THE TEACHING OF MATHEMATICS
2025, Vol. XXVIII, No. 1, pp. 42–73
DOI: 10.57016/TM-NOQK3870

BALANCED INCOMPLETE BLOCK DESIGNS FOR TEACHING COMBINATORICS: CONSTRUCTION AND APPLICATIONS

Daniel Martín-Cudero

Abstract. This article presents balanced incomplete block designs as an effective pedagogical tool for teaching combinatorics. Through their construction, analysis, and practical application, the article proposes an interdisciplinary approach that enables abstract content to be addressed in a contextualized and meaningful way. Specifically, it explores algebraic and matrix structures that model situations with structural regularity, fostering the development of logical and abstract thinking in the classroom. Additionally, key statistical concepts, such as experimental design and analysis, are introduced to provide an applied perspective on decision-making and data interpretation. These tools are presented through real-world examples that help students develop reasoning, modeling, and critical analysis skills, while also reinforcing the understanding of mathematics as a powerful tool for solving relevant and structured combinatorial problems.

MathEduc Subject Classification: K25

AMS Subject Classification: 97K20

Key words and phrases: BIBD; balanced incomplete block design; combinatorial design; teaching combinatorics; Steiner triple system; resolvable design; Kramer-Mesner; Hadamard matrix; experimental design.

1. Introduction

Combinatorics is a branch of mathematics traditionally presented as a collection of techniques for counting, ordering, or selecting elements. However, its real power lies in its ability to model complex real-world problems using simple and elegant structures. Among these structures are Balanced Incomplete Block Designs (BIBDs)—tools that, beyond their theoretical value, find applications in diverse fields such as statistics, information theory, cybersecurity, and event organization.

A BIBD is a combinatorial structure defined on a finite set X of v elements, arranged into b blocks, and satisfying the following conditions:

(1) Each block contains exactly k elements.

(2) Each element of X appears in exactly r blocks.

(3) Every pair of elements from X appears together in exactly λ blocks.

Such a design is called incomplete because no block contains all the elements of X (that is, $k < v$), and balanced due to the symmetry conditions imposed by the parameters r and λ [1].

A first didactic approach to BIBDs can be made through recreational mathematics. Classical problems such as magic squares, Sudoku puzzles, chess challenges, or the well-known Kirkman's schoolgirl problem are examples of configurations that can be reinterpreted as resolvable designs, thereby sparking students' interest in their structural beauty. However, the application of such designs goes far beyond recreational purposes. In applied game theory, for instance, they are used to model decision-making situations, conflict simulations, and planning tasks in artificial intelligence, where combinatorial heuristics and strategies are employed to assess the complexity of certain game scenarios.

Another relevant field of application is information theory, particularly in the construction of error-detecting and error-correcting codes [2]. These codes ensure the reliable transmission of data even in highly noisy environments, such as space communications. Mathematically, such coding relies on Linear Algebra over Galois Fields. This area also includes secret sharing schemes [3], in which certain information can only be reconstructed if at least k out of the v participants collaborate, thus ensuring the security of sensitive data.

In the field of security and cryptography, combinatorial designs are used to generate message authentication codes, providing guarantees of authenticity and integrity [4]. Resolvable or partially balanced designs are applied here to define valid key or tag combinations that verify messages. However, perhaps the most structured and well-known application of combinatorial designs is found in statistics, through the theory of experimental design [5]. In this context, BIBDs enable the planning of experiments aimed at minimizing the number of necessary trials while maximizing the information obtained, all while controlling multiple variables.

The aim of this article is to show how BIBDs can be used as a pedagogical resource for teaching combinatorics, through real, engaging, and contextualized examples that may serve to motivate students and deepen their understanding of the subject.

2. Background

Definition 2.1. Let v, k and λ be positive integers such that $v > k \geq 2$. A *balanced incomplete block design* (BIBD) or *2-design* is a pair $(X, \mathcal{B})$ where $X = \{x_i\}_{i=1}^{v}$ is a set of v elements and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ is a collection of b blocks. Each block B_j contains exactly k elements from X, and every pair of distinct elements from X appears together in exactly λ blocks. This design is denoted as a 2-(v, k, λ) design, or (v, k, λ)-BIBD.

This combinatorial structure can be conveniently represented using an incidence matrix, which records the presence or absence of each element within each block. This algebraic representation is essential for analyzing and manipulating designs computationally [6].

Definition 2.2. Let $(X, \mathcal{B})$ be a 2-design where $|X| = v$ and $|\mathcal{B}| = b$. The boolean matrix $A = (a_{ij})$ of dimension $v \times b$ such that

$$a_{ij} = \begin{cases} 1 & \text{if } x_i \in B_j \\ 0 & \text{if } x_i \notin B_j \end{cases}$$

is called the *incidence matrix* of $(X, \mathcal{B})$.

One of the key numerical properties of a 2-design is the number of blocks required to meet the balancing condition. This quantity is determined by the parameters of the design, as given by the following theorem:

THEOREM 2.3. *The number of blocks in a (v, k, λ)-BIBD is*

$$b = \frac{\lambda v(v-1)}{k(k-1)}.$$

Proof. Let $(X, \mathcal{B})$ be a 2-(v, k, λ) design. Consider a 2-subset $T \subseteq X$ and a block $B \in \mathcal{B}$ that contains T. We will count the number of such pairs (T, B) in two different ways:

(1) First, observe that each block contains exactly $\binom{k}{2}$ distinct 2-subsets, since we are choosing 2 elements from the k elements in each block. As there are b blocks, the total number of such pairs (T, B) is $b\binom{k}{2}$.

(2) On the other hand, the total number of 2-subsets in X is $\binom{v}{2}$. By definition of a 2-(v, k, λ) design, each 2-subset $T \subseteq X$ is contained in exactly λ blocks. Therefore, the total number of such pairs is also $\lambda\binom{v}{2}$.

Equating both expressions for the number of pairs (T, B) and expanding the binomial coefficients, we can easily derive the formula for b. ■

Another key quantity in the study of designs is the number of times each element appears in the blocks, known as the *replication number*. This is also precisely determined in terms of the design's parameters:

THEOREM 2.4. *Let the pair $(X, \mathcal{B})$ be a (v, k, λ)-BIBD, with $|X| = v > k \geq 2$ and $\lambda \geq 1$. Then, every element of X is contained in exactly*

$$r = \frac{\lambda(v-1)}{k-1}$$

blocks.

Proof. Let $(X, \mathcal{B})$ be a 2-(v, k, λ) design. Fix an element $x \in X$, and let r denote the number of blocks in which x appears. Now, define the set

$$V = \{(x, B_j) : y \in X, : y \neq x, : B_j \in \mathcal{B}, : \{x, y\} \subseteq B_j\}.$$

We will count the number of such pairs $(x, B_j) \in V$ in two different ways:

(1) On the one hand, since there ar $v - 1$ possible elements $y \in X$ such that $y \neq x$, and each pair $\{x, y\}$ appears in exactly λ blocks by the definition of a 2-design, the total number of such pairs is $|V| = \lambda(v - 1)$.

(2) On the other hand, the element x lies in exactly r blocks, and within each such block, there are $k-1$ elements other than x to form a pair $\{x, y\}$. Therefore, we also have $|V| = r(k-1)$.

Since both expressions count the same quantity, it follows that $r(k-1) = \lambda(v-1)$. The identity holds for any choice of $x \in X$, completing the proof. [16] ■

A direct consequence of the previous equations is the identity

$$bk = rv,$$

which must hold for any valid 2-(v, k, λ) design. This identity indicates that not all combinations of parameters will yield a valid design, since both the replication number r and the total number of blocks b must be positive integers. Additionally, if such a design exists, then it must satisfy *Fisher's inequality*, which states that $b \geq v$ (see the proof in [7]).

EXAMPLE 2.5. [16] The pair $(X, \mathcal{B})$ defined by the set of varieties $X = \{1, 2, 3, 4, 5, 6\}$ and the collection of blocks $\mathcal{B} = \{B_j \subset X \mid j = 1, 2, \ldots, 15\}$:

$$\begin{array}{lll}
B_1 = \{1,2,3,4\} & B_6 = \{3,4,5,6\} & B_{11} = \{1,3,5,6\} \\
B_2 = \{1,4,5,6\} & B_7 = \{1,2,3,6\} & B_{12} = \{2,3,5,6\} \\
B_3 = \{2,3,4,6\} & B_8 = \{1,3,4,5\} & B_{13} = \{1,2,5,6\} \\
B_4 = \{1,2,3,5\} & B_9 = \{2,4,5,6\} & B_{14} = \{1,3,4,6\} \\
B_5 = \{1,2,4,6\} & B_{10} = \{1,2,4,5\} & B_{15} = \{2,3,4,5\}
\end{array}$$

is a 2-$(6, 4, 6)$ design. Indeed, we observe that $|X| = v = 6$, each block contains $k = 4$ elements of the set X, and every pair of distinct elements of X appears in exactly $\lambda = 6$ blocks. We can verify, by Theorems 2.3 and 2.4, that the number of blocks is indeed $|\mathcal{B}| = b = 15$, and that each element of X appears in exactly $r = 10$ blocks. Moreover, by applying Definition 2.2, we obtain that the incidence matrix of the design is given by:

$$A = \begin{pmatrix}
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}. \qquad \triangle$$

Among the different types of designs, there are particular cases that have noteworthy applications. One such case is the Steiner Triple System (STS), which can be viewed as a 2-design with blocks of size 3 and $\lambda = 1$.

DEFINITION 2.6. A *Steiner Triple System* of order v, denoted by $STS(v)$, is a pair $(X, \mathcal{B})$ where X is a set with v elements and $\mathcal{B}$ is a collection of triples (subsets of three elements) of X, such that every pair of distinct elements of X is contained in exactly one triple. That is, an $STS(v)$ is simply a 2-$(v, 3, 1)$ design.

This type of design exists only for certain values of v, as indicated by the following result (see the proof in [1]).

Theorem 2.7. *If an $STS(v)$ exists with $v \geq 7$, then $v \equiv 1$ or $3 \pmod 6$.*

Example 2.8. A classical example of a Steiner triple system is the one derived from the *Fano plane*, which is the smallest finite projective plane. It can also be represented geometrically, as shown in Figure 1. Let $X = \{1,2,3,4,5,6,7\}$ be the point set, and let $\mathcal{B}$ be the collection of blocks given by:

$$\mathcal{B} = \{\{1,2,5\},\{1,3,6\},\{1,4,7\},\{5,6,7\},\{2,3,7\},\{3,4,5\},\{2,4,6\}\}.$$

Then, the pair $(X,\mathcal{B})$ forms a 2-$(7,3,1)$ design or $STS(7)$. In this configuration, each block contains exactly 3 elements, and every pair of distinct elements from X occurs in exactly one block. △

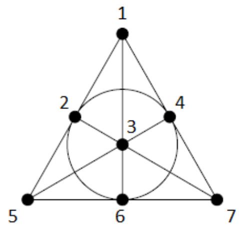

Figure 1. Steiner triple system of order 7 constructed from the fano plane – projective plane of order 2.

In practical applications, such as experimental designs or scheduling, there may be a need for an additional layer of structure: *resolvability*. A 2-design is said to be resolvable if its blocks can be partitioned into parallel classes, each of which forms a partition of the point set [7]. These designs are known as *resolvable BIBDs*, and their construction often poses significant combinatorial challenges due to the extra resolution constraints [8].

Definition 2.9. Let $(X,\mathcal{B})$ be a 2-(v,k,λ) design:

(1) A *parallel class* in $(X,\mathcal{B})$ is a subset of pairwise disjoint blocks from $\mathcal{B}$, whose union is the entire set X. In other words, it is a collection of blocks from $\mathcal{B}$ that partition the set X.

(2) A 2-(v,k,λ) *resolvable design* is a 2-(v,k,λ) design whose block family $\mathcal{B}$ admits at least one partition into parallel classes.

Each parallel class consists of $c = \frac{v}{k}$ blocks. Therefore, the condition $v \equiv 0 \pmod k$ is necessary, but not sufficient, for the existence of a parallel class in a 2-(v,k,λ) design. We denote the parallel classes by $\mathcal{C}_i$, where $i = 1,2,\ldots,r = \frac{b}{c}$.

Example 2.10. Let $(X,\mathcal{B})$ be a 2-$(9,3,1)$ design, where $X = \{1,2,\ldots,9\}$ and $\mathcal{B}$ is the set consisting of the following blocks:

$$\begin{array}{lll} B_1 = \{1,2,3\} & B_5 = \{4,5,6\} & B_9 = \{7,8,9\} \\ B_2 = \{1,4,7\} & B_6 = \{2,5,8\} & B_{10} = \{3,6,9\} \\ B_3 = \{1,5,9\} & B_7 = \{2,6,7\} & B_{11} = \{3,4,8\} \\ B_4 = \{1,6,8\} & B_8 = \{2,4,9\} & B_{12} = \{3,5,7\} \end{array}$$

The parallel classes of this design are given by:

$$\mathcal{C}_1 = \{B_1, B_5, B_9\},\ \ \mathcal{C}_2 = \{B_2, B_6, B_{10}\},\ \ \mathcal{C}_3 = \{B_3, B_7, B_{11}\},\ \ \mathcal{C}_4 = \{B_4, B_8, B_{12}\}.$$

Observe that the union of the blocks in each parallel class is the entire set X. Furthermore, any two blocks within a parallel class are pairwise disjoint. For instance, in $\mathcal{C}_1$, we have $B_1 \cup B_5 \cup B_9 = X$, along with $B_1 \cap B_5 = \emptyset$, $B_1 \cap B_9 = \emptyset$, and $B_5 \cap B_9 = \emptyset$. The same properties hold for the remaining parallel classes of the design. Therefore, we conclude that the given structure is a 2-$(9, 3, 1)$ resolvable design. $\triangle$

In the study of resolvable designs, it is essential to understand the combinatorial constraints that their parameters must satisfy. One such constraint is given by Bose's inequality, which provides a lower bound on the number of blocks in terms of the other parameters of the design (see the proof in [7]).

THEOREM 2.11. [*Bose's Inequality*] *If a* 2-(v, k, λ) *resolvable design exists, then it must satisfy* $b \geq v + r - 1$.

From this, it follows that the condition $b \geq v + r - 1$ holds if and only if $r \geq k + \lambda$.

It is also worth noting that the existence of an $STS(v)$ is closely related to the presence of other combinatorial structures. For instance, it is tied to the concept of resolvability. This structure, where each parallel class forms a partition of the point set, introduces an additional layer of combinatorial complexity to the STS, thereby giving rise to the Kirkman Triple Systems (KTS).

DEFINITION 2.12. A *Kirkman Triple System* of order v is a 2-$(v, 3, 1)$ resolvable design with its blocks arranged into parallel classes. It is denoted by $KTS(v)$.

Just as with STS, a KTS does not exist for every value of v. A necessary and sufficient condition for its existence is given in the following theorem (see the proof in [7]).

THEOREM 2.13. *A Kirkman Triple System of order* $v \geq 9$ *exists if and only if* $v \equiv 3 \pmod 6$, *with* v *odd.*

REMARK 2.14. Example 2.10 is one of the possible Kirkman triple systems of order 9 that can be constructed. Another combination of blocks for this design can be constructed with the successive diagonals Algorithm 3.19 that we will see later in Section 3.3.

Another interesting class of designs is that of symmetric designs, where the number of blocks equals the number of elements, i.e., $b = v$. This automatically implies that $r = k$.

DEFINITION 2.15. A 2-(v, k, λ) design in which $b = v$ (or equivalently, $r = k$) is called a 2-(v, k, λ) *symmetric design.* Such a design may also be denoted as a (v, k, λ)-SD.

Finally, symmetric designs also have a remarkable property: every pair of distinct blocks intersects in exactly λ elements. This feature makes them highly uniform structures, useful in code theory, finite geometry, and other fields [9]. One important property of such designs is that any two distinct blocks intersect in a fixed number of elements, as stated in the following theorem (see the proof in [7]).

THEOREM 2.16. *Let* $(X, \mathcal{B})$ *be a* 2-(v, k, λ) *symmetric design. Then, for any* $1 \leq i < j \leq v$, *we have* $|B_i \cap B_j| = \lambda$. *That is, every pair of distinct blocks in* $\mathcal{B} = \{B_j\}_{j=1}^{v}$ *intersects exactly in* λ *elements.*

EXAMPLE 2.17. Consider the 2-$(4, 3, 2)$ symmetric design given by the pair $(X, \mathcal{B})$, where $X = \{1, 2, 3, 4\}$ and

$$\mathcal{B} = \big\{B_1 = \{1, 2, 3\},\ B_2 = \{1, 2, 4\},\ B_3 = \{1, 3, 4\},\ B_4 = \{2, 3, 4\}\big\}.$$

It can be verified that

$$|B_1 \cap B_2| = |B_1 \cap B_3| = |B_1 \cap B_4| = |B_2 \cap B_3| = |B_2 \cap B_4| = |B_3 \cap B_4| = \lambda = 2. \quad \triangle$$

REMARK 2.18. In Section 3.4, we will see how to construct symmetric designs using Hadamard matrices.

3. Construction of balanced incomplete block designs

3.1. Kramer-Mesner Theorem

One of the most effective algebraic approaches to construct BIBDs involves exploiting the symmetries of the design via group actions. In particular, the Kramer-Mesner method allows us to translate the existence problem of certain combinatorial designs into a system of linear equations, governed by the action of a permutation group on subsets of the point set [10]. This subsection introduces the fundamental concepts underlying this method, including automorphisms, group actions on set systems, orbit structures, and culminates with the statement and proof of the Kramer-Mesner Theorem (The definitions corresponding to this subsection are taken from [7] and [16]). This theorem not only establishes a theoretical framework but also serves as a practical tool for the algorithmic construction of BIBDs with prescribed symmetry groups.

DEFINITION 3.1. Let $(X, \mathcal{B})$ and $(X', \mathcal{B}')$ be two designs such that $|X| = |X'|$. We say that $(X, \mathcal{B})$ and $(X', \mathcal{B}')$ are *isomorphic* if there exists a bijection $\alpha : X \to X'$ such that

$$\big\{\,\{\alpha(x) : x \in B\} : B \in \mathcal{B}\,\big\} = \mathcal{B}'.$$

The bijection α is called an *isomorphism*. In other words, $(X, \mathcal{B})$ and $(X', \mathcal{B}')$ are isomorphic if one can be obtained from the other by relabeling points or blocks.

DEFINITION 3.2. Let $(X, \mathcal{B})$ be a design. A bijection $\alpha : X \to X$ such that

$$\big\{\,\{\alpha(x) : x \in B\} : B \in \mathcal{B}\,\big\} = \mathcal{B}$$

is called an *automorphism* of $(X, \mathcal{B})$. That is, α is an isomorphism from $(X, \mathcal{B})$ to itself, and therefore a permutation of X.

Since an automorphism is a permutation of the set X, from now on we will work with the permutations of the symmetric group on the set X of v elements, which we denote by S_v.

DEFINITION 3.3. The set of all automorphisms of a design $(X, \mathcal{B})$ with $|X| = v$ forms a group under the composition of permutations. This group is called the *automorphism group* of $(X, \mathcal{B})$ and is denoted by $\mathrm{Aut}(X, \mathcal{B})$. It is a subgroup of the *symmetric group* S_v, which has order $|S_v| = v!$ and consists of all $v!$ permutations of the set X. A subgroup of S_v is called a *permutation group*.

We will often use the *cycle decomposition* to describe elements of S_v. An *ℓ-cycle* $(a_1, a_2, \ldots, a_\ell)$ is the element of S_v defined by:

$$\begin{aligned} a_i &\mapsto a_{i+1}, \quad \text{for } 1 \leq i \leq \ell - 1, \\ a_\ell &\mapsto a_1. \end{aligned}$$

DEFINITION 3.4. Two cycles $(a_1, a_2, \ldots, a_\ell)$ and $(b_1, b_2, \ldots, b_m)$ are said to be *disjoint* if $a_i \neq b_j$ for all i and j.

Note that every element of S_v can be expressed as a product of disjoint cycles, and this decomposition is unique up to the order of the cycles. From now on, we will express permutations of the elements of a design using their disjoint cycle decompositions.

DEFINITION 3.5. Let $X = \{1, 2, \ldots, v\}$ be the point set of a 2-(v, k, λ) design, and let S_v be the symmetric group consisting of the $v!$ permutations of X. A subgroup $G \leq S_v$ acts by evaluation on the set of all j-element subsets of X, denoted by $\binom{X}{j}$. The *orbits* induced by this group action are defined as:

$$\mathcal{O}_j(J) = \{\alpha(J) : \alpha \in G\}, \quad \text{for } J \in \binom{X}{j}.$$

To emphasize that the group action is applied to subsets of size j, we will refer to these orbits as *j-orbits*. Thus, each j-orbit is a subset of $\binom{X}{j}$.

DEFINITION 3.6. [Kramer-Mesner matrix] Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_n$ be the k-orbits, and let $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m$ be the 2-orbits of the design. The *Kramer-Mesner matrix* $A_{k,2} = (a_{i,j})_{i=1,\ldots,n}^{j=1,\ldots,m}$ is defined as:

$$a_{i,j} = |\{A \in \mathcal{O}_i : Y_j \subset A\}|, \quad \text{where } Y_j \in \mathcal{P}_j.$$

The (i, j)-entry of the matrix counts the number of occurrences of $\mathcal{P}_j$ among the 2-subsets of elements in $\mathcal{O}_i$. This value is well-defined, that is, independent of the choice of the representative $Y_j \in \mathcal{P}_j$. Indeed, for any $Y, Y' \in \mathcal{P}_j$, there exists an automorphism $\beta \in G$ such that $\beta(Y) = Y'$. Therefore, if $Y \subset A$, then $Y' \subset \beta(A)$. Since β is a permutation, we have $\beta(A) = \beta(B)$ if and only if $A = B$, implying that for each $A \in \mathcal{O}_i$ with $Y \subset A$, there exists a unique $A' = \beta(A)$ such that $Y' \subset A'$. Applying the same argument to β^{-1}, we obtain:

$$|\{A \in \mathcal{O}_i : Y \subset A\}| = |\{A \in \mathcal{O}_i : Y' \subset A\}|.$$

This matrix encodes all the necessary information for the group G to act as a group of automorphisms of the design. This is formalized in the following theorem, which gives a necessary and sufficient condition for the existence of a design admitting G as a group of automorphisms.

THEOREM 3.7. [Kramer-Mesner Theorem] *A 2-(v, k, λ) design $(X, \mathcal{B})$ exists with G as a group of automorphisms if and only if there exists a solution $\mathbf{z} \in \{0, 1\}^n$ to the matrix equation*

$$\mathbf{z}A_{k,2} = \lambda \mathbf{u}^t,$$

where $\mathbf{u}$ *is the all-ones vector.*

Proof. If the vector $\mathbf{z} = (z_1, \ldots, z_n) \in \{0, 1\}^n$ is a solution to the above system of equations, then the 2-(v, k, λ) design whose blocks consist of the family

$$\mathcal{B} = \bigcup_{\{i : z_i = 1\}} \mathcal{O}_i,$$

has G as its automorphism group. Indeed, on the one hand, since each set $\mathcal{O}_i$ is a k-orbit of the action of the group G, it follows that G is a subgroup of the automorphism group of the design. On the other hand, given two vertices $x_i, x_j \in X$, the set $\{x_i, x_j\}$ belongs to some 2-orbit $\mathcal{P}_t$. One of the equations in the system tells us that

$$z_1 a_{1,t} + z_2 a_{2,t} + \cdots + z_n a_{n,t} = \lambda,$$

where $a_{i,t} = \{A \in \mathcal{O}_i : \{x_i, x_j\} \subset A\}$. Therefore, we conclude that $\{x_i, x_j\}$ is contained in exactly λ blocks of the design.

For the implication in the other direction, observe that if G is a subgroup of the automorphism group of $(X, \mathcal{B})$, then the family $\mathcal{B}$ must consist of the union of some k-orbits $\mathcal{O}_i$. Define $z_i = 1$ if the elements of the orbit $\mathcal{O}_i$ are part of the blocks of the design and $z_i = 0$ otherwise. In this sense, the fact that each pair of vertices $\{x_i, x_j\}$ is contained in exactly λ blocks ensures that we have a solution to the system of equations (Proof taken from [16]). ∎

Finding a solution to the system $\mathbf{z}A_{k,2} = \lambda \mathbf{u}^t$ not only guarantees the existence of a 2-design, but also allows us to explicitly construct such a design from the k-orbits $\mathcal{O}_i$ used to form the Kramer-Mesner matrix. Of course, there may exist other designs that also admit G as a group of automorphisms, but the Kramer-Mesner theorem ensures that at least one such design can be constructed.

ALGORITHM 3.8. [Construction of 2-Designs Using the Kramer-Mesner Theorem] To construct a 2-(v, k, λ) design from permutations composed of cycles using the Kramer-Mesner Theorem, follow these steps [16]:

(1) Determine the permutations in the group $G = \langle \alpha \rangle$.
(2) Compute the 2-orbits and k-orbits of X under the action induced by the group G. These will be used to construct the Kramer-Mesner matrix $A_{k,2}$.
(3) Let m and n denote the number of 2-orbits and k-orbits, respectively. The Kramer-Mesner matrix $A_{k,2}$ is of dimension $n \times m$. Select a representative

subset from each orbit and study the matrix $A_{3,2}$ formed with these representatives. Note that the sum of the entries in each column of this matrix must be constant.

(4) Solve the matrix equation $\mathbf{z}A_{k,2} = \lambda\mathbf{u}^t$ with the constraint that $\mathbf{z} \in \{0,1\}^n$. From these solutions, determine all possible values of λ and thus identify the number of distinct 2-designs that can be constructed for a fixed value of k.

(5) For each solution vector $\mathbf{z}$, associate the component $\mathbf{z}_i$ with the k-orbit $\mathcal{O}_i$, for all $i = 1, \dots, n$. The resulting 2-(v,k,λ) designs are formed by the blocks belonging to those k-orbits $\mathcal{O}_i$ such that $\mathbf{z}_i = 1$.

Remark 3.9. In Section 4.1.1., we will demonstrate the application of this algorithm through a concrete example. Specifically, we construct a 2-$(9,3,3)$ design to address a problem related to error-detecting codes.

3.2. Cyclic Steiner triple system

While the Kramer-Mesner method provides a general and flexible framework for constructing 2-designs with specified automorphism groups, certain families of designs can also be constructed explicitly using algebraic structures with high symmetry. Among these, Steiner triple systems that are invariant under cyclic group actions, known as cyclic Steiner triple systems, are of particular interest due to their elegant algebraic properties and constructive simplicity.

This subsection introduces the notion of difference families in finite groups, a classical tool for generating cyclic designs, and shows how these families can be used to construct cyclic Steiner triple systems of specific orders. We conclude with an explicit construction based on primitive roots in finite fields, yielding infinite families of such systems (the definitions and theorems of this subsection are taken from [7]).

Definition 3.10. Let $(G,+)$ be a finite group of order v with identity element 0. Let k and λ be positive integers such that $2 \le k \le v$. A (v,k,λ) *difference family* in $(G,+)$ is a collection of subsets of G, denoted by $\mathcal{F} = \{F_i : i = 1,2,\dots,L\}$, satisfying the following properties:

(1) Each subset has size k, i.e., $|F_i| = k$ for all $1 \le i \le L$.

(2) The multiset $\mathcal{M} = \bigcup_{i=1}^{L}\{x-y, y-x : x,y \in F_i, x \neq y\}$ contains every nonzero element of G exactly λ times.

We denote the set of differences of each subset F_i by $\triangle F_i$, for $i = 1,2,\dots,L$.

Difference families in abelian groups play a central role in the construction of various combinatorial designs. The parameters of such families must satisfy certain arithmetic conditions, one of which is given below (see the proof in [1]).

Lemma 3.11. *Let $(G,+)$ be an abelian group of order v with identity element 0. Let $\mathcal{F}$ be a (v,k,λ) difference family in $(G,+)$ consisting of L subsets. A* *necessary (but not sufficient) condition for the existence of such a family is*

$$\lambda(v-1) = Lk(k-1).$$

Definition 3.12. Let $\mathcal{F} = \{F_i : i = 1, 2, \dots, L\}$ be a (v, k, λ) difference family in an abelian group $(G, +)$:

(1) The set $\mathcal{T}_i = \{g + F_i : g \in G\}$ is called the *translate* of F_i.
(2) The collection of all translates of each F_i is called the *development* of $\mathcal{F}$.

The following theorem shows that the development of a difference family yields a 2-design with the same parameters (see the proof in [7]).

Theorem 3.13. *Let $\mathcal{F}$ be a (v, k, λ) difference family in an abelian group $(G, +)$. Then, if $\mathcal{B}$ is the development of $\mathcal{F}$, the pair $(G, \mathcal{B})$ forms a 2-(v, k, λ) design.*

Definition 3.14. Let $(X, \mathcal{B})$ be a Steiner triple system of order v. We say that it is *cyclic* if the cyclic group $(\mathbb{F}_v, +)$ is a subgroup of the automorphism group of the pair $(\mathbb{F}_v, \mathcal{B})$. We denote such a system by $CSTS(v)$.

The existence of a Circular Steiner Triple System (CSTS) depends on congruence conditions modulo 6, as established in the following characterization (see the proof in [11]).

Theorem 3.15. *A $CSTS(v)$ exists if and only if $v \equiv 1, 3 \pmod 6$, with the exception of $v = 9$.*

We now present a construction of cyclic Steiner triple systems of order a prime power $v = p^n$ based on a $(v, 3, 1)$ difference family where $v \equiv 1 \pmod 6$ (see the proof in [12]).

Theorem 3.16. *Let $v = 6m + 1$ be a prime power with $m \geq 1$, and let α be a primitive root of the finite field $\mathbb{F}_v$. Then the blocks*

$$\{\alpha^0, \alpha^{2m}, \alpha^{4m}\}, \dots, \{\alpha^i, \alpha^{2m+i}, \alpha^{4m+i}\}, \dots, \{\alpha^{m-1}, \alpha^{3m-1}, \alpha^{5m-1}\}$$

for $0 \leq i \leq m-1$ form a $(v, 3, 1)$ difference family. Therefore, these blocks and their development define a $CSTS(6m + 1)$, that is, a 2-$(6m + 1, 3, 1)$ design.

Recall that an element α is a *primitive root* modulo a natural number v if α generates the multiplicative group $\mathbb{F}_v^*$. That is, for every $x \in \mathbb{F}_v^*$, there exists $k \in \mathbb{N}$ such that $\alpha^k \equiv x \pmod v$. The group $\mathbb{F}_v^*$ consists of all invertible elements modulo v, and its order is

$$\phi(v) = v \prod_{p \mid v} \left(1 - \frac{1}{p}\right).$$

If v is a prime power, then clearly $\phi(v) = |\mathbb{F}_v^*| = v - 1$. Hence, $\mathbb{F}_v^*$ is cyclic and has order $v - 1 = p^n - 1 = 6m$, where p is a prime with $p \equiv 1 \pmod 6$. Let α be a generator of this group. Then, if we define $x = \alpha^{2m}$, we observe that

$$x^3 - 1 = (x - 1)(x^2 + x + 1) \equiv 0 \pmod{p^n},$$

which implies $\alpha^0 + \alpha^{2m} + \alpha^{4m} \equiv 0 \pmod{p^n}$ since $\alpha^{2m} - 1$ is not a zero divisor.

The following construction provides a method to generate a CSTS of order $6m+1$ using the multiplicative structure of finite fields. The approach relies on carefully chosen initial blocks and their development under the action of the cyclic group $\mathbb{F}_v^*$.

ALGORITHM 3.17. Let $(X, \mathcal{B})$ be a design where $X = \mathbb{F}_v^*$ and $\alpha^{2m} - 1 = \alpha^t$. We define the block

$$B_0 = \{\alpha^0, \alpha^{2m}, \alpha^{4m}\} = \{1, \alpha^{2m}, \alpha^{4m}\}.$$

To compute the pairwise differences within B_0, recall that since the order of $\mathbb{F}_v^*$ is $6m$, then $\alpha^{6m} = 1$ and $\alpha^{3m} = -1$. Thus,

$$\begin{aligned}
\alpha^{2m} - 1 &= \alpha^t \\
\alpha^{4m} - 1 &= \alpha^{4m}(1 - \alpha^{2m}) = \alpha^{4m}(-\alpha^t) = \alpha^{3m}\alpha^{t+4m} = \alpha^{t+m} \\
\alpha^{4m} - \alpha^{2m} &= \alpha^{2m}(\alpha^{2m} - 1) = \alpha^{2m}\alpha^t = \alpha^{t+2m} \\
1 - \alpha^{2m} &= -\alpha^t = \alpha^{3m}\alpha^t = \alpha^{t+3m} \\
1 - \alpha^{4m} &= \alpha^{4m}(\alpha^{2m} - 1) = \alpha^{t+4m} \\
\alpha^{2m} - \alpha^{4m} &= \alpha^{2m}(1 - \alpha^{2m}) = \alpha^{t+5m}
\end{aligned}$$

These six differences from B_0 form the set

$$\triangle B_0 = \{\alpha^t, \alpha^{t+m}, \alpha^{t+2m}, \alpha^{t+3m}, \alpha^{t+4m}, \alpha^{t+5m}\}.$$

Now consider the blocks $B_i = \alpha^i B_0$, for $0 \le i \le t-1$:

$$B_i = \alpha^i B_0 = \{\alpha^i, \alpha^{2m+i}, \alpha^{4m+i}\}$$

For a fixed i, the differences within B_i are:

$$\begin{aligned}
\alpha^{2m+i} - \alpha^i &= \alpha^i(\alpha^{2m} - 1) = \alpha^{t+i} \\
\alpha^{4m+i} - \alpha^i &= \alpha^i(\alpha^{4m} - 1) = \alpha^{t+m+i} \\
\alpha^{4m+i} - \alpha^{2m+i} &= \alpha^{2m+i}(\alpha^{2m} - 1) = \alpha^{t+2m+i} \\
\alpha^i - \alpha^{2m+i} &= -\alpha^{t+i} = \alpha^{t+3m+i} \\
\alpha^i - \alpha^{4m+i} &= -\alpha^{t+m+i} = \alpha^{t+4m+i} \\
\alpha^{2m+i} - \alpha^{4m+i} &= -\alpha^{t+2m+i} = \alpha^{t+5m+i}
\end{aligned}$$

Thus, the differences from B_i are

$$\triangle B_i = \{\alpha^{t+i}, \alpha^{t+m+i}, \alpha^{t+2m+i}, \alpha^{t+3m+i}, \alpha^{t+4m+i}, \alpha^{t+5m+i}\}.$$

Since $\mathbb{F}_v^*$ is cyclic and generated by α, we have

$$\bigcup_{i=0}^{t-1} \triangle B_i = \{\alpha^0, \alpha^1, \dots, \alpha^{6m-1}\} = \mathbb{F}_v^*.$$

Therefore, the set $\{B_i\}_{i=0}^{t-1}$ forms a $(v, 3, 1)$ difference family. Consequently, the translates of each block B_i are given by

$$\mathcal{T}_i = \{g + B_i : g \in \mathbb{F}_v,\ i = 0, 1, \dots, t-1\}.$$

Let $\mathcal{B}$ denote the development of this $(v, 3, 1)$ difference family, i.e., the union of all translated blocks. Then, the pair $(\mathbb{F}_v, \mathcal{B})$ is a 2-$(v, 3, 1)$ design with $v = 6m + 1$, that is, a CSTS of order $6m + 1$.

Remark 3.18. In Section 4.2.1., we construct a 2-$(13, 3, 1)$ design using this algorithm to address a problem arising in the context of secret sharing schemes.

3.3. Resolvable BIBDs

Constructing 2-resolvable designs, especially when dealing with a large number of blocks, can be challenging. This is due not only to the conditions required by a 2-design, but also to the need to partition the blocks into parallel classes, as described in Definition 2.9. To address this, we apply the *method of successive diagonals* [13] to construct resolvable designs with parameters 2-$(q^2, q, 1)$ and 2-$(q^3, q, 1)$, where q is a prime power. This elegant matrix-based approach provides both structural insight and algorithmic efficiency in constructing RBIBDs with large numbers of blocks.

In the case $v = q^2$, the parameters $(v, k, \lambda) = (q^2, q, 1)$ yield the following:

- Number of blocks:

$$b = \frac{v(v-1)}{k(k-1)} = \frac{q^2(q^2-1)}{q(q-1)} = q^2 + q.$$

- Replication number:

$$r = \frac{v-1}{k-1} = \frac{q(q^2+q)}{q^2} = q + 1.$$

Hence, the design consists of $r = q+1$ parallel classes, each containing $v/k = q$ mutually disjoint blocks of size $k = q$.

Algorithm 3.19. [Method of successive diagonals] The steps to construct the resolvable 2-$(q^2, q, 1)$ design are as follows [14]:

(1) List the elements of the set $X = \{1, 2, \ldots, q^2\}$ in increasing order, arranged row by row into a square matrix of size $q \times q$. Each row is taken as a block. This yields the first q blocks of size q, which form the first parallel class:

$$\mathcal{C}_1 = \{B_1, B_2, \ldots, B_q\}.$$

(2) Compute the transpose of the matrix A_1, denoted by $A_2 = A_1^T$. The rows of A_2 yield a second set of q mutually disjoint blocks forming the parallel class

$$\mathcal{C}_2 = \{B_{q+1}, B_{q+2}, \ldots, B_{2q}\}.$$

(3) Construct a new square matrix A_3 by taking the main diagonal of A_2 as the first row. Then, for each column of A_2, cyclically shift its entries to fill the corresponding column of A_3. Again, take the rows of A_3 as blocks to obtain a new parallel class

$$\mathcal{C}_3 = \{B_{2q+1}, B_{2q+2}, \ldots, B_{3q}\}.$$

(4) Repeat the previous step iteratively: generate A_4 from A_3, and so on, until obtaining A_{q+1}. At this point, the cycle repeats, since $A_{q+2} = A_2$.

In the case $v = q^3$, the parameters $(v, k, \lambda) = (q^3, q, 1)$ yield the following:

- Number of blocks:
$$b = \frac{v(v-1)}{k(k-1)} = \frac{q^3(q^3-1)}{q(q-1)} = q^2(q^2+q+1).$$
- Replication number:
$$r = \frac{v-1}{k-1} = \frac{q^3-1}{q-1} = q^2+q+1.$$

Thus, this is a 2-resolvable design with $r = q^2+q+1$ parallel classes, each consisting of $v/k = q^2$ mutually disjoint blocks of size $k = q$.

ALGORITHM 3.20. [An adaptation of of the method of successive diagonals] The steps to construct the 2-$(q^3, q, 1)$ resolvable design are as follows [14]:

(1) List the elements of the set $X = \{1, 2, \ldots, q^3\}$ in increasing order and arrange them row by row into a matrix A_1 of size $q^2 \times q$. Taking the rows as blocks, we obtain the first parallel class $\mathcal{C}_1$ consisting of q^2 blocks of size q.

(2) The matrix A_1 consists of q square submatrices $A_{1,1}, A_{1,2}, \ldots, A_{1,q}$, each of size $q \times q$. Apply the method of successive diagonals to each submatrix to generate q new parallel classes $\mathcal{C}_2, \mathcal{C}_3, \ldots, \mathcal{C}_{q+1}$, each with q^2 blocks. Let $A_2, A_3, \ldots, A_{q+1}$ denote the corresponding block matrices. In total, this step yields q^3 blocks. Each matrix A_i for $i = 2, \ldots, q+1$ is again composed of q submatrices $A_{i,1}, A_{i,2}, \ldots, A_{i,q}$.

(3) Construct a new matrix A_{q+2} from $A_1 = (a_{ij})$, where $i = 1, \ldots, q$ and $j = 1, \ldots, q^2$, by selecting columns with a step size of q and stacking them as follows:
$$A_{q+2} = \begin{pmatrix} a_{1,1} & a_{q+1,1} & \cdots & a_{q^2-q+1,1} \\ a_{1,2} & a_{q+1,2} & \cdots & a_{q^2-q+1,2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{q,q} & a_{2q,q} & \cdots & a_{q^2,q} \end{pmatrix}.$$
This new matrix consists of q submatrices of size $q \times q$. We apply the method of successive diagonals to each submatrix *excluding the transposition step* (step 2 of the method), since otherwise we would reproduce blocks already generated in A_2. This yields q new matrices $A_{q+2}, A_{q+3}, \ldots, A_{2q+1}$, corresponding to parallel classes $\mathcal{C}_{q+2}, \mathcal{C}_{q+3}, \ldots, \mathcal{C}_{2q+1}$, each containing q^2 blocks. Again, this step produces a total of q^3 blocks.

(4) Repeat step 3 for the matrices $A_2, A_3, \ldots, A_{q+1}$ generated in step 2. However, note that each of these matrices yields row permutations of A_{q+2}, and therefore produce the same parallel classes as those already obtained. As a result, the q redundant matrices must be discarded.

Remark 3.21. In Section 4.3.1., we demonstrate how these algorithms can be applied to solve a problem related to event organization, specifically in the context of sports scheduling. In particular, we construct a 2-$(8, 2, 1)$ resolvable design and a 2-$(4, 2, 1)$ resolvable design corresponding to the case $q = 2$.

3.4. Hadamard matrices

Hadamard matrices occupy a central role in combinatorial design theory due to their deep connections with orthogonality, error-correcting codes, and symmetric block designs. These matrices, composed solely of $+1$ and -1 entries, are defined by the property that their rows (and columns) are mutually orthogonal. Geometrically, each pair of rows represents two orthogonal vectors, while combinatorially, each pair has exactly half of their entries in common and the other half differing. This structure not only makes them fundamental in signal processing and quantum computing, but also instrumental in constructing symmetric 2-designs with particular incidence properties [15].

In this subsection, we review the key properties of Hadamard matrices and present methods for their recursive construction, particularly through the Kronecker product. We then demonstrate how these matrices can be employed to generate symmetric Hadamard designs, including families of 2-(v, k, λ) designs, by leveraging their incidence matrices. Finally, we present two classical constructions of Hadamard 2-designs, highlighting their theoretical and practical significance within the broader landscape of combinatorial designs [7].

Definition 3.22. A matrix $H = (h_{ij})$ of order $n \times n$ with $h_{ij} \in \{-1, 1\}$ is an *Hadamard matrix* of order n if it satisfies $HH^T = nI_n$, where H^T denotes the transpose of H, and I_n is the identity matrix of order n. The matrix H is said to be *normalized* if $h_{1j} = h_{i1} = 1$ for all $i, j = 1, 2, \ldots, n$.

Some important properties of an Hadamard matrix of order n are:

(1) The inner product of any two distinct rows (or columns) is zero.

(2) The inner product of a row (or column) with itself is n.

(3) Permuting rows and/or columns yields another Hadamard matrix.

(4) Multiplying any row and/or column by -1 results in another Hadamard matrix.

(5) The transpose of an Hadamard matrix is also an Hadamard matrix.

One of the most famous open problems in combinatorial design theory is the *Hadamard conjecture*, which states that an Hadamard matrix exists for every order n divisible by 4. While this conjecture remains unproven, a well-known necessary condition can be established (see the proof in [7]).

Theorem 3.23. *If there exists an Hadamard matrix of order* $n > 2$*, then* n *must be divisible by* 4.

There are several known methods for constructing Hadamard matrices of order $n > 2$. We will focus on the Kronecker product.

Definition 3.24. Let $A = (a_{ij})$ and $H = (h_{kl})$ be Hadamard matrices of orders n and m, respectively. The *Kronecker product* $A \otimes H$ is an Hadamard matrix of order $t = n \cdot m$, formed by replacing each entry a_{ij} in A with the block $a_{ij}H$.

Let H_1 be the Hadamard matrix of order t obtained from the Kronecker product $A \otimes H$. Define the recurrence:

$$\begin{cases} H_0 = H, \\ H_k = A \otimes H_{k-1}, \quad \text{for } k \geq 1. \end{cases}$$

Then, the Hadamard matrix generated at the k-th iteration has order $t \cdot 2^{k-1}$.

Definition 3.25. Let H be the normalized Hadamard matrix of order 2:

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The Kronecker product $H \otimes H$ yields an Hadamard matrix of order 4. Repeating this construction k times defines the *Sylvester matrix* of order 2^k, denoted $S(k)$. Formally,

$$\begin{cases} S(1) = H, \\ S(k) = H \otimes S(k-1), \quad \text{for } k > 1. \end{cases}$$

Definition 3.26. An *Hadamard 2-design* is any 2-(v, k, λ) symmetric design that has been derived from a normalized Hadamard matrix of order n.

Hadamard matrices play a crucial role in the construction of symmetric designs with specific parameters. The following theorems establishes that the existence of an Hadamard matrix of order $4m$ guarantees the existence of a corresponding symmetric Hadamard design (the proofs of both results can be found in [7]).

Theorem 3.27. *If an Hadamard matrix of order $4m$, with $m > 1$, exists, then a 2-$(4m-1, 2m-1, m-1)$ symmetric Hadamard design also exists.*

Theorem 3.28. *If an Hadamard matrix of order $4m$, with $m > 1$, exists, then a 2-$(4m-1, 2m, m)$ symmetric Hadamard design also exists.*

In this regard, the following algorithms outlines a construction method that utilizes an Hadamard matrix to generate a symmetric block design. By manipulating the Hadamard matrix and using a matrix of all ones, we can derive the incidence matrix for a symmetric design with specific parameters [15].

Algorithm 3.29. Let H be an Hadamard matrix of order $4m$. We take its normalized matrix and remove the first row and the first column of 1's, obtaining matrix A. Let J be a matrix of dimension $(4m-1) \times (4m-1)$, consisting entirely of 1's. We construct matrix $B = \frac{1}{2}(A + J)$, whose entries are 0's and 1's, and whose rows and columns sum to $2m - 1$. Matrix B is the incidence matrix of a 2-$(4m-1, 2m-1, m-1)$ symmetric design.

Algorithm 3.30. We take the normalized matrix H and remove its first row and column of 1's, obtaining matrix A. We construct matrix $C = \frac{1}{2}(J - A)$, which is also composed of 0's and 1's, and whose rows and columns now sum to $2m$. Matrix C turns out to be the incidence matrix of a 2-$(4m-1, 2m, m)$ symmetric design.

Remark 3.31. In Section 4.4., we present an example of how one of these algorithms can be used to address a problem involving fair assignments in evaluation systems.

3.5. Design of Experiments

One of the most impactful applications of 2-designs arises in the planning and analysis of experiments. In this context, a 2-(v, k, λ) design provides a rigorous statistical framework to assign v treatments across b blocks in such a way that ensures balanced comparisons and controlled variability [5]. We will denote by $N = vr = bk$ the *total number of observations* made in the experiment. This balance is particularly valuable when the number of treatments and experimental units is large, or when uniform precision in estimating treatment effects is desired.

The combinatorial structure of 2-designs improves the reliability and interpretability of the experimental results. Once the experimental runs are conducted, the collected data can be analyzed using analysis of variance (ANOVA), a powerful statistical tool for testing the significance of treatment and block effects.

This subsection presents the statistical model used in analyzing 2-designs, introduces the relevant ANOVA tables, and details the procedures for hypothesis testing [5]. In particular, we compute the contrast statistics to assess whether treatment or block effects are significantly different from one another, using Snedecor's F-distribution as the reference.

Given the following statistical elements:

- y_s: The sum of all experimental data,
- y_{ij}: A random variable representing the i-th observation of the j-th block,
- T_i: The adjusted total for the blocks of the i-th treatment (it satisfies the condition $\sum_{i=1}^{v} T_i = 0$),
- B_j: The adjusted total for the treatments of the j-th block (it satisfies the condition $\sum_{j=1}^{b} B_j = 0$),
- y_i: The total for the i-th treatment,
- y_j: The total for the j-th block,
- n_{ij}: Takes the value of 1 if treatment i appears in block j, and 0 otherwise,

Tables 1 and 2 show the ANOVA corresponding to the effects of treatments and blocks in a 2-(v, k, λ) design, respectively, while Tables 3 and 4 present the statistical variables used to assess the effects of these treatments and blocks in the experimental design.

Algorithm 3.32. [Hypothesis testing] The appropriate statistic for estimating the effects of treatments and/or blocks in the design, with a significance level α, follows a F-distribution (Snedecor's F distribution) with degrees of freedom $v-1$

and $N - v - b + 1$, that is, $F_{\alpha;v-1,N-v-b+1}$. The hypothesis tests are carried out as follows:

(1) The contrast statistic for the treatments is

$$F_{exp} = \frac{MST_r}{MSE},$$

where:

- $MST_r = \frac{SST_r}{v-1}$ is the mean square for treatments.
- $MSE = \frac{SSE}{N-v-b+1}$ is the mean square for experimental error.

(2) The contrast statistic for the blocks is

$$F^*_{exp} = \frac{MSB^*}{MSE^*},$$

where:

- $MSB^* = \frac{SSB^*}{b-1}$ is the mean square for blocks.
- $MSE^* = \frac{SSE^*}{N-v-b+1}$ is the mean square for experimental error.

We compare the statistics F_{exp} and F^*_{exp} with the critical value from the theoretical F-distribution with $v - 1$ and $N - v - b + 1$ degrees of freedom:

(1) If $F_{exp} < F_{v-1,N-v-b+1}$ (equality of treatment means) or $F^*_{exp} < F_{v-1,N-v-b+1}$ (equality of block means), we accept the null hypothesis H_0. In this case, we conclude that there are no significant differences between the effects of the treatments and/or blocks.

(2) If the opposite holds, we reject the null hypothesis H_0. This implies that at least two treatments and/or blocks have significantly different effects.

Source of variation	Sum of squares	Degrees of freedom	Mean squares	F-Statistic
Adjusted treatments	SST_r	$v-1$	MST_r	F_{exp}
Unadjusted blocks	SSB	$b-1$	–	–
Experimental error	SSE	$N-v-b+1$	MSE	–
TOTAL	SST	$N-1$	–	–

Table 1. ANOVA for a 2-(v,k,λ) design for the effect of treatments [5]

Source of variation	Sum of squares	Degrees of freedom	Mean squares	F-Statistic
Unadjusted treatments	SST^*_r	$v-1$	–	–
Adjusted blocks	SSB^*	$b-1$	MSB^*	F^*_{exp}
Experimental error	SSE^*	$N-v-b+1$	MSE^*	–
TOTAL	SST^*	$N-1$	–	–

Table 2. ANOVA for a 2-(v,k,λ) design for the effect of blocks [5]

Statistical variable	Formula
SST: Adjusted total sum of squares	$\sum_{i=1}^{v}\sum_{j=1}^{b} y_{ij}^2 - \frac{y_s^2}{N}$
SST_r: Adjusted sum of squares of treatments	$\frac{k}{\lambda v}\sum_{i=1}^{v} T_i^2,\quad T_i = y_i - \frac{1}{k}\sum_{j=1}^{b} n_{ij} y_j$
SSB: Unadjusted sum of squares of blocks	$\sum_{j=1}^{b} \frac{y_j^2}{k} - \frac{y_s^2}{N}$
SSE: Sum of squares of experimental error	$SST - SST_r - SSB$

Table 3. Statistical variables for the effect of treatments [5]

Statistical variable	Formula
SST: Adjusted sum of squares	$\sum_{i=1}^{v}\sum_{j=1}^{b} y_{ij}^2 - \frac{y_s^2}{N}$
SST_r^*: Unadjusted sum of squares of treatments	$\sum_{i=1}^{v} \frac{y_i^2}{r} - \frac{y_s^2}{N}$
SSB^*: Adjusted total sum of squares of blocks	$\frac{r}{\lambda b}\sum_{j=1}^{b} B_j^2,\quad B_j = y_j - \frac{1}{r}\sum_{i=1}^{v} n_{ij} y_i$
SSE^*: Sum of squares of experimental error	$SST - SST_r^* - SSB^*$

Table 4. Statistical variables for the effect of blocks [5]

REMARK 3.33. In Section 4.5.1., we present a real-world application from agricultural experimentation, where a cotton industry aims to evaluate the impact of different fertilizers on seed yield. Due to practical constraints, the experiment cannot be conducted under fully randomized conditions. Instead, a 2-$(7,4,2)$ symmetric design is used to control for block effects and ensure fair comparisons. This case illustrates how combinatorial designs can be applied to construct statistically sound experimental plans under resource limitations.

4. Applications for teaching

4.1. Error detection codes

Error detection codes are schemes used to identify alterations in data during transmission or storage. These codes enable the detection of errors without necessarily correcting them, thereby ensuring the integrity of the information before it is used [3].

In the classroom, this context provides an excellent opportunity to introduce advanced concepts in combinatorics, group theory, design theory, and information theory through a concrete and motivating application. In addition, error detection codes offer an outstanding platform for developing mathematical modeling skills, allowing students to connect real-world problems with formal mathematical solutions.

Therefore, their study not only strengthens competencies in discrete mathematics and information theory but also provides students with a deep understanding of the importance of reliability and accuracy in digital systems—skills that are essential in the modern world, where secure data transmission is a central concern.

4.1.1. Practical example

In space missions, probes that transmit information back to Earth often face challenges due to transmission interference or the extreme conditions of space. These factors can lead to data loss or the incorrect reception of information. To prevent the loss or corruption of data, probes incorporate error correction codes during transmission.

Suppose we want to design an information encoding system for data transmission from a space probe. Specifically, the goal is to transmit 9 different messages, each represented by a sequence of bits. The objective is to organize these messages into blocks in such a way that every pair of messages appears in exactly 3 blocks.

This ensures that any loss or alteration of bits can be either corrected or detected upon reception of the data on Earth. In this way, the correct message can always be recovered by analyzing the repetitions of the messages in the remaining blocks. This can be organized by constructing a 2-$(9,3,3)$ design using the Kramer-Mesner Theorem, based on a permutation group derived from the symmetric group S_9.

This design was already constructed in [16] by considering the permutation $\alpha = (012345)(678)$. In this context, let $\mathbb{Z}_9 = \{0,1,2,\ldots,8\}$, we study the group generated by α, denoted by

$$G = \langle\alpha\rangle = \{\alpha^l : 0 \le l \le 5\},$$

which gives:

$$\begin{aligned}
\alpha^0 &= (0)(1)(2)(3)(4)(5)(6)(7)(8)\\
\alpha^1 &= (012345)(678)\\
\alpha^2 &= (024)(135)(678),\\
\alpha^3 &= (03)(14)(25)(6)(7)(8)\\
\alpha^4 &= (042)(153)(678)\\
\alpha^5 &= (054321)(678)
\end{aligned}$$

The 2-orbits of $\mathbb{Z}_9$ under α are

$$\begin{aligned}
&\mathcal{P}_1 = \{01,12,23,34,45,50\} && \mathcal{P}_2 = \{02,13,24,35,40,51\}\\
&\mathcal{P}_3 = \{03,14,25\}, && \mathcal{P}_4 = \{67,78,86\}\\
&\mathcal{P}_5 = \{06,17,28,36,47,58\} && \mathcal{P}_6 = \{07,18,26,37,48,56\}\\
&\mathcal{P}_7 = \{08,16,27,38,46,57\}
\end{aligned}$$

and the 3-orbits:

$$\begin{aligned}
&\mathcal{O}_1 = \{012,123,234,345,450,501\} && \mathcal{O}_2 = \{013,124,235,340,451,502\}\\
&\mathcal{O}_3 = \{014,125,230,341,452,503\} && \mathcal{O}_4 = \{024,135\}\\
&\mathcal{O}_5 = \{678\} && \mathcal{O}_6 = \{016,127,238,346,457,508\}\\
&\mathcal{O}_7 = \{017,128,236,347,458,506\} && \mathcal{O}_8 = \{018,126,237,348,456,507\}\\
&\mathcal{O}_9 = \{026,137,248,356,407,518\} && \mathcal{O}_{10} = \{027,138,246,357,408,516\}
\end{aligned}$$

$\mathcal{O}_{11} = \{028, 136, 247, 358, 406, 517\}$ $\mathcal{O}_{12} = \{036, 147, 258\}$
$\mathcal{O}_{13} = \{037, 148, 256\}$, $\mathcal{O}_{14} = \{038, 146, 257\}$
$\mathcal{O}_{15} = \{067, 178, 286, 367, 478, 586\}$ $\mathcal{O}_{16} = \{078, 186, 267, 378, 486, 567\}$
$\mathcal{O}_{17} = \{086, 167, 278, 386, 467, 578\}$

Consequently, the Kramer-Mesner matrix $A_{3,2}$ has dimension 17×7. To compute the entry (i, j) of this matrix, we fix a representative of the j-th 2-orbit and count how many elements of the i-th 3-orbit contain it. For instance, to compute entry $(1, 1)$, we fix the pair 01 and observe that it appears in the blocks $\{012, 501\}$ of $\mathcal{O}_1$. Therefore, $A_{3,2}(1, 1) = 2$. All other entries can be computed similarly, resulting in the matrix shown in Table 5.

	(01)	(02)	(03)	(67)	(06)	(07)	(08)
(012)	2	1	0	0	0	0	0
(013)	1	1	2	0	0	0	0
(014)	1	1	2	0	0	0	0
(024)	0	1	0	0	0	0	0
(678)	0	0	0	1	0	0	0
(016)	1	0	0	0	1	0	1
(017)	1	0	0	0	1	1	0
(018)	1	0	0	0	0	1	1
(026)	0	1	0	0	1	1	0
(027)	0	1	0	0	0	1	1
(028)	0	1	0	0	1	0	1
(036)	0	0	1	0	1	0	0
(037)	0	0	1	0	0	1	0
(038)	0	0	1	0	0	0	1
(067)	0	0	0	2	1	1	0
(013)	0	0	0	2	0	1	1
(013)	0	0	0	2	1	0	1

Table 5. Kramer-Mesner matrix

Each solution to the matrix equation $\mathbf{z}A_{3,2} = \lambda \mathbf{u}^t$ implies the existence of a 2-design on the set $\mathbb{Z}_9$. Below, we present the possible solutions to this matrix equation, generated using the following Python code (obtained from [16]):

```
import numpy as np

# Define the matrix from the system
matrix = np.matrix([
   [2, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0],
   [1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0],
   [0, 2, 2, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0],
   [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2],
   [0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1],
   [0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1],
   [0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1]
], dtype='int16')
```

```
# Vector to enforce conditions z4 = z5 = 1
vecCond = np.zeros((7,1), dtype="int16")
vecCond[1,0] = 1
vecCond[3,0] = 1

counter = 0
max = (2**15)-1
while counter <= max:
  # Loop through all possible binary vectors of length 15
  vecSol = np.array([list(np.binary_repr(counter, 15))], dtype="int16").T

  # Multiply and define lambda vector
  vecRes = matrix * vecSol + vecCond
  lam = np.full((7,1), vecRes[0])

  # Check if solution is valid
  if np.all(np.array(lam == vecRes)) == True:
    print("Solution:  \n")
    print("Vector:")
    print(np.transpose(vecSol))
    print("Lambda value:  " + str(lam[0]))
    print("\n###############################################\n")

    counter += 1
```

For $\lambda = 3$, a solution to the matrix equation $\mathbf{z}A_{3,2} = 3\mathbf{u}^t$ is given by the vector

$$\mathbf{z} = (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0).$$

Note that the conditions $z_4 = 1$ and $z_5 = 1$ must be imposed on the resulting system of equations, since it is clear that the blocks from the 3-orbits $\mathcal{O}_4$ and $\mathcal{O}_5$ will be part of the design. This is due to the fact that there are no other 3-orbits of length 1 or 2 apart from the ones indicated. This solution gives rise to a 2-$(9, 3, 3)$ design whose blocks correspond to the triples in the 3-orbits $\mathcal{O}_i$, for $i = 3, 4, 5, 7, 8, 11, 14, 15$.

4.2. Secret Sharing Schemes

In environments where security and shared responsibility are paramount, it is essential to implement mechanisms that prevent reliance on a single individual. In this context, secret sharing schemes provide an effective solution for distributing authority among multiple participants, ensuring both confidentiality and resilience against faults or malicious behavior.

Such schemes extend beyond financial applications and are well-suited for distributed trust systems, critical infrastructure access, and collaborative control protocols, where it is desirable, or necessary, that a specific subset of users jointly authorize sensitive or irreversible actions. Furthermore, their combinatorial foundation allows the design of systems that are not only secure but also auditable and mathematically verifiable.

Beyond its theoretical interest, this property provides a valuable opportunity to introduce key concepts from combinatorics, design theory, and information security through a practical and relatable real-world scenario. In an educational context, employing such a scheme allows students to connect abstract mathematical ideas with real-life applications, such as secure authorization in banking systems.

The structure of the STS supports the exploration of concepts like pairwise coverage, fairness in participation, and distributed access control. Moreover, it promotes critical thinking and mathematical modeling, making it an effective pedagogical tool for teaching advanced curriculum topics from an applied and interdisciplinary perspective.

4.2.1. Practical example

Large financial transactions carried out within a given banking institution must be confirmed simultaneously by several individuals due to the high level of responsibility involved. The execution of the operation does not depend on a single person; rather, multiple professionals must agree to carry out the transaction [4].

Suppose a bank employs 13 individuals responsible for authorizing transactions above a certain threshold (e.g., several million euros). To complete any such transaction, it is required that 3 of these 13 individuals confirm it simultaneously. Each person holds a segment of a code; therefore, the code segments of 3 individuals are needed to complete the transaction.

Since there are $\binom{13}{3} = 286$ possible combinations, it is reasonable to restrict the number of confirmations assigned to each individual. Once all combinations have been used, new code segments are distributed for future transactions.

This problem can be addressed using a 2-$(13, 3, 1)$ design. We organize the $v = 13$ individuals into $b = 26$ blocks of size $k = 3$. In this way, each person is involved in $r = 6$ confirmation groups. It is sufficient for any 2 individuals to agree and persuade a third to authorize the operation, since there will be exactly $\lambda = 1$ block containing those two individuals.

We construct a cyclic Steiner triple system of order 13 from a $(13, 3, 1)$ difference family. Since $v = 6m + 1 = 13$, it follows that $m = 2$.

We begin by identifying the primitive roots modulo 13. We factor the order of the multiplicative group $\mathbb{F}_{13}^*$, which is $|\mathbb{F}_{13}^*| = 12 = 2^2 \cdot 3$. To determine whether an element $\alpha \in \mathbb{F}_{13}$ is a primitive root modulo 13, it suffices to check that α does not satisfy any of the following congruences:

$$\alpha^2 \equiv 1 \pmod{13}, \;\; \alpha^3 \equiv 1 \pmod{13}, \;\; \alpha^4 \equiv 1 \pmod{13}, \;\; \alpha^6 \equiv 1 \pmod{13}.$$

Let us test $\alpha = 2$:

$$2^2 \equiv 4 \pmod{13}, \;\; 2^4 \equiv 3 \pmod{13}, \;\; 2^6 \equiv 12 \pmod{13}.$$

Since none of these are congruent to 1, we conclude that $\alpha = 2$ is a primitive root modulo 13. The same holds for $\alpha = 6$, $\alpha = 7$, and $\alpha = 11$, as they also satisfy none of the above congruences, and are therefore primitive roots.

Let $m = 2$ and choose $\alpha = 2$. The set $\mathcal{F} = \{B_i\}_{i=0}^{t-1} = \{B_0, B_1\}$, where:

$$B_0 = \{1, \alpha^{2m}, \alpha^{4m}\} = \{1, 2^4, 2^8\} = \{1, 3, 9\}$$
$$B_1 = \{\alpha, \alpha^{2m+1}, \alpha^{4m+1}\} = \{2, 2^5, 2^9\} = \{2, 6, 5\}$$

is a $(13, 3, 1)$ difference family.

The translates of B_0 and B_1 form the following sets:

$$
\begin{array}{ll}
T_1 = \{1,3,9\} & T_{14} = \{2,6,5\} \\
T_2 = \{2,4,10\} & T_{15} = \{3,7,6\} \\
T_3 = \{3,5,11\} & T_{16} = \{4,8,7\} \\
T_4 = \{4,6,12\} & T_{17} = \{5,9,8\} \\
T_5 = \{5,7,0\} & T_{18} = \{6,10,9\} \\
T_6 = \{6,8,1\} & T_{19} = \{7,11,10\} \\
T_7 = \{7,9,2\} & T_{20} = \{8,12,11\} \\
T_8 = \{8,10,3\} & T_{21} = \{9,0,12\} \\
T_9 = \{9,11,4\} & T_{22} = \{10,1,0\} \\
T_{10} = \{10,12,5\} & T_{23} = \{11,2,1\} \\
T_{11} = \{11,0,6\} & T_{24} = \{12,3,2\} \\
T_{12} = \{12,1,7\} & T_{25} = \{0,4,3\} \\
T_{13} = \{0,2,8\} & T_{26} = \{1,5,4\}
\end{array}
$$

The first column lists the translates of B_0, while the second contains the translates of B_1. The development of $\mathcal{F}$, denoted by $\mathcal{B}$, is the union of all these blocks. Hence, the pair $(\mathbb{F}_{13}, \mathcal{B})$ forms a 2-$(13,3,1)$ design, or equivalently, an $STS(13)$.

Moreover, observe that adding 1 modulo 13 to each element in any block results in another block of the design. Thus, the design is invariant under cyclic shifts, and we conclude that it is a $CSTS(13)$. Naturally, if we choose a different primitive root of 13, such as $\alpha = 6$, $\alpha = 7$, or $\alpha = 11$, we will obtain other, distinct designs.

By labeling each individual with a number from 0 to 12, we observe, for instance, that individuals 8 and 10 occur together in exactly one triple (the $\mathbb{T}_8$ one). Consequently, they only need to coordinate with individual 3 to complete the code, thus enabling them to execute the transaction.

This approach ensures a uniform and controlled coverage of collaborative possibilities, resulting in a robust and equitable system for joint decision-making.

4.3. Combinatorial approaches to activity scheduling

Efficient scheduling of activities in contexts involving multiple participants and logistical constraints is a common problem across many domains, from tournament organization to shift or task allocation. In such scenarios, one of the main challenges lies in equitably distributing interactions among individuals, while adhering to conditions such as the maximum number of encounters per day, full coverage of possible pairings, or the total duration of the event [17].

Combinatorial design theory, and in particular resolvable designs, provides a powerful mathematical framework for addressing these challenges. These designs allow for the structuring of sets of elements into blocks that satisfy specific coverage and partition properties, which is especially useful when a system needs to be decomposed into phases or days with mutually exclusive tasks.

From a pedagogical perspective, such applications enable students to connect abstract concepts with practical problems of organization and management. Moreover, they foster the development of skills such as logical reasoning, algorithmic thinking, and decision-making based on mathematical structures, thereby contributing to a deeper and more contextualized understanding of mathematics.

4.3.1. Practical example

Every year a chess championship is organized at regional level, in which only 8 players participate (one representative from each province). The championship is divided into 3 rounds: the elimination round, the semifinals, and the final. The 4 players who win the most games in the first elimination round will advance to the semifinals.

In case of a tie, the player who has made the fewest checks will advance, and if there is still a tie, the player who has taken the least amount of time to defeat their opponent will proceed. The same criteria will be applied to determine the 2 players who will compete in the final. Let us assume that each participant can play at most 2 times in a single day.

In order to organize a possible timetable for this championship, it must be taken into account that each of the 8 players must play against each of their opponents once in the first elimination round, we need to construct a 2-$(8, 2, 1)$ resolvable design. To solve it, we will use the Algorithm 3.20 taking $q = 2$.

We first find the matrices A_1 (step 1), A_2, and A_3 (step 2):

$$A_1 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \\ 7 & 8 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & 3 \\ 2 & 4 \\ 5 & 7 \\ 6 & 8 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} 1 & 4 \\ 2 & 3 \\ 5 & 8 \\ 6 & 7 \end{pmatrix}.$$

Next, we perform step 3 with the matrix A_1. We obtain the matrices A_4 and A_5:

$$A_4 = \begin{pmatrix} 1 & 5 \\ 2 & 6 \\ 3 & 7 \\ 4 & 8 \end{pmatrix}, \qquad A_5 = \begin{pmatrix} 1 & 6 \\ 2 & 5 \\ 3 & 8 \\ 4 & 7 \end{pmatrix}.$$

We then repeat step 3, but now with the matrices A_2 and A_3 from step 2 (step 4). In this way, we obtain the matrices A_6, A_7, A_8, and A_9:

$$A_6 = \begin{pmatrix} 1 & 5 \\ 3 & 7 \\ 2 & 6 \\ 4 & 8 \end{pmatrix}, \qquad A_7 = \begin{pmatrix} 1 & 7 \\ 3 & 5 \\ 2 & 8 \\ 4 & 6 \end{pmatrix}, \qquad A_8 = \begin{pmatrix} 1 & 5 \\ 4 & 8 \\ 2 & 6 \\ 3 & 7 \end{pmatrix}, \qquad A_9 = \begin{pmatrix} 1 & 8 \\ 4 & 5 \\ 2 & 7 \\ 3 & 6 \end{pmatrix}.$$

Note that the matrices A_6 and A_8 are obtained by permuting the rows of matrix A_4. Therefore, we discard them, as otherwise we would get repeated parallel classes.

We are left with the matrices A_1, A_2, A_3, A_4, A_5, A_7, and A_9. Considering the rows of each of these matrices as blocks, we obtain $r = q^2 + q + 1 = 7$ parallel classes, each consisting of $q^2 = 4$ mutually disjoint blocks, each containing $q = 2$ elements.

$$\begin{aligned}
\mathcal{C}_1 &= \big\{\{1,2\},\{3,4\},\{5,6\},\{7,8\}\big\}\\
\mathcal{C}_2 &= \big\{\{1,3\},\{2,4\},\{5,7\},\{6,8\}\big\}\\
\mathcal{C}_3 &= \big\{\{1,4\},\{2,3\},\{5,8\},\{6,7\}\big\}\\
\mathcal{C}_4 &= \big\{\{1,5\},\{2,6\},\{3,7\},\{4,8\}\big\}\\
\mathcal{C}_5 &= \big\{\{1,6\},\{2,5\},\{3,8\},\{4,7\}\big\}\\
\mathcal{C}_6 &= \big\{\{1,7\},\{3,5\},\{2,8\},\{4,6\}\big\}\\
\mathcal{C}_7 &= \big\{\{1,8\},\{4,5\},\{2,7\},\{3,6\}\big\}
\end{aligned}$$

Thus, the pair $(X, \mathcal{B})$ consisting of $X = \{1, 2, \dots, 8\}$ and $\mathcal{B} = \{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_7\}$ is a 2-$(8, 2, 1)$ resolvable design, where $|X| = q^3 = 8$ and $|\mathcal{B}| = q^2(q^2 + q + 1) = 28$. Note also that the union of the blocks from each parallel class is the set X.

Since each participant can play at most 2 times in a single day, the first elimination round will last 4 days; the first three days will feature 2 games each, and on the fourth day only 1 game will be played (in total, each player will play 7 games). The 4 best players from the first round will advance to the semifinals.

Let us assume that the players advancing to the semifinals are 3, 5, 6, and 8. We now need to construct a 2-$(4, 2, 1)$ resolvable design to organize the semifinals. This will be done using the method of successive diagonals (3.19):

$$A_1 = \begin{pmatrix} 3 & 5 \\ 6 & 8 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 3 & 6 \\ 5 & 8 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} 3 & 8 \\ 5 & 6 \end{pmatrix}.$$

This results in the following blocks distributed across 3 parallel classes:

$$\mathcal{C}_1 = \big\{\{3,5\},\{6,8\}\big\}, \quad \mathcal{C}_2 = \big\{\{3,6\},\{5,8\}\big\}, \quad \mathcal{C}_3 = \big\{\{3,8\},\{5,6\}\big\}.$$

As before, since each player can only play a maximum of 2 games per day, the semifinal will last 2 days; on the first day, 2 games will be played, and on the second day, only 1 game will be played (in total, each player will play 3 games). Finally, the 2 best players from the semifinals will advance to the final. Let us assume that these players are 3 and 8. We conclude that the championship will last 7 days: 4 (elimination round) + 2 (semifinal) + 1 (final). A possible schedule for the championship is as follows:

- Elimination Round Day 1: $\{1,2\},\{3,4\},\{5,6\},\{7,8\},\{1,3\},\{2,4\},\{5,7\},\{6,8\}$.
- Elimination Round Day 2: $\{1,4\},\{2,3\},\{5,8\},\{6,7\},\{1,5\},\{2,6\},\{3,7\},\{4,8\}$.
- Elimination Round Day 3: $\{1,6\},\{2,5\},\{3,8\},\{4,7\},\{1,7\},\{3,5\},\{2,8\},\{4,6\}$.
- Elimination Round Day 4: $\{1,8\},\{4,5\},\{2,7\},\{3,6\}$.
- Semifinal Day 5: $\{3,5\},\{6,8\},\{3,6\},\{5,8\}$.
- Semifinal Day 6: $\{3,8\},\{5,6\}$.
- Final Day 7: $\{3,8\}$.

4.4. *Fair allocations in evaluation systems*

Mathematics, beyond its theoretical development, finds powerful applications in the efficient and equitable organization of complex human activities. In contexts such as competitions, or evaluations, combinatorial designs can be used to ensure that all parties involved are treated fairly and that practical constraints are respected. Through the study of these methods, students can appreciate the utility of mathematics as a language that allows for modeling real-life situations in a logical, fair, and efficient manner, particularly those involving resource distribution, task allocation, and fair decision-making [18].

4.4.1. *Practical example*

At a national wine fair, the country's 7 best wineries present their wines for competition. A panel of 7 professional sommeliers has been selected to judge which winery will be awarded the prize for the best wine in the country and thus qualify for the international wine fair. As a general rule in wine competitions, a professional taster may not sample more than 4 different wines, and must wait a reasonable period between tasting.

Therefore, the panel must be organized so that each sommelier evaluates exactly 4 different wines, with the additional condition that exactly 2 of the wines are to be evaluated by 2 different sommeliers each. To ensure fairness, the tasting will be conducted blindly, that is, each sommelier will not know the identity of the winery associated with any wine they taste.

One possible solution to this problem is a 2-$(7,4,2)$ symmetric design. We label each wine with a number from 1 to 7, obtaining the set $X = \{1,2,\dots,7\}$ consisting of the $v = 7$ wines to be evaluated. Similarly, the $b = 7$ sommeliers will be identified with labels from the letters A to G. Each of them is assigned a block containing the $k = r = 4$ different wines they are to evaluate. With this setup, it follows from Theorem 2.4 that $\lambda = 2$, meaning that any pair of wines will be jointly evaluated by exactly 2 sommeliers. To construct such a design, we can use an Hadamard matrix of order 8 as a supporting structure.

Let H be the normalized Hadamard matrix of order 2, or equivalently, the Sylvester matrix $S(1)$,

$$H = S(1) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

By Definition 3.25, we obtain:

$$S(2) = H \otimes S(1) = \begin{pmatrix} S(1) & S(1) \\ S(1) & -S(1) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$S(3) = H \otimes S(2) = \begin{pmatrix} S(2) & S(2) \\ S(2) & -S(2) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

The Sylvester matrix of order 3, $S(3)$, is the normalized Hadamard matrix of order 8 that we were looking for. According to Algorithm 3.30, let J be the 7×7 matrix whose entries are all 1, and let A be the matrix obtained by deleting the first row and the first column of $S(3)$.

We then compute the matrix $C = \frac{1}{2}(J - A)$. This is equivalent to replacing all -1's in A by 1, and all 1's by 0, or equivalently, flipping all 0's and 1's in the complementary matrix B. The resulting incidence matrix is:

$$C = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

The matrix C is the incidence matrix of a $(X, \mathcal{B})$ design, where $X = \mathbb{F}_8 \setminus \{0\}$ and the set of blocks is

$$\mathcal{B} = \{\{1,3,5,7\},\ \{2,3,6,7\},\ \{1,2,5,6\},\ \{4,5,6,7\},\ \{1,3,4,6\},\ \{2,3,4,5\},\ \{1,2,4,7\}\}.$$

For instance, the sommelier labeled with the letter A will taste wines 1, 3, 5, and 7 ($k = 4$); wine 2 will be evaluated by sommeliers B, C, F, and G ($r = 4$); and wines 2 and 7 will be assessed by sommeliers B and G ($\lambda = 2$).

4.5. Designs for controlled experiments

In the field of scientific experimentation, one of the main challenges is isolating the effect of different variables on the observed outcomes. To achieve this, mathematics provides fundamental tools that allow for the rigorous and controlled planning of experiments.

Experimental designs, particularly those based on combinatorial principles, make it possible to distribute treatments in a balanced manner across different conditions (such as plots or blocks), thereby minimizing bias and improving the statistical validity of the conclusions. These methods not only optimize the use of limited resources but also enable the application of robust statistical analyses to determine whether the observed effects are significant [5].

4.5.1. Practical example

A cotton industry, interested in maximizing the yield of cottonseed, aims to determine whether this yield depends on the type of fertilizer used to treat the plant. For this purpose, 7 types of fertilizers are available. Since the type of soil may also affect the seed yield, the field is divided into 7 blocks, and each block is further divided into 4 plots. Within each block, each of the four plots is treated with a different fertilizer.

However, due to the size of the blocks and limited resources, it is not possible to apply all seven fertilizers in each block. Instead, only 4 out of the 7 fertilizers can be applied in each block. At harvest time, the yield is measured as a percentage, and the observed values are shown in Table 6, where F_i indicates the fertilizer used and B_j the field block.

	B_1	B_2	B_3	B_4	B_5	B_6	B_7
F_1	96	92	94	90	98	97	91
F_2	95	90	88	99	97	95	97
F_3	100	96	93	100	98	95	94
F_4	78	82	85	79	85	80	83
F_5	75	86	91	78	89	93	87
F_6	82	88	76	84	97	72	94
F_7	85	100	97	89	91	76	95

Table 6. Yields (as percentages)

The objective is to develop an experimental design based on a 2-design that allows us to control the effects of both the type of fertilizer and the field blocks. For this purpose, we will evaluate, at a significance level of $\alpha = 0.05$, whether there are statistically significant differences between the types of fertilizers used and between the blocks of land.

We consider the set of treatments $X = \{1,2,3,4,5,6,7\}$ to be the 7 types of fertilizer used. On the other hand, let $\mathcal{B} = \{B_i : i \in X\}$ denote the set of 7 blocks into which the field is divided.

- Since each block of land is divided into 4 plots, only 4 types of fertilizer can be applied per block. Therefore, it is clear that the block size must be $k = 4$.
- Given that $b = v = 7$, we are dealing with a symmetric design. Thus, $k = r = 4$, and by Theorem 2.3, it follows that $\lambda = 2$.

Hence, the design that best fits the problem is a 2-$(7,4,2)$ symmetric design. We propose a biplane of order 2 (see construction in [19]) with blocks:

$$\mathcal{B} = \{\{1,2,4,7\},\ \{1,2,3,5\},\ \{2,3,4,6\},\ \{3,4,5,7\},\ \{1,4,5,6\},\ \{2,5,6,7\},\ \{1,3,6,7\}\}.$$

Now, in order to apply this design to our problem, we must remove from each block the fertilizer types that are not part of the corresponding block. That is, we will eliminate fertilizers 3, 5, and 6 from block B_1, fertilizers 4, 6, and 7 from block

B_2, and so on for the other blocks. The resulting data matrix is

$$M = \begin{pmatrix} 96 & 92 & - & - & 98 & - & 91 \\ 95 & 90 & 88 & - & - & 95 & - \\ - & 96 & 93 & 100 & - & - & 94 \\ 78 & - & 85 & 79 & 85 & - & - \\ - & 86 & - & 78 & 89 & 93 & - \\ - & - & 76 & - & 97 & 72 & 94 \\ 75 & - & - & 89 & - & 76 & 95 \end{pmatrix}.$$

This matrix M represents the observed yields (in percentage) for the seven different types of fertilizers applied to seven different blocks of land. For each block, only four of the seven fertilizers are used. The dashes represent the missing data for the fertilizer types that were not applied in that particular block.

Next, we will perform an analysis of variance to assess whether there are significant differences in the cotton seed yield between the different fertilizers and between the different blocks. We will consider a significance level of $\alpha = 0.05$. The results of the ANOVA will be summarized in Tables 7 and 8.

Source of Variation	Mean Square	Degrees of Freedom	Sum of Squares	F-statistic
Fertilizer	702.07	6	117.01	2.43
Blocks	339.93	6	–	–
Exper. error	723.68	15	48.25	–
Total	1764.68	27	–	–

Table 7. ANOVA Table for the Fertilizer Effect

Source of Variation	Mean Square	Degrees of Freedom	Sum of Squares	F-statistic
Fertilizer	753.93	6	–	–
Blocks	305.07	6	50.85	1.05
Exper. error	723.68	15	48.25	–
Total	1764.68	27	–	–

Table 8. ANOVA Table for the Block Effect

By comparing the calculated F-statistics with the critical values from the F-distribution table at a significance level of $\alpha = 0.05$ ($F_{0.05;6;15} = 2.79$), we can conclude, by Algorithm 3.32 that:

(1) Since $F_{\text{exp}} = 2.43 < 2.79$, we fail to reject the null hypothesis. Therefore, there are no statistically significant differences in the yield of cotton seed among the different types of fertilizer.

(2) Since $F^*_{\text{exp}} = 1.05 < 2.79$, we also fail to reject the null hypothesis. It is concluded that the effects of the plots (blocks) of land do not significantly differ from each other. That is, dividing the land into plots and using different types of fertilizer within the same block does not result in significant changes in cotton seed productivity.

5. Conclussion

The use of BIBDs in the teaching of combinatorics provides a powerful and engaging pedagogical tool. By connecting abstract mathematical ideas to real-world problems—such as message encryption, cybersecurity, or organizing fair tournaments—students are encouraged to build a deeper, more intuitive understanding of combinatorial structures.

Through their foundation in algebraic and matrix-based concepts, including permutation groups, group actions, finite fields, and incidence matrices, BIBDs make it possible to explore advanced topics in a way that remains accessible and meaningful to learners. These connections also open the door to interdisciplinary learning, especially through links with statistics and experimental design, showing students how mathematics applies across different fields.

The approach taken in this work-blending clear theoretical development with constructive algorithms and practical examples-supports not only the development of mathematical thinking but also helps spark interest in discrete mathematics by presenting it in an applied and relevant context. In this sense, BIBDs serve as an effective educational resource for promoting active, contextualized learning in upper-level mathematics education.

REFERENCES

[1] I. Anderson, I. Honkala, *A Short Course in Combinatorial Designs*, Internet Edition, 1997.

[2] S. J. Michael Hwang, *Application of Balanced Incomplete Block Designs in Error Detection and Correction*, University of Waterloo, 2016.

[3] W.C. Guffman, V. Pless, *Fundamentals of Error-correcting Codes*, Cambridge University Press, 2003.

[4] D. Pei, *Authentication Codes and Combinatorial Designs*, CRC Press, 2006.

[5] D. C. Montgomery, *Diseño y análisis de experimentos*, Limusa Wiley, 2004.

[6] W. D. Wallis, *Introduction to Combinatorial Design*, Chapman and Hall/CRC, 2007.

[7] D. R. Stinson, *Combinatorial Designs: Constructions and Analysis*, New York: Springer, 2004.

[8] A. Jamiu Saka, *Mutually orthogonal latin squares of constructing resolvable balanced incomplete block designs*, Fundamental Journal of Mathematics and Mathematical Sciences, **10**(1) (2018), 9–17.

[9] C. J. Colbourn, J. H. Dinitz, *Handbook of combinatorial designs (Discrete mathematics and its applications)*, Chapman and Hall/CRC, 2006.

[10] E. S. Kramer, D. M. Mesner, *t-Designs on hypergraphs*, Discrete Mathematics, **15**(3) (1976), 263–296.

[11] E. Mendelsohn, K. Phelps, A. Rosa. *Cyclic Steiner Triple Systems with Cyclic Subsystems*, Academic Press Limited, 1989.

[12] M. Hall Jr., *Combinatorial Theory*, John Wiley and Sons Inc., 1986.

[13] M. Khare, W. T. Federer, *A simple construction procedure for resolvable incomplete block designs for any number of treatments*, Biometrics Unit, New York: Cornell University, Ithaca, 1979.

[14] D. Martín-Cudero, *El triple resoluble de Kirkman: un problema con historia*, Lva2, **1**(2) (2024), 31–42.

[15] S. Kumar, P. L. Sharma, *Balanced incomplete block design using Hadamard rhotrices*, International J. Technology, **4**(1) (2014).

[16] D. Martín-Cudero, Á. Carballeira. *El teorema de Kramer-Mesner: caracterización de 2-diseñs mediante sistemas de ecuaciones diofánticas*, La Gaceta de la RSME, **27**(2) (2024), 259–284.

[17] T. Shekar Goud, N. Ch. Bhatra Charyulu, *Construction of balanced incomplete block designs*, International Journal of Mathematics and Statistics Invention (IJMSI), **4**(1) (2016), 9–11.

[18] J. L. Gross, *Combinatorial Methods with Computer Applications (Discrete Mathematics and Its Applications*, Chapman and Hall/CRC, 2007.

[19] L. M. Baten, *Combinatorics of Finite Geometries*, Cambridge University Press, 2008.

Area of Mathematics Education, Rey Juan Carlos University, Madrid, Spain

ORCID: 0009-0007-5946-6744

E-mail: daniel.mcudero@urjc.es

Received: 22.05.2025, *in revised form*: 24.06.2025

Accepted: 26.06.2025