UTILITAS MATHEMATICA 128 (2026) 441–456

Utilitas Mathematica
www.combinatorialpress.com/um

Combinatorial Press

Some combinatorial applications of tactical decomposable rectangular designs families

Shyam Saurabh*

ABSTRACT

A brief survey on tactical decomposable families of rectangular designs (RDs) is presented. Rectangular designs have well–known applications in statistics. Here, applications of RDs in cryptography and coding theory are described. Earlier, $(2,\ n)-$threshold schemes were proposed from tactical decomposable regular group divisible designs. Threshold schemes are proposed here from tactical decomposable RDs. Further, an application of RDs in low–density parity–check (LDPC) codes is also given. Tactical decomposable RDs had not been previously used in the constructions of threshold schemes and LDPC codes.

Keywords: rectangular design, skew−Hadamard design, tactical decomposable design, threshold scheme, LDPC code, doubly resolvable design

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

1. Introduction and contributions

A brief survey on tactical decomposable rectangular designs (RDs) families is presented and their applications in cryptography and coding theory are also described. Earlier, Saurabh [20] proposed $(2,\ n)-$threshold schemes from tactical decomposable regular group divisible designs. Threshold schemes are obtained here from tactical decomposable RDs.

Previously low–density parity–check (LDPC) codes from group divisible designs had been studied by Shan and Li [28], Xu et al. [39] and Saurabh and Sinha [24], among others. Here, an application of RDs in low–density parity–check (LDPC) codes is also given. A brief survey on the constructions of LDPC codes based on certain combinatorial structures is available in Saurabh and Sinha [27].

* Corresponding author.

Received 19 Jun 2026; Revised 10 Aug 2026; Accepted 13 Aug 2026; Published Online 29 Aug 2026.
DOI: 10.61091/um128-21

The paper is organized as follows: Section 1 contains introduction and contributions, Section 2 contains some preliminaries on rectangular designs and their applications in statistics, Section 3 contains some previously obtained tactical decomposable RDs families, applications of RDs in threshold schemes and LDPC codes are described in Sections 4 and 5 respectively, whereas discussion and conclusion are given in Section 6.

The theorems related to tactical decomposable RDs families given in Section 3, are taken from earlier sources. Such families of designs are applied here in threshold schemes and LDPC code constructions. Tactical decomposable RDs had not been previously used in the constructions of threshold schemes and LDPC codes.

Notations: 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^T is the transpose of matrix A, $A \otimes B$ is the Kronecker product of two matrices A and B and $\alpha = circ\ (0\ 1\ 0 \ldots 0)$ is a permutation circulant matrix of order q such that $\alpha^q = I_q$. $EA\,(p^n) = C_p \times C_p \times \cdots \times C_p$ (n copies) denotes the elementary abelian group $EA\ (q)$ of order $q = p^n$ and $C_p = \{1,\ \alpha,\ \alpha^2, \ldots, \alpha^{p-1}\}$ is a cyclic group of order p where p is a prime.

Some relevant definitions related to the paper are as follows:

Definition 1.1 (Dual design)**.** The dual of a design $D\ (v,\ b,\ r,\ k)$ is a design $D^{'}(b,\ v,\ k,\ r)$ whose elements are the blocks of the design D and whose blocks are the elements of the design D. If N is the incidence matrix of a design D then N^T is the incidence matrix of design $D^{'}$, see Clatworthy [7].

Definition 1.2 (Balanced incomplete block design)**.** A balanced incomplete block (BIB) design/a $2-(v,k,\lambda)$ design is an arrangement of v elements into b blocks such that

(i) Every block contains $k(< v)$ distinct elements;

(ii) Every element is replicated r times and any pair of distinct elements occurs together in exactly λ blocks.

The integers: v, b, r, k, λ are known as parameters of the BIB design and they satisfy the relations:

$$bk = vr, r(k-1) = \lambda(v-1), b = \frac{\lambda v(v-1)}{k(k-1)}.$$

Definition 1.3 (Skew–Hadamard design)**.** A $(1,-1)-$matrix H of order $4t$ is called a skew–Hadamard matrix if $HH^T = 4tI_{4t}$ and $H - I_{4t}$ is a skew–symmetric matrix. A skew–Hadamard matrix is in normalized form if its first row as well as first column contains entirely 1's. For details, we refer to Wallis et al. [37] and Koukouvinos and Stylianou [14].

The matrix of order $4t-1$ obtained by deleting 1^{st} row and 1^{st} column of a normalized skew–Hadamard matrix H is called the core C of H. Then $N = \frac{(C+J_{4t-1})}{2}$ is the incidence matrix of a skew–Hadamard $(4t-1, 2t-1, t-1)-$design and N satisfies the following relations:

(i) $N + N^T = (J-I)_{4t-1}, NN^T = N^TN = (2t-1)I_{4t-1} + (t-1)(J-I)_{4t-1}$;

(ii)$N^2 + N = \left(N^T\right)^2 + N^T = t(J-I)_{4t-1},\ N^2 + \left(N^T\right)^2 = (2t-1)(J-I)_{4t-1}$.

Example 1.4. $N = circ.\ (0\ 1\ 1\ 0\ 1\ 0\ 0)$ is the incidence matrix of a skew–Hadamard $(7,\ 3,\ 1)-$design.

Definition 1.5 (Generalized Hadamard matrix)**.** Let G be a multiplicative group of order g. Then a generalized Hadamard matrix $GH(\lambda g; G)$ is a $\lambda g \times \lambda g$ array with entries from G such that

(i) Each row and column contain exactly λg group elements (repeated or non–repeated) as entries;

(ii) For each pair of distinct rows (columns): $(x_1,\ x_2,\ \ldots,\ x_b)$ and $(y_1,\ y_2,\ \ldots,\ y_b)$, the multi–set $\{x_i y_i^{-1} : i = 1,\ 2,\ \ldots,\ b(= \lambda g)\}$ contains each group element exactly λ times.

A $GH(\lambda g; G)$ is in normalized form if its first row and column contain only identity element of G.

Example 1.6. $GH\,(6;\ C_3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & 1 \\ 1 & \alpha^2 & \alpha & \alpha & 1 & \alpha^2 \\ 1 & \alpha^2 & \alpha^2 & 1 & \alpha & \alpha \\ 1 & 1 & \alpha & \alpha^2 & \alpha^2 & \alpha \\ 1 & \alpha & 1 & \alpha^2 & \alpha & \alpha^2 \end{pmatrix}$ over a cyclic group $C_3 = \{1,\ \alpha,\ \alpha^2\}$.

2. Preliminaries on rectangular designs

Let $v = mn$ elements be arranged in an $m \times n$ array A. A rectangular design (RD), introduced by Vartak [36], 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 exactly r blocks;
3. Every pair of elements, which are in the same row of the array A occur together in λ_1 blocks; which are in same column occur together in λ_2 blocks; while every other pair of elements occur together in λ_3 blocks. The elements in the same row are first associates, the elements in the same column are second associates and the elements not in the same row or column are third associates.

The non–negative integers $v = mn, r, k, b, \lambda_1, \lambda_2, \lambda_3, m, n$ are known as parameters of the RD and they satisfy the relations: $bk = vr; (n-1)\lambda_1 + (m-1)\lambda_2 + (n-1)(m-1)\lambda_3 = r(k-1)$.

The $m \times n$ array A is given as:

$$\begin{matrix} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (m-1)n+1 & (m-1)n+2 & (m-1)n+3 & \cdots & mn \end{matrix}.$$

Further, let N be $v \times b$ $(0,\ 1)-$incidence matrix of a block design which satisfies the

following conditions:

(i) $J_v N = kJ_{v\times b}$, which confirms that each column sum of N is k;

(ii) $NN^T = \begin{pmatrix} P & Q & \cdots & Q \\ Q & P & \cdots & Q \\ \vdots & \vdots & \vdots & \vdots \\ Q & Q & \cdots & P \end{pmatrix}$, where $P = (r-\lambda_1)\, I_n + \lambda_1 J_n$ and $Q = (\lambda_2 - \lambda_3)\, I_n + \lambda_3 J_n = r\,(I_m \otimes I_n) + \lambda_1\,(I_m \otimes I_n^c) + \lambda_2\,(I_m^c \otimes I_n) + \lambda_3\,(I_m^c \otimes I_n^c)\,;\ I_n^c = (J-I)_n$.

Alternatively, let R_i and R_j be any two rows of blocks of N. Then the inner product of rows is

$$R_i R_j^T = \begin{cases} rI_n + \lambda_1 (J-I)_n; i = j \\ \lambda_2 I_n + \lambda_3 (J-I)_n; i \neq j \end{cases} = \begin{cases} (r-\lambda_1) I_n + \lambda_1 J_n; i = j, \\ (\lambda_2 - \lambda_3) I_n + \lambda_3 J_n; i \neq j. \end{cases} \tag{1}$$

Then N represents an RD with parameters: $v = mn, r, k, b, \lambda_1, \lambda_2, \lambda_3, m, n$. The RD will be called STD(n) with orthogonal rows if its incidence matrix satisfies the condition (1). Clearly a STD(n) RD with $v = mn$ elements has $\frac{m(m-1)}{2}$ pairs of orthogonal rows. Group divisible designs and L_2 designs are special cases of RDs [30].

Further, let N be the incidence matrix of an RD with parameters: $v, r, k, b, \lambda_1, \lambda_2, \lambda_3, m, n$. Then four distinct eigenvalues of NN^T are given as:

$\theta_0 = rk, \theta_1 = r - \lambda_1 + (m-1)\,(\lambda_2 - \lambda_3)\,, \theta_2 = r - \lambda_2 + (n-1)(\lambda_1 - \lambda_3), \theta_3 = r - \lambda_1 - \lambda_2 + \lambda_3$ with respective multiplicities: $1, n-1, m-1,\ (m-1)(n-1)$.

A classification of RDs based on the eigenvalues of NN^T is given in Singh and Saurabh [30]. The complementary design of an RD with parameters: $v = mn, r, k, b, \lambda_1, \lambda_2, \lambda_3, m, n$ is again an RD with parameters: $v^* = mn, r^* = b - r, k^* = v - k, b^* = b, {\lambda_1}^* = b - 2r + \lambda_1$, ${\lambda_2}^* = b - 2r + \lambda_2, {\lambda_3}^* = b - 2r + \lambda_3, m, n$.

A recent survey on RDs are available in Singh and Saurabh [30]. Some series of cyclic RDs are obtained by Sinha et al. [31] and Saurabh [21], among others. RDs are useful as factorial experiments, having balance as well as orthogonality, see Gupta and Mukerjee [11]. In addition, RDs having $\lambda_3 > \lambda_1, \lambda_2$ when used as the $m \times n$ complete confounded experiments, the loss of information on the main effects is small, see Suen [34]. An application of RD in cluster sampling is described in Raghavarao and Singh [17]. RDs are also applicable in agricultural field trials.

3. Tactical decomposable rectangular designs families

Let a (0, 1) – matrix N have a decomposition $N = [N_{ij}]_{\substack{i=1,2,\ldots,s \\ j=1,2,\ldots,t}}$ 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, 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 $n \times n$ matrix, D is called square tactical decomposable design, STD (n).

Several methods of constructions of tactical decomposable rectangular, group divisible

and L_2 designs are available in Bekar et al. [4], Singh and Saurabh [30], Saurabh and Sinha [23, 25] and Saurabh [18, 20, 19], among others. Recently, STD (n) RDs have been extensively studied by Singh and Saurabh [30]. Here, some series are given to illustrate their applications in threshold schemes and LDPC codes constructions. Theorems (1–5) are taken from Singh and Saurabh [30].

Theorem 3.1. *The existence of symmetric* $2-(n,k_i,\lambda_i)$ *designs* $(i=1,2)$*, whose incidence matrices* $N_i, i=1,2$ *satisfy the relation:* $N_1N_2^{'}+N_2N_1^{'}=\mu_1 I_n+\mu_2(J-I)_n$*, implies the existence of a STD* (n) *RD with parameters:*

$$\left.\begin{array}{r} v=b=mn, r=k=k_1+(m-1)k_2, \lambda_1^{'}=\lambda_1+(m-1)\lambda_2, \\ \lambda_2^{'}=(m-2)k_2+\mu_1, \lambda_3^{'}=(m-2)\lambda_2+\mu_2, m, n. \end{array}\right\} \tag{2}$$

Proof. Consider a block matrix: $N=I_m\otimes N_1+I_m^c\otimes N_2$, where $I_m^c=(J-I)_m$, N_1 and N_2 are same as defined above. Then we have

(i) $J_{mn}N=\{k_1+(m-1)k_2\}J_{mn}$;

(ii) $NN^T=r\,(I_m\otimes I_n)+\lambda_1^{'}\,(I_m\otimes I_n^c)+\lambda_2^{'}\,(I_m^c\otimes I_n)+\lambda_3^{'}\,(I_m^c\otimes I_n^c)$, where

$r=k_1+(m-1)k_2,\ \lambda_1^{'}=\lambda_1+(m-1)\lambda_2, \lambda_2^{'}=(m-2)k_2+\mu_1, \lambda_3^{'}=(m-2)\lambda_2+\mu_2.$

Hence, N represents an RD with above mentioned parameters (2). □

For Corollaries 3.2–3.4 of RDs obtained from Theorem 3.1, N_{4t-1} denotes the incidence matrix of a Skew–Hadamard $(4t-1, 2t-1, t-1)$–design.

Corollary 3.2. *For* $N_1=N_{4t-1}, N_2=I_{4t-1}$*, we get a series of STD* $(4t-1)$ *RDs with parameters:*

$$v=b=m(4t-1), r=k=m+2t-2, \lambda_1=t-1, \lambda_2=m-2, \lambda_3=1, m, n=4t-1. \tag{3}$$

Proof. For $N_1=N_{4t-1}, N_2=I_{4t-1}$, we have $N_1N_2^T+N_2N_1^T=I_{4t-1}^c$. Hence, $N=I_m\otimes N_1+I_m^c\otimes N_2$ represents an RD with above mentioned parameters (3). □

Example 3.3. For $t=2$, we have $N_1=circ.\ (0\ 1\ 1\ 0\ 1\ 0\ 0), N_2=I_7$. Consider the block matrix

$$N=\begin{pmatrix} N_1 & I_7 & I_7 & I_7 \\ I_7 & N_1 & I_7 & I_7 \\ I_7 & I_7 & N_1 & I_7 \\ I_7 & I_7 & I_7 & N_1 \end{pmatrix}.$$

Then N represents a STD (7) RD with parameters: $v=b=28, r=k=6, \lambda_1=1, \lambda_2=2, \lambda_3=1, m=4, n=7$, which reduces to a group divisible design.

Corollary 3.4. *For* $N_1=I_{4t-1}+N_{4t-1}, N_2=I_{4t-1}$*, we get a series of STD* $(4t-1)$ *RDs with parameters:*

$$v=b=m(4t-1), r=k=m+2t-1, \lambda_1=t, \lambda_2=m, \lambda_3=1, m, n=4t-1. \tag{4}$$

Proof. For $N_1 = I_{4t-1}+N_{4t-1}, N_2 = I_{4t-1}$, we have $N_1N_2^T+N_2N_1^T = 2I_{4t-1}+I_{4t-1}^c$. Hence, $N = I_m \otimes N_1 + I_m^c \otimes N_2$ represents an RD with above mentioned parameters (4). □

Example 3.5. For $t = 2$, we have $N_1 = circ.\ (0\ 1\ 1\ 0\ 1\ 0\ 0), N_2 = I_7$. Consider the block matrix

$$N = \begin{pmatrix} I_7 + N_1 & I_7 & I_7 \\ I_7 & I_7 + N_1 & I_7 \\ I_7 & I_7 & I_7 + N_1 \end{pmatrix}.$$

Then N represents a STD (7) RD with parameters: $v = b = 21, r = k = 6, \lambda_1 = 2, \lambda_2 = 3, \lambda_3 = 1, m = 3, n = 7$.

The proof of following Theorem 3.6 using mutually orthogonal Latin squares (MOLSs) are described in Singh and Saurabh [30]:

Theorem 3.6. *Let q be a prime or prime power. Then there exist STD (q) RDs with parameters:*

$$\left.\begin{array}{r} v = b = q^2 - q, r = k = (q-1)^2, \lambda_1 = \lambda_2 = (q-1)(q-2), \\ \lambda_3 = (q-1)(q-2)+1, m = q-1, n = q. \end{array}\right\} \quad (5)$$

Theorem 3.7. *Let q be a prime or prime power. Then there exists a STD (q) RD with parameters:*

$$v = q^2, b = q(q-1), r = q-1, k = q, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 1, m = n = q. \quad (6)$$

Proof. It is well known that a $GH\ (q,\ EA\ (q))$ always exists, where $EA\ (q)$ is an elementary abelian group of order q, see Launey [8]. We obtain a $q \times (q-1)$ matrix M obtained by deleting first column of $GH\ (q,\ EA\ (q))$ in the normalized form.

Further, let N be a $q^2 \times q(q-1)$ matrix obtained from replacing the group elements of M by corresponding permutation matrices. Then using properties of permutation matrices, we have

(i) $J_{q^2}N = qJ_{q^2 \times q(q-1)}$;

(ii) $NN^T = (q-1)\,(I_q \otimes I_q) + \left(I_q^c \otimes I_q^c\right)$, where $I_q^c = (J-I)_q$.

Hence, N represents an RD with above mentioned parameters (6). □

Further, removing any $t(> 1)$ rows of blocks of the incidence matrix of RD with parameters (6), we obtain:

Corollary 3.8. *Let q be a prime or prime power. Then there exists a STD (q) RD with parameters:*

$$v = q(q-t), b = q(q-1), r = q-1, k = q-t, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 1, m = q-t, n = q. \quad (7)$$

Proof. Let $N = [N_{ij}]_{\substack{1 \le i \le q \\ 1 \le j \le (q-1)}}$ be the incidence matrix of the RD with parameters (6), where each N_{ij} is a permutation matrix of size $'q'$. Let M be a matrix obtained by removing $'t'$ rows of blocks of N. Since each column sum of N_{ij} is one, each column sum of the block matrix M is $q-t$ i. e.

$$J_{q^2-qt}M = (q-t)J_{(q^2-qt)\times q(q-1)}.$$

Clearly M also satisfies the condition (ii) as the same condition is preserved even after removing $'t'$ rows of blocks of N. Then we have

$MM^T = (q-1)\left(I_{q-t} \otimes I_q\right) + \left(I^c_{q-t} \otimes I^c_q\right)$, where $I^c_q = (J-I)_q$.

Hence, M represents an RD with above mentioned parameters (7). □

Remark 3.9. If q is a prime then the incidence matrix $'N'$ of the STD (q) RD of Theorem 3.7 is given as:

$$N = \begin{pmatrix} I_q & I_q & \cdots & I_q \\ \alpha & \alpha^2 & \cdots & \alpha^{q-1} \\ \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^{q-1})^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q-1} & (\alpha^2)^{q-1} & \cdots & (\alpha^{q-1})^{q-1} \end{pmatrix},$$

where $\alpha = circ\ (0\ 1 \ldots 0)$ *such that* $\alpha^q = I_q$ *and* $\alpha^i = circ\ (0\ 0 \ldots 0\ 1\ 0 \ldots 0)$ is a permutation circulant matrix of order q with 1 situated at $(i+1)-th$ position.

Example 3.10. For $q = 5$. the following block matrix represents an RD with parameters: $v = 25, b = 20, r = 4, k = 5, \lambda_1 = \lambda_2 = 0, \lambda_3 = 1, m = n = 5$, where $\alpha = circ\ (0\ 1\ 0\ 0\ 0)$ is a permutation circulant matrix of order 5.

$$N = \begin{pmatrix} I_5 & I_5 & I_5 & I_5 \\ \alpha & \alpha^2 & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^4 & \alpha & \alpha^3 \\ \alpha^3 & \alpha & \alpha^4 & \alpha^2 \\ \alpha^4 & \alpha^3 & \alpha^2 & \alpha \end{pmatrix}.$$

Further, removing any row of blocks of N, we obtain an RD with parameters: $v = b = 20, r = k = 4, \lambda_1 = \lambda_2 = 0, \lambda_3 = 1, m = 4,\ n = 5$.

Theorem 3.11. *There exists a STD* $(4t-1)$ *RD with parameters:*

$$v = b = 5(4t-1), r = k = 8t-3, \lambda_1 = 4(t-1), \lambda_2 = 2t-1, \lambda_3 = 3t-1, m = 5, n = 4t-1. \tag{8}$$

Proof. Let N be the incidence matrix of a skew−Hadamard $(4t-1,\ 2t-1,\ t-1)$−design.

Consider a block matrix:

$$M = \begin{pmatrix} I_{4t-1} & N & N & N^T & N^T \\ N & I_{4t-1} & N^T & N^T & N \\ N & N^T & I_{4t-1} & N & N^T \\ N^T & N^T & N & I_{4t-1} & N \\ N^T & N & N^T & N & I_{4t-1} \end{pmatrix}.$$

Then we have
(i) $J_{5(4t-1)}M = (8t-1)J_{5(4t-1)}$;
(ii) $NN^T = r\,(I_m \otimes I_n) + \lambda_1\,(I_m \otimes I_n^c) + \lambda_2\,(I_m^c \otimes I_n) + \lambda_3\,(I_m^c \otimes I_n^c)$, where

$$I_m^c = (J-I)_m, r = 8t-3,\ \lambda_1 = 4(t-1), \lambda_2 = 2t-1, \lambda_3 = 3t-1.$$

Hence, N represents an RD with above mentioned parameters (8). □

Example 3.12. For $t = 3$, $N = circ$ (0 1 0 1 0 1 0 1 0 1 0) represents a skew−Hadamard (11, 5, 2)− design. Hence, we obtain a STD (11) RD with parameters: $v = b = 55, r = k = 21, \lambda_1 = 8, \lambda_2 = 5, \lambda_3 = 8, m = 5, n = 11$.

Corollary 3.13. *The complement of* $M : M^c = J_{5(4t-1)} - M$ *represents a STD* $(4t-1)$ *RD with parameters* $v = 5(4t-1), k = 2(6t-1), \lambda_1 = 8t-3, \lambda_2 = 6t, \lambda_3 = 7t, m = 5, n = 4t-1$.

Theorem 3.14. *Let* q *be a prime or prime power. Then there exists a STD* (q) *RD with parameters:*

$$v = q^2 - q, k = 2(q-1), \lambda_1 = 2, \lambda_2 = q-1, \lambda_3 = 3, m = q-1, n = q. \tag{9}$$

The proof of Theorem 3.14 is based on MOLSs. Some series of tactical decomposable RD families in which all internal block matrices are not square are given below:

Theorem 3.15. *[Sinha et al. [31], Th. 2.5] The existence of a BIB design with parameters:* v', b', r', k', λ' *implies the existence of an RD with parameters:*

$$\begin{cases} v = 2v', b = 2\left(b' - r'\right), r = b' - r', k = v', \lambda_1 = 0, \\ \lambda_2 = b' - 2r' + \lambda', \lambda_3 = r' - \lambda', m = v', n = 2. \end{cases} \tag{10}$$

Proof. Let N be the $v' \times b'$ incidence matrix of a BIB design with parameters: v', b', r', k', λ'.
Consider the following block matrix:

$$M = \begin{pmatrix} N & J_{v' \times \left(b' - 2r'\right)} \\ J_{v' \times b'} - N & O_{v' \times \left(b' - 2r'\right)} \end{pmatrix},$$

where $O_{v' \times \left(b' - 2r'\right)}$ is a null matrix of order $v' \times \left(b' - 2r'\right)$. Then we have
(i) $J_{2v'}N = v' J_{2v' \times 2\left(b' - r'\right)}$;

(ii) $NN^T = (b^{'} - r^{'})\ (I_{v^{'}} \otimes I_2) + (b^{'} - 2r^{'} + \lambda^{'}) \left(I^c_{v^{'}} \otimes I_2\right) + (r^{'} - \lambda^{'}) \left(I^c_{v^{'}} \otimes I^c_2\right)$; $I^c_m = (J - I)_m$.

Hence, M represents an RD with above mentioned parameters (10). □

Theorem 3.16. *[Sinha and Kageyama [13], Th. 2.3] The existence of a BIB design with parameters: $v^{'} = m, b^{'}, r^{'}, k^{'}, \lambda^{'}$ implies the existence of an RD with parameters:*

$$\begin{cases} v = mn, b = nb^{'}, r = (n-1)r^{'} + b^{'}, k = (n-1)k^{'} + v^{'}, \\ \lambda_1 = nr^{'}, \lambda_2 = (n-1)\lambda^{'} + b^{'}, \lambda_3 = (n-2)\lambda^{'} + 2r^{'}. \end{cases} \tag{11}$$

Proof. Let N be the $m \times b^{'}$ incidence matrix of a BIB design with parameters: $v^{'} = m, b^{'}, r^{'}, k^{'}, \lambda^{'}$. Consider the following block matrix: $M = (J - I)_n \otimes N + I_n \otimes J_{m \times b^{'}}$.

Then we have

(i) $J_{mn}N = \{(n-1)k^{'} + v^{'}\}J_{mn \times nb^{'}}$;

(ii) $NN^T = \{(n-1)r^{'} + b^{'})\}\,(I_m \otimes I_n) + \lambda_1\,(I_m \otimes I^c_n) + \lambda_2\,(I^c_m \otimes I_n) + \lambda_3\,(I^c_m \otimes I^c_n)$; $I^c_m = (J - I)_m$, where $\lambda_1 = nr^{'}, \lambda_2 = (n-1)\lambda^{'} + b^{'}, \lambda_3 = (n-2)\lambda^{'} + 2r^{'}$.

Hence, M represents an RD with above mentioned parameters (11). □

Theorem 3.17. *[Sinha and Kageyama [13], Th. 2.4] The existence of a BIB design with parameters: $v^{'} = m, b^{'}, r^{'}, k^{'}, \lambda^{'}$ implies the existence of an RD with parameters:*

$$\begin{cases} v = mn, b = nb^{'}, r = (n-2)r^{'} + b^{'}, k = (n-2)k^{'} + v^{'}, \\ \lambda_1 = (n-2)r^{'}, \lambda_2 = b^{'} - 2r^{'} + n\lambda^{'}, \lambda_3 = (n-4)\lambda^{'} + 2r^{'}. \end{cases} \tag{12}$$

Proof. Let N be the $m \times b^{'}$ incidence matrix of a BIB design with parameters: $v^{'} = m, b^{'}, r^{'}, k^{'}, \lambda^{'}$. Consider the following block matrix: $M = (J - I)_n \otimes N + I_n \otimes (J_{m \times b^{'}} - N)$.

Then we have

(i) $J_{mn}N = \{(n-1)k^{'} + v^{'}\}J_{mn \times nb^{'}}$;

(ii) $NN^T = \{(n-2)r^{'} + b^{'})\}\,(I_m \otimes I_n) + \lambda_1\,(I_m \otimes I^c_n) + \lambda_2\,(I^c_m \otimes I_n) + \lambda_3\,(I^c_m \otimes I^c_n)$; $I^c_m = (J - I)_m$, where $\lambda_1 = (n-2)r^{'}, \lambda_2 = b^{'} - 2r^{'} + n\lambda^{'}, \lambda_3 = (n-4)\lambda^{'} + 2r^{'}$.

Hence, M represents an RD with above mentioned parameters (12). □

4. Threshold scheme: Construction and proof

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 $t-1$ 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 $n = 3$, $t = 2$, op. cit. Stinson and Vanstone [33], Stinson [32].

Pieprzyk and Zhang [16] 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 [33] 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 [22, 26]. A recent survey on threshold schemes from combinatorial designs may be found in Bose [6]. Recently Saurabh [20] obtained $(2,\ n)$−threshold schemes from tactical decomposable regular GD designs. The schemes used here are presented below:

Scheme 1. Consider a STD (n) matrix N whose each submatrix is of size n. Then there are m rows of blocks and $\frac{m(m-1)}{2}$ pairs of rows in N. The dealer provides arbitrary pair $(R_i, R_j)(1 \leq i \neq j \leq \frac{m(m-1)}{2})$ of rows to any two participants as their shares. Two participants can reveal the secret if their shares R_i and R_j are any arbitrary pair of orthogonal rows of the STD (n) RD design i. e.

$$R_i R_j^T = \begin{cases} rI_n + \lambda_1(J-I)_n; i = j \\ \lambda_2 I_n + \lambda_3(J-I)_n; i \neq j \end{cases} = \begin{cases} (r-\lambda_1)I_n + \lambda_1 J_n; i = j, \\ (\lambda_2 - \lambda_3)I_n + \lambda_3 J_n; i \neq j. \end{cases}$$

Hence, corresponding to a STD (n) RD, we obtain a $\left(2,\ \frac{m(m-1)}{2}\right)$ −threshold scheme. Proceeding similarly, a $\left(2,\ \frac{n(n-1)}{2}\right)$ −threshold scheme can also be obtained from STD (n) L_2 designs based on n elements. Some recent constructions of STD (n) L_2 designs are available in Saurabh and Sinha [23] and Saurabh [19]. Clearly, the tactical decomposable RDs families given in Section 3 correspond to $\left(2,\ \frac{m(m-1)}{2}\right)$ −threshold schemes.

Example 4.1. For $q = 27$ in Theorem 3.7 (see Section 3), we obtain a STD (27) RD with parameters: $v = b = 702, r = k = 676, \lambda_1 = \lambda_2 = 650, \lambda_3 = 651, m = 26, n = 27$.

Then the incidence matrix of STD (27) RD with above mentioned parameters contains 26 orthogonal rows of blocks which can be used to obtain a $(2,\ 325)$−threshold scheme.

Scheme 2. Consider an uniform column STD (n) matrix N whose each submatrix is of size n. Then there are m rows of blocks and ${}^mC_t = \frac{m!}{t!(m-t)!}$ 't−combinations' of rows in N.

Then N may be decomposed as: $N = [N_{ij}]_{1 \leq i,j \leq m}$, where each N_{ij} is of size n. Let each N_{ij} has constant column sum, say s i. e. $J_n N_{ij} = sJ_n$.

The dealer provides t−combinations of rows $R_i(1 \leq i \leq \frac{m!}{t!(m-t)!})$ of blocks of N to $'t'$

participants as their shares. Then $t(\leq m)$ participants can reveal the secret if their shares are arbitrarily chosen $'t'$ orthogonal rows of the uniform column STD (n) RD design and each column sum of shares of the participants is ts (constant) i. e. $\sum_{i=1}^{t} N_{ij} = ts$ $(1 \leq j \leq m)$. Hence, we obtain a $\left(t,\ \frac{m!}{t!(m-t)!}\right)$ $-$threshold scheme.

Example 4.2. For $q = 11$ in Theorem 3.7 (see Section 3), we obtain an uniform column STD (11) RD with parameters: $v = 121, b = 110, r = 10, k = 11, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 1, m = n = 11$. This design can be used to obtain a $(5,\ 462)-$threshold scheme for $t = s = 5$, where ${}^{11}_{5}C = 462$.

5. LDPC codes: Construction, proof and code rate

A binary $(m, n,\ \rho, \mu)-$regular low–density parity–check $(LDPC)$ *code* is the null space of an $m \times n$ $(m < n)$ sparse $(0,\ 1)$ parity–check matrix H over a Galois field $GF\ (2)$ of order 2 such that each row has μ nonzero elements and each column has ρ nonzero elements where $\mu \ll n$ and $\rho \ll m$, where m and n are the number of parity–check equations and code length respectively. LDPC codes are the codes specified by a matrix containing mostly 0's and relatively few 1's.

The minimum distance of a code is equal to the minimum number of nonzero columns in the parity–check matrix such that a nontrivial linear combination of these columns sums to zero over $GF\ (2)$, see Wicker [38, p. 84] and Johnson and Weller [12, p. 1416]. The code rate is given as $\frac{(n-rank(H))}{n}$ and the code dimension is $n-rank(H)$, where $rank(H)$ is calculated over $GF\ (2)$. Further, for a given a parity–check matrix: $H = (h_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$, an $n-$tuple $v = (v_1,\ v_2, v_3 \ldots, v_n)$ is a code word if and only if the value of the expression $T = \sum_{j=1}^{n} [h_{ij} v_j \mod 2]$, where $1 \leq i \leq m$, is the zero vector.

The LDPC code may also be represented by a *Tanner bipartite graph.* A *cycle* in a graph is a sequence of connected vertices with same initial and terminal vertex and no other vertex appears more than once. The number of edges is the length of the cycle and length of the smallest cycle is *girth* of a graph. Since the Tanner graph is bipartite, the length of a cycle must be even and at least four.

An LDPC code performs well with iterative decoding if the corresponding Tanner graph is free of short cycles, mainly four cycles. These short cycles limit the performance of iterative decoding. The iterative decoding becomes correlated after two iterations for these cycles. Hence, the four length cycles should be avoided in code construction, see Bonello et al. [5], Mostari and Ahmed [15], Alinejad and Khashyarmanesh [2] and Gholami and Nassaj [10].

A binary regular LDPC code is free of 4–cycles provided the inner product of any two distinct rows (or two distinct columns) of its parity–check matrix H is at most one which is known as a row–column (RC) constraint on H, see Diao et al. [9], Saurabh and Sinha [27]. This constraint confirms that the girth of the LDPC codes is at least six.

The following result is an extension of Lemma 5.1 of Saurabh and Sinha [24]:

Lemma 5.1. *The incidence matrix 'N' of an RD with parameters:* $v = mn, b, r, k, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 1, m, n$ *satisfies RC–constraint and the corresponding LDPC code is free of 4 – cycles.*

Proof. Consider an RD design with parameters:

$$v = mn, b, r, k, \lambda_1 = \lambda_2 = 0, \lambda_3 = 1. \tag{13}$$

Let B_i and B_j be any two distinct blocks of the RD with parameters (13). The condition $\lambda_1 = \lambda_2 = 0, \lambda_3 = 1$ confirms that any two elements occur in either one block or no block, we have $|B_i \cap B_j| \leq 1$. Hence any two distinct columns of the incidence matrix N have at most one nonzero element common.

Further since for an RD with parameters (13), every pair of elements is contained in at most one block, any two distinct rows of N have at most one nonzero element common. Thus N satisfies the RC– constraint. If we consider N as parity – check matrix then the corresponding LDPC code (or Tanner graph) is free of 4 –cycles. Also since N is the incidence matrix, its each column sum is k and each row sum is r. Hence the $(v,\ b,\ k,\ r)$–LDPC code is regular. □

Remark 5.2. Applying same logic to the dual of RD with parameters (13), it can be easily verified that N^T also satisfies RC–constraint.

Further, it should be noted that the number of columns in a parity–check matrix should be greater than the number of rows for positive code rate. Let N be same as defined in Lemma 5.1. Then N is the parity–check matrix of a $(v,\ b,\ k,\ r)$–LDPC code $(v < b$) with code rate $\frac{(b-rank(N))}{n}$ and the code dimension: $b - rank(N)$, where $rank(N)$ is calculated over $GF\ (2)$.

Also N^T is the parity–check matrix of a $(b, v,\ r,\ k)$–LDPC code with $(b < v)$ with code rate $\frac{(v-rank(N^T))}{n}$ and the code dimension: $v - rank\left(N^T\right)$, where $rank\left(N^T\right)$ is calculated over $GF\ (2)$.

Result. In view of Lemma 5.1 and Remark 5.2, we have following results:

1. The dual of RD with parameters: $v = q^2, b = q(q-1), r = q-1, k = q, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 1, m = n = q$ yields an LDPC code free of 4–cycles with length q^2, column weight $q-1$, row weight q, rank over field of order $2 = q^2 - 2q + 2$ and code rate: $R = \frac{2(q-1)}{q^2}$.
2. The RD design with parameters: $v = q(q-t), b = q(q-1), r = q-1, k = q-t, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 1, m = q-t, n = q\ (t \geq 2)$ yields an LDPC code free of 4–cycles with length $q(q-1)$, column weight $q-t$, row weight $q-1$, rank over field of order $2 = (q^2 - 2q + 2) - (t-1)(q-1)$ and code rate:

$$R = \frac{[(q-1)(q+t-1) - (q^2 - 2q + 2)]}{q(q-1)}.$$

The ranks in results 1 and 2 are determined using polyfit() function of MATLAB.

Example 5.3. For $q = 7$ in Result 1 above, we obtain an RD with parameters: $v = 49, b = 42, r = 6, k = 7, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 1, m = n = 7$. The dual of this design yields an LDPC code free of 4–cycles with length 49, column weight 6, row weight 7, rank 37 and rate $R = 0.24$.

Example 5.4. For $q = 31,\ t = 2$ in Result 2 above, we obtain an RD with parameters: $v = 899, b = 930, r = 30, k = 29, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 1, m = 29, n = 31$. Then the design yields an LDPC code free of 4–cycles with length 930, column weight 29, row weight 30, rank 871 and rate $R = 0.06$.

6. Discussion and conclusion

Here, a brief survey on tactical decomposable RD families is presented. RDs already have wide applications in statistics and agricultural field experiments. Some applications of RDs in cryptography and coding theory are described here. Tactical decomposable RDs had not been previously used in the constructions of threshold schemes and LDPC codes. RDs provide candidate incidence structures for threshold scheme and LDPC−code constructions, subject to the additional reconstruction, privacy, rank, and performance analyses.

A binary $(m, n, \rho, \{\mu - 1, \mu\})$ $-$*near regular (NR) LDPC code* $\mathbb{C}$ of block length n is the null space of a $m \times n$ sparse parity–check matrix H over a Galois field $GF\ (2)$ such that each row has varying weights $\mu - 1$ or μ and each column has constant weight ρ where $\mu, \mu - 1 \ll n$ and $\rho \ll m$. RDs may also have possible applications in the constructions of NRLDPC codes.

The following aspects of RDs can be investigated further:

(i) Although several series of doubly resolvable group divisible designs are available in the literature, no such series is available for RDs. It would be interesting to obtain some series of doubly resolvable RDs. Doubly resolvable designs are also applicable in coding theory, see Topalova and Zhelezova [35].

(ii) Recently Singh [29] introduced doubly near affine doubly $(\mu,\ \nu)-$resolvable designs. Interested workers in design theory can obtain some series of such RDs.

(iii) An association scheme (AS) on triples on a set Ω is a partition of $\Omega\times\Omega\times\Omega$ satisfying certain regularity properties, see Balmaceda et al. [3]. Some series of RDs based on this AS can be obtained and their applications in statistics, cryptography and coding theory can also be explored.

(iv) Some series of tactical decomposable RD families, in which all internal block matrices are not square, are provided in Section 3 (Theorems: 3.15, 3.16 and 3.17). Such series of designs can also be used in the constructions of threshold schemes.

Conflict of Interest

The author has no financial or non–financial conflict of interest to declare for the research work conducted in this article.

Acknowledgements

The author is grateful to anonymous reviewers and Dr. M. K. Singh and for their valuable suggestions in improving the content and presentation of the paper. The author is also obliged to Dr. S. N. Topno for determining the rank of some block matrices.

Funding

This research received no external funding.

Data Availability

This study is theoretical and does not involve the generation or analysis of datasets.

References

[1] T. Adachi and X. Lu. Magic cubes and secret sharing schemes. *Research Institute of Mathematical Sciences, Kokyuroku, Kyoto University*, 2096:115–118, 2018.

[2] M. Alinejad and K. Khashyarmanesh. Counting short cycles of (c, d)–regular bipartite graphs. *Discrete Mathematics, Algorithms and Applications*, 13(3), 2150022, 2021. https://doi.org/10.1142/S1793830921500221.

[3] J. M. P. Balmaceda, D. V. A. Briones, and J. N. Buloron. Association scheme on triples from the unitary group, 2025. arXiv: 2511.01604 [math.CO].

[4] H. Bekar, C. Mitchell, and F. Piper. Tactical decomposition of designs. *Aequationes Mathematicae*, 25:123–152, 1982. https://doi.org/10.1007/BF02189612.

[5] N. Bonello, S. Chen, and L. Hanzo. Low–density parity–check codes and their rateless relatives. *IEEE Communications Surveys & Tutorials*, 13(1):3–26, 2011. https://doi.org/10.1109/SURV.2011.040410.00042.

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

[7] W. H. Clatworthy. *Tables of Two–Associate–Class Partially Balanced Designs*, number 63 in National Bureau of Standards Applied Mathematics Series. U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., 1973.

[8] W. de Launey. Generalized hadamard matrices. In C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, pages 301–306. Chapman & Hall/CRC, Boca Raton, FL, 2nd edition, 2007.

[9] Q. Diao, Y. Tai, S. Lin, and K. Abdel–Ghaffar. Ldpc codes on partial geometries: construction, trapping set structure, and puncturing. *IEEE Transactions on Information Theory*, 59(12):7898–7914, 2013. https://doi.org/10.1109/TIT.2013.2280640.

[10] M. Gholami and A. Nassaj. Ldpc codes based on rational functions. *IETE Journal of Research*, 69(7):4224–4229, 2023. https://doi.org/10.1080/03772063.2021.1951365.

[11] S. Gupta and R. Mukerjee. *A Calculus for Factorial Arrangements*, volume 59 of *Lecture Notes in Statistics*. Springer-Verlag, New York, 1989.

[12] S. J. Johnson and S. R. Weller. Resolvable 2–design for regular low–density parity–check codes. *IEEE Transactions on Communications*, 51(9):1413–1419, 2003. https://doi.org/10.1109/TCOMM.2003.816987.

[13] S. Kageyama and K. Sinha. Some patterned constructions of rectangular designs. *Journal of the Japan Statistical Society*, 33(1):137–144, 2003. https://doi.org/10.14490/jjss.33.137.

[14] C. Koukouvinos and S. Stylianou. On skew–hadamard matrices. *Discrete Mathematics*, 308:2723–2731, 2008. https://doi.org/10.1016/j.disc.2006.06.037.

[15] L. Mostari and A. Taleb-Ahmed. High performance short–block binary regular ldpc codes. *Alexandria Engineering Journal*, 57(4):2633–2639, 2018. https://doi.org/10.1016/j.aej.2017.09.016.

[16] J. Pieprzyk and X. Zhang. Ideal threshold schemes from orthogonal arrays. In R. Deng, S. Qing, F. Bao, and J. Zhou, editors, *Information and Communications Security*, pages 469–479. Springer, 2002.

[17] D. Raghavarao and R. Singh. Applications of pbib designs in cluster sampling. *Proceedings of the Indian National Science Academy*, 41:281–288, 1975.

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

[19] S. Saurabh. Some series of tactical decomposable regular group divisible designs. *Congressus Numerantium*, 236:65–72, 2025. https://doi.org/10.61091/cn236-05.

[20] S. Saurabh. Tactical decomposable regular group divisible designs and their threshold schemes. *Utilitas Mathematica*, 122:109–116, 2025. https://doi.org/10.61091/um122-08.

[21] S. Saurabh. Some series of cyclic partially balanced designs. *Journal of the Indian Society of Agricultural Statistics*, 80(2):389–394, 2026. https://doi.org/10.56093/JISAS.V80I2.9.

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

[23] S. Saurabh and K. Sinha. Some matrix constructions of L_2–type latin square designs. *Bulletin of the ICA*, 95:93–104, 2022.

[24] S. Saurabh and K. Sinha. Ldpc codes based on α–resolvable designs. *SN Computer Science*, 4, 617, 2023. https://doi.org/10.1007/s42979-023-02088-2.

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

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

[27] S. Saurabh and K. Sinha. Ldpc codes based on new combinatorial designs. *Statistics and Applications*, 22(2):109–119, 2024.

[28] X. Shan and T. Li. A construction of low–density parity–check codes. *Journal of Mathematical Research with Applications*, 33(3):330–336, 2013.

[29] M. K. Singh. Doubly near affine doubly (μ, ν)–resolvable group divisible packing designs. *Bulletin of the ICA*, 105:70–105, 2025.

[30] 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.

[31] K. Sinha, M. K. Singh, S. Kageyama, and R. S. Singh. Some series of rectangular designs. *Journal of Statistical Planning and Inference*, 106:39–46, 2002. https://doi.org/10.1016/S0378-3758(02)00200-8.

[32] D. R. Stinson. *Cryptography: Theory and Practice*. Chapman & Hall/CRC, Boca Raton, FL, 3rd edition, 2006.

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

[34] C. Suen. Some rectangular designs constructed by the method of differences. *Journal of Statistical Planning and Inference*, 21:273–276, 1989. https://doi.org/10.1016/0378-3758(89)90011-6.

[35] S. Topalova and S. Zhelezova. Doubly resolvable designs with small parameters. *Ars Combinatoria*, 117:289–302, 2014.

[36] M. N. Vartak. On an application of kronecker product of matrices to statistical designs. *Annals of Mathematical Statistics*, 26:420–438, 1955. https://doi.org/10.1214/aoms/1177728488.

[37] W. D. Wallis, A. P. Street, and J. S. Wallis. *Combinatorics: Room Squares, Sum–Free Sets, Hadamard Matrices*, volume 292 of *Lecture Notes in Mathematics*. Springer–Verlag, Berlin, Heidelberg, 1972.

[38] S. B. Wicker. *Error Control Systems for Digital Communication and Storage*. Prentice-Hall, Englewood Cliffs, NJ, 1995.

[39] H. Xu, D. Feng, C. Sun, and B. Bai. Construction of ldpc codes based on resolvable group divisible designs. In *2015 International Workshop on High Mobility Wireless Communications (HMWC)*, pages 111–115, 2015. https://doi.org/10.1109/HMWC.2015.7354346.

Shyam Saurabh
Department of Mathematics, Tata College, Kolhan University, Chaibasa, India
E-mail shyamsaurabh785@gmail.com