}{ccc|ccc} \alpha + \alpha^2 & \alpha & \alpha & \alpha + \alpha^3 & \alpha & \alpha \\ \alpha & \alpha + \alpha^2 & \alpha & \alpha & \alpha + \alpha^3 & \alpha \\ \alpha & \alpha & \alpha + \alpha^2 & \alpha & \alpha & \alpha + \alpha^3 \end{array}\right].$$

Since each row sum of N_1 and N_2 is 4, the design is 4−resolvable.

4) $R128 : v = 26, r = 8, k = 4, b = 52, \lambda_1 = 0, \lambda_2 = 1, m = 13, n = 2$.

$$N = [N_1 \mid N_2] = \left[\begin{array}{cc|cc} \alpha^2 + \alpha^4 + \alpha^{10} & \alpha & \alpha^3 + \alpha^6 + \alpha^7 & \alpha \\ \alpha & \alpha^2 + \alpha^4 + \alpha^{10} & \alpha & \alpha^3 + \alpha^6 + \alpha^7 \end{array}\right].$$

Since each row sum of N_1 and N_2 is 4, the design is 4−resolvable.

5) $R132 : v = 30, r = 10, k = 4, b = 75, \lambda_1 = 2, \lambda_2 = 1, m = 15, n = 2$.

$$N = [N_1 \mid N_2 \mid N_3] = \left[\begin{array}{cc|cc|c} \alpha + \alpha^3 + I_{15} & \alpha^5 & \alpha + \alpha^5 + \alpha^{11} & \alpha^2 & \alpha + \alpha^9 \\ \alpha^5 & \alpha + \alpha^3 + I_{15} & \alpha^2 & \alpha + \alpha^5 + \alpha^{11} & \alpha + \alpha^9 \end{array}\right].$$

Since each row sum of N_1, N_2 and N_3 is 4, 4 and 2 respectively, the design is $(2,\ 4,\ 4)$ −resolvable.

6) $R152 : v = 20, r = 10, k = 5, b = 40, \lambda_1 = 8, \lambda_2 = 1, m = 5, n = 4$.

$$N = [N_1 \mid N_2] = \left[\begin{array}{cccc|cccc} \alpha + \alpha^2 & \alpha & \alpha & \alpha & \alpha + \alpha^3 & \alpha & \alpha & \alpha \\ \alpha & \alpha + \alpha^2 & \alpha & \alpha & \alpha & \alpha + \alpha^3 & \alpha & \alpha \\ \alpha & \alpha & \alpha + \alpha^2 & \alpha & \alpha & \alpha & \alpha + \alpha^3 & \alpha \\ \alpha & \alpha & \alpha & \alpha + \alpha^2 & \alpha & \alpha & \alpha & \alpha + \alpha^3 \end{array}\right].$$

Since each row sum of N_1 and N_2 is 5, the design is 5−resolvable.

7) $R159 : v = 35, r = 10, k = 5, b = 70, \lambda_1 = 2, \lambda_2 = 1, m = 5, n = 7$.

$$N = [N_1 \mid N_2] = \left[circ\ \left(0_5, 0_5, 0_5,\ \alpha, \alpha, \alpha, \alpha^2 + I_5 \;\middle|\; circ\ (0_5, 0_5, 0_5,\ \alpha, \alpha, \alpha, \alpha^3 + \alpha^4\right)\right].$$

Since each row sum of N_1 and N_2 is 5, the design is 5−resolvable.

8) $R160 : v = 39, r = 10, k = 5, b = 78, \lambda_1 = 2, \lambda_2 = 1, m = 13, n = 3$.

$$N = [N_1 \mid N_2]$$
$$= \left[\begin{array}{ccc|ccc} \alpha^2 + \alpha^4 + \alpha^{10} & \alpha & \alpha & \alpha^3 + \alpha^6 + \alpha^7 & \alpha & \alpha \\ \alpha & \alpha^2 + \alpha^4 + \alpha^{10} & \alpha & \alpha & \alpha^3 + \alpha^6 + \alpha^7 & \alpha \\ \alpha & \alpha & \alpha^2 + \alpha^4 + \alpha^{10} & \alpha & \alpha & \alpha^3 + \alpha^6 + \alpha^7 \end{array}\right].$$

Since each row sum of N_1 and N_2 is 5, the design is 5−resolvable.

9) $R189: v=b=24, r=k=8,\ \lambda_1=4, \lambda_2=2, m=4, n=6.$

$$N=\left[I_6\otimes\left(\alpha^2+\alpha^3+I_4\right)+(J-I)_6\otimes\alpha\right].$$

10) $R200: v=b=28, r=k=9,\ \lambda_1=5, \lambda_2=2, m=4, n=7.$

$$N=\left[I_7\otimes\left(\alpha^2+\alpha^3+I_4\right)+(J-I)_7\otimes\alpha\right].$$

11) $R208: v=b=32, r=k=10,\ \lambda_1=6, \lambda_2=2, m=4, n=8.$

$$N=\left[I_8\otimes\left(\alpha^2+\alpha^3+I_4\right)+(J-I)_8\otimes\alpha\right].$$

4. Application in $(2,\ n)$ −threshold schemes

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 $(t,\ n)$ −threshold scheme is a secret sharing scheme in which if any $t(\leq n)$ or more participants pool their shares, where $n=|P|$, then they can reconstruct the secret key $K\in\mathcal{K}$, but any $n-1$ 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 $n=3$, $t=2$, op. cit. Stinson and Vanstone [21], Stinson [20].

Pieprzyk and Zhang [11] obtained ideal $(t,\ w)$ −threshold schemes from $b^t\times(n+1)$ orthogonal array $OA\ (b^t,\ n+1,\ b,\ t)$ by considering $OA\ (i,j)$ as the shares of participants P_j $(1\leq j\leq n)$ and $OA\ (i,0)$ as a secret key $(1\leq i\leq b^t)$ where $OA\ (i,j)$ denotes the entry in the i^{th} row and j^{th} column of $OA\ (b^t,\ n+1,\ b,\ t)$. Stinson and Vanstone [21] obtained perfect threshold schemes from Steiner system $S(t,\ w,\ v)$. Adachi and Lu [1] constructed $(3,\ 3)$ −threshold schemes from magic cubes by considering magic cube as a secret key and the corresponding three cubes as the shadows.

Some recent constructions of perfect secret sharing schemes from doubly resolvable GD designs and orthogonal resolutions of certain combinatorial designs can be found in Saurabh and Sinha [15, 18]. A recent survey on threshold schemes from combinatorial designs may be found in Bose [3].

Present scheme: Consider a STD (m) RGD design whose each submatrix is of size m. Then there are n rows of blocks in its incidence matrix N. The dealer provides rows $R_i(1\leq i\leq n)$ of blocks of N to n participants as their shares. Two participants can reveal the secret if their shares R_i and R_j are orthogonal rows of the STD (m) RGD design, i.e.,

$$R_i\bullet R_j=\begin{cases}rI_m+\lambda_2(J-I)_m, & i=j,\\ \lambda_1I_m+\lambda_2(J-I)_m, & i\neq j,\end{cases}$$
$$=\begin{cases}(r-\lambda_2)I_m+\lambda_2J_m, & i=j,\\ (\lambda_1-\lambda_2)I_m+\lambda_2J_m, & i\neq j.\end{cases}$$

Hence corresponding to a STD (m) RGD design, we obtain a $(2,\ n)$ −threshold scheme.

Further using Theorems 2.1 and 2.2, we obtain:

Scheme: The tactical decomposable RGD designs in Theorem 2.1 correspond to $(2,\ n)$ −threshold schemes whereas the designs of Theorem 2.2 correspond to $(2,\ 2k)$ − threshold schemes.

Example 4.1. The STD (4) RGD design R200 given in Section 3 can be used to obtain a (2, 7) − threshold scheme.

References

[1] T. Adachi and X.-N. Lu. Magic cubes and secret sharing schemes (algebras, logics, languages and related areas). *Proceedings of the Research Institute for Mathematical Sciences*, 2096:115–118, 2018.

[2] H. Bekar, C. Mitchell, and F. Piper. Tactical decomposition of designs. *Aequationes Mathematicae*, 25:123–152, 1982.

[3] M. Bose. Some combinatorial structures and their applications in cryptography. *Statistics and Applications*, 22(3):227–242, 2024.

[4] W. H. Clatworthy. *Tables of Two-Associate-Class Partially Balanced Designs*, volume 63. US National Bureau of Standards, 1948.

[5] A. Dey and K. Balasubramanian. Construction of some families of group divisible designs. *Utilitas Mathematica*, 40:283–290, 1991.

[6] A. Dey and A. Nigam. Construction of group divisible designs. *Journal of the Indian Society of Agricultural Statistics*, 37:163–166, 1985.

[7] G. Ge and Y. Miao. Pbds, frames, and resolvability. In *Handbook of Combinatorial Designs*, pages 287–291. Chapman and Hall/CRC, 2006.

[8] S. Kageyama. Resolvability of block designs. *The Annals of Statistics*:655–661, 1976.

[9] C. K. Midha and A. Dey. Cyclic group divisible designs. *Calcutta Statistical Association Bulletin*, 45(3-4):253–258, 1995. https://doi.org/10.1177/0008068319950311.

[10] R. Mukerjee, M. Jimbo, and S. Kageyama. On cyclic semiregular group divisible designs. *Osaka Journal of Mathematics*, 24:395–407, 1987.

[11] J. Pieprzyk and X.-M. Zhang. Ideal threshold schemes from orthogonal arrays. In *Information and Communications Security: 4th International Conference, ICICS 2002 Singapore, December 9–12, 2002 Proceedings 4*, pages 469–479. Springer, 2002. https://doi.org/10.1007/3-540-36159-6_40.

[12] S. Saurabh. A note on cyclic and partial cyclic solutions of block designs. *Gujrat Journal of Statistics and Data Science*, 40:45–50, 2024.

[13] S. Saurabh. Resolvability of a bib design of takeuchi (1962). *Statistics and Applications*, 22(2):361–362, 2024.

[14] S. Saurabh. Some matrix constructions of non-symmetric regular group divisible designs. *Bulletin of the ICA*, 102:129–146, 2024.

[15] S. Saurabh and K. Sinha. Perfect secret sharing schemes from combinatorial squares. *Security and Privacy*, 5(6):e262, 2022. https://doi.org/10.1002/spy2.262.

[16] S. Saurabh and K. Sinha. Some matrix constructions of l2-type latin square designs. *Bulletin of the ICA*, 95:93–104, 2022.

[17] S. Saurabh and K. Sinha. Matrix approaches to constructions of group divisible designs. *Bulletin of the ICA*, 97:83–105, 2023.

[18] S. Saurabh, K. Sinha, et al. $(2, w)$-threshold schemes constructed from orthogonal resolutions. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 120:231–239, 2024. https://doi.org/10.61091/jcmcc120-20.

[19] M. K. Singh and S. Saurabh. On certain classes of rectangular designs. *Calcutta Statistical Association Bulletin*, 75(1):72–96, 2023. https://doi.org/10.1177/00080683231162746.

[20] D. R. Stinson. *Cryptography: Theory and Practice*. Chapman and Hall/CRC, 2005.

[21] D. R. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. *SIAM Journal on Discrete Mathematics*, 1(2):230–236, 1988. https://doi.org/10.1137/0401024.