Ideal Secret Sharing Schemes over Small Domains

Amos Beimel[1], Aner Ben-Efraim[2], Oriol Farràs[3], and Adriana Moya[3]

[1] Ben Gurion University, Beer-Sheva
[2] Ariel University, Ariel
[3] Universitat Rovira i Virgili, Tarragona
amos.beimel@gmail.com, anermosh@post.bgu.ac.il,
{oriol.farras,adriana.moya}@urv.cat

Abstract. In any secret sharing scheme, the size of each share must be at least as large as the size of the secret. Schemes that attain this lower bound are called k-ideal, where k is the size of the domain of the secrets and shares, or simply ideal if they are k-ideal for some k. An access structure is called k-ideal if it admits a k-ideal secret sharing scheme. The characterization of ideal access structures is a longstanding open problem at the intersection of cryptography, matroid theory, and information theory, previously solved only for $k = 2$ and $k = 3$.
In this work, we solve this problem for $k = 4$ and $k = 6$. Our results exploit the connections between ideal secret sharing schemes and matroids and new techniques based on latin squares. For $k = 4$, we show that an access structure is 4-ideal if and only if it admits a $\mathbb{F}_4$-linear ideal secret sharing scheme, i.e., a scheme where the shares and the secret are elements of $\mathbb{F}_4$ and the sharing and reconstruction functions are linear. To prove this result, we show that the class of matroids determined by ideal $\mathbb{F}_4$-linear schemes coincides with those determined by 4-ideal schemes.
For $k = 6$, we prove that an access structure admits a 6-ideal scheme if and only if it admits a k-ideal scheme for every $k \geq 2$. This result shows that domains of size $k = 6$ are the most restrictive domains for constructing ideal secret sharing schemes, and that 6-ideal schemes can be essentially built by combining ideal $\mathbb{F}_2$-linear schemes with ideal $\mathbb{F}_3$-linear schemes via the Chinese Remainder Theorem.
Beyond these characterizations, our main technical contributions are the introduction of new techniques for analyzing ideal secret sharing schemes, extending the connections between ideal threshold schemes and latin squares to the general case, and the classification of the values of k for which some relevant matroids are k-entropic.

1 Introduction

Secret sharing schemes [Bla79,Sha79,ISN87] are a fundamental cryptographic primitive designed to protect a secret by distributing it among multiple parties. In such schemes, the secret is held by a *dealer*, who privately distributes one share of the secret to each party in such a way that some predefined subsets, called *authorized*, can recover the secret, while all other sets obtain no

information about the secret (in the information-theoretic sense). The collection of the authorized subsets is called the *access structure* of the scheme. Secret sharing schemes have been widely used to prevent both the disclosure and loss of sensitive information in numerous cryptographic applications, such as multiparty computation [BGW88,CCD88,CDM00], threshold cryptography [DF92], and attribute-based encryption [GPSW06,Wat11] (see [Bei25], for example, for a survey of such applications).

For a secret sharing scheme to be practical, the shares must be small. In any secret sharing scheme, the size of each share must be at least as large as the size of the secret. Schemes where the share size achieves this lower bound with a domain of the secrets of size k are called *k-ideal*; schemes are called *ideal* if they are k-ideal for some k. An access structure is k-ideal if it admits a k-ideal scheme. In this work, we study k-ideal secret sharing schemes for general access structures and characterize the family of k-ideal access structures for $k = 4$ and $k = 6$.

We next describe some relevant previous works. Secret sharing schemes were independently introduced by Blakley [Bla79] and Shamir [Sha79] in 1979; they presented ideal schemes for (t, n)-threshold access structures. These are access structures defined on a set of n parties in which a subset is authorized if and only if its size is at least t. Their schemes are also linear, i.e., they are schemes where the shares and the secret are elements of a finite field $\mathbb{F}$, and the sharing and reconstruction functions are linear over $\mathbb{F}$. Their techniques, together with subsequent developments by Karnin, Greene, and Hellman [KGH83], present constructions of k-ideal schemes for every prime power k satisfying $k \geq n$. In [KGH83], they proved that ideal threshold secret sharing schemes are equivalent to maximal distance separable (MDS) error-correcting codes. Using this connection, the MDS conjecture [Seg55] states that for $k < n$ and $1 < t < n$, it is not possible to construct k-ideal linear schemes for (t, n)-threshold access structures, except for two well-known cases.

For the particular case of $(2, n)$-threshold access structures, Brickell and Davenport [BD91] showed that finding k-ideal schemes is equivalent to finding n mutually orthogonal latin squares (MOLS) of order k. Later, Matúš [Mat99, Example 1.5] observed that it is enough to find $n - 1$ MOLS to deduce an ideal $(2, n)$-threshold secret sharing scheme (see Construction 1.9 for more details). It is implied by the equivalence between ideal threshold secret sharing schemes and MDS codes in [KGH83] and a previous work of Singleton [Sin64]. Singleton [Sin64, Theorem 3] proved that MDS codes with length $n + 1$ and minimum distance n are equivalent to sets of $n - 1$ MOLS.

The existence of MOLS for specific orders was studied by Euler [Eul82] in the 18th century, and determining the maximum number of MOLS for a specific order k is still an open problem for almost all k.

The connection between ideal $(2, n)$-threshold schemes and MOLS can be extended to ideal (t, n)-threshold schemes and sets of $(n-1)$ t-dimensional latin hypercubes (see [Mat99, Example 1.5] and [Sin64]).

For general access structures, Brickell and Davenport [BD91] showed a fruitful connection between ideal secret sharing schemes and matroids, which are combinatorial structures that generalize linear dependency and cycles of undirected graphs. They showed that ideal secret sharing schemes determine matroids and that their access structures are completely determined by these matroids, i.e., they are the so-called ports of the matroids. In the other direction, Brickell and Davenport [BD91] proved that if an access structure is a port of an $\mathbb{F}$-linear matroid for some finite field $\mathbb{F}$ (i.e., a matroid constructed from a linear vector space over the field $\mathbb{F}$), then the access structure is ideal.

Seymour [Sey92] and Matúš [Mat93,Mat99] studied these classes of matroids and showed that not all matroids can be determined by ideal schemes; i.e., there are matroids whose ports are not ideal access structures. Simonis and Ashikhmin [SA98] showed that there are access structures that admit ideal schemes but fail to admit ideal linear schemes[4]. The class of matroids that are determined by k-ideal secret sharing schemes coincides with the class of *k-entropic* matroids. Hence, the characterization of k-ideal access structures is equivalent to the characterization of k-entropic matroids, and this is a fundamental open problem in cryptography, matroid theory, coding theory, and information theory. This is the main open problem considered in this work.

Lehman [Leh64] and Seymour [Sey76a,Sey76b] characterized the ports of binary matroids, determining the access structures that admit ideal $\mathbb{F}_2$-linear secret sharing schemes before secret sharing was introduced. Later, the family of 2-ideal access structures was independently characterized by Beimel and Chor [BC94], Matúš [Mat93], and Golić [Gol98], providing different descriptions. Similarly, the family of 3-ideal access structures was characterized by Beimel and Chor [BC94] and Matúš [Mat93]. Beyond these cases, no characterizations of the class of k-ideal access structures have been established for any other value of k. The connection between ideal secret sharing schemes and matroids allowed the design of efficient linear schemes for useful access structures (for example, [PG06,CDG+08,FMP12,FP12,FPXY14]) and has been used to identify both the inherent limitations of ideal schemes and the limitations of general schemes (for example, [BTW05,BLP08,MP10,BF20]).

The current best secret sharing schemes for general access structures have exponential share size [LV18,ABF+19,ABNP20,AN21,ABL24], and it is known that most access structures require linear schemes with exponential share size [BGW99,RBG01,BF20]. This situation motivates two lines of research that are also considered in this work. First, the identification of families of access structures that admit efficient schemes. In particular, the identification of access structures that admit ideal schemes with polynomial share size. This is very relevant for the cryptographic applications where secret sharing schemes are used as building blocks. Second, the study of the expressive power of non-linear secret sharing schemes and the possibility of constructing schemes with significantly

[4] The ideal schemes they constructed are multilinear, a generalization of linear schemes where the secret is a vector.

smaller share size. This question is relevant for applications that do not require linearity in their schemes.

1.1 Our Results

We study the construction and existence of k-ideal secret sharing schemes for general access structures. We solve this problem for $k = 4$ and $k = 6$, providing new techniques for the study of ideal schemes and presenting new results that generalize the connections between ideal schemes and latin squares. For $k = 2$, it was shown that all 2-ideal access structures admit ideal $\mathbb{F}_2$-linear schemes [BC94,Mat93,Gol98]. Therefore, in this case, it is enough to consider ideal linear schemes, and general non-linear schemes do not provide any advantage in this case. For $k = 3$, the situation is the same.

For the case of $k = 4$, there is a richer class of schemes. In addition to $\mathbb{F}_4$-linear schemes, it is also possible to construct multilinear schemes; that is, schemes in which the secret and each share are two elements in $\mathbb{F}_2$, and the shares are determined by linear mappings over $\mathbb{F}_2$. Simonis and Ashikhmin [SA98] proved that for $k = 9$, multilinear schemes are more powerful than linear ones: there exist 9-ideal multilinear schemes for access structures that do not admit ideal $\mathbb{F}_9$-linear schemes. For $k = 4$, one question was to determine if there is a gap between the access structures determined by ideal linear, ideal multilinear, and general ideal schemes. We prove the following result.

Theorem 1.1. *An access structure is 4-ideal if and only if it admits an ideal $\mathbb{F}_4$-linear secret sharing scheme.*

The proof of this result exploits the connection between ideal access structures and matroids by Brickell and Davenport [BD91] and the characterization of $\mathbb{F}_4$-linear matroids by Geelen, Gerards, and Kapoor [GGK00]. This result does not imply that all 4-ideal schemes are $\mathbb{F}_4$-linear; rather, it establishes that $\mathbb{F}_4$-linear secret sharing schemes are essentially sufficient to realize any access structure that is 4-ideal. As detailed in Section 1.3, we provide a compact characterization based on the properties of the matroids associated with these access structures. To prove this result, we develop techniques based on latin squares and latin cubes to analyze 4-ideal secret sharing schemes. To the best of our knowledge, this work is the first to use latin squares and latin cubes to analyze ideal secret sharing schemes for non-threshold access structures.

For $k = 6$, we also fully characterize the family of 6-ideal access structures. It is not possible to construct 6-ideal linear or multilinear schemes because 6 is not a prime power; however, it is possible to build schemes of different kinds. For example, if an access structure admits a 2-ideal scheme and a 3-ideal scheme, then it is possible to construct a 6-ideal scheme for the same access structure using the Chinese Remainder Theorem (see Construction 1.16). A natural question is whether there exist other 6-ideal access structures outside the intersection of the classes of 2-ideal and 3-ideal access structures. We know that for some other composite integers like $k = 10$, the answer to the analogous question is

yes: there exist 10-ideal access structures that are neither 2-ideal nor 5-ideal (see Section 1.3 for more details).

Some partial results to this question arise from other combinatorial results related to latin squares. The problem of finding 6-ideal $(2, n)$-threshold schemes is equivalent to finding a solution to the so-called 36-officers problem. Euler [Eul82] conjectured that it does not have a solution, and Tarry [Tar00] proved the conjecture. As a consequence, there do not exist 6-ideal $(2, n)$-threshold secret sharing schemes for any $n > 2$. This impossibility result only holds for $k = 2$ and $k = 6$, and so the domain $k = 6$ is very restrictive for the construction of ideal threshold schemes.

We show that $k = 6$ is also very restrictive in constructing ideal schemes for general access structures, not only for threshold access structures. Indeed, it is the most restrictive domain. We prove it in the following result.

Theorem 1.2. *An access structure is* 6*-ideal if and only if it is* 2*-ideal and* 3*-ideal. Equivalently, it is* 6*-ideal if and only if it is* k*-ideal for every* $k \geq 2$*.*

This result contrasts with known positive results for private information retrieval (PIR) encodings [Efr12,LVW17], conditional disclosure of secrets (CDS) protocols [LVW17], and secret sharing schemes for general access structures [LV18], where it is possible to construct efficient schemes by taking advantage of $\mathbb{Z}_6$ arithmetic.

We provide a compact combinatorial characterization of the class of 6-ideal access structures by characterizing the matroids associated to these access structures. To prove this result, we analyze the representations of matroids that are not 2-ideal or 3-ideal. These technical results are presented in Section 1.3.

Our work revisits connections between ideal secret sharing schemes and combinatorial structures as orthogonal arrays, latin squares, latin cubes and latin hypercubes. Using these connections, we observe that the Bush bound [Bus52] provides a slight improvement on the lower bound for the size of the share domain in ideal threshold schemes.

Theorem 1.3. *Let* $2 \leq t < n$*, and let* Σ *be a* k*-ideal* (t, n)*-threshold ideal secret sharing scheme. Then,* $k \geq \max\{t, n-t+2\}$ *if* k *is even and* $k \geq \max\{t, n-t+3\}$ *if* k *is odd.*

The improvement is for domains of size $k \geq t \geq 3$ when k is odd. The previous bound was $k \geq n - t + 2$ [KGH83, Theorem 5] (and [KN90,CCX13] for the general threshold case), but applying results on orthogonal arrays, we obtain the slightly more restrictive bound $k \geq n - t + 3$ for the case where k is odd. Note that the bounds in [KN90,CCX13] are lower bounds on the maximum domain size of the shares for general threshold schemes, meaning they also apply to non-ideal schemes with domain of secrets of size at least 2. It remains an open question whether this discrepancy between the bounds is a consequence of the ideality restriction or not.

Concurrent Work Recently, Kalantari and Khazaei [KK26] independently proved Theorem 1.1 using different techniques and computational help. [5]

1.2 Background

In this section, we provide a general introduction to the results on matroids and latin squares that are needed to present our technical contributions, described in Section 1.3. First, we give a short introduction to matroids and matroid ports. In Section 2.2 we complement it with more technical results.

Matroids. A *matroid* is a combinatorial structure generalizing linear spaces and cycles in undirected graphs. A matroid can be defined as a pair $\mathcal{M} = (E, r)$, where E is a finite set of points and $r : 2^E \to \mathbb{N}$ is a rank function that is monotone increasing, submodular, and satisfies $r(A) \leq |A|$ for every $A \in E$ (see Definition 2.4).

Example 1.4. Let $\mathbb{F}$ be a finite field and let $v_1, \ldots, v_n$ be vectors in $\mathbb{F}^m$. Define the function $r : \{1, \ldots, n\} \to \mathbb{N}$ as follows: $r(A)$ is the dimension of the span of the vectors $\{v_i : i \in A\}$. This function r satisfies the matroid axioms, and so the pair $\mathcal{M} = (\{1, \ldots, n\}, r)$ is a matroid. If a matroid $\mathcal{M}$ can be defined in this way, we say that $\mathcal{M}$ is $\mathbb{F}$-linear. △

A set A is an independent set of a matroid if $r(A) = |A|$ and it is dependent otherwise. A circuit is a minimal dependent set. A basis of a matroid is a maximal independent set; the size of all bases is $r(E)$. A port of a matroid at point e is the collection determined by the circuits that contain e; it is defined as follows:

$$\{C \setminus \{e\} : C \text{ is a circuit such that } e \in C\}.$$

Example 1.5. Let $\mathcal{M} = (E, r)$ be the matroid defined in Example 1.4. A subset $A \subseteq E$ is independent if the set of vectors $\{v_i\}_{i \in A}$ is linearly independent over $\mathbb{F}^m$. An independent set is a basis if it spans the vector subspace $V \subseteq \mathbb{F}^m$ generated by $v_1, \ldots, v_n$. △

Brickell and Davenport [BD91] proved that ideal access structures are determined by matroids; i.e., the minimal authorized subsets of an ideal access structure correspond to the circuits of a matroid containing a fixed point. In this case, we say that the access structure is a *port* of that matroid. In contrast, Seymour [Sey92] showed that not all matroids determine ideal access structures; that is, there are matroids whose ports are not ideal access structures, i.e., they do not admit ideal secret sharing schemes.

[5] Their work was posted on arXiv on August 20, 2026. Our paper has been accepted at TCC, and we submitted it on May 19, 2026, but we did not make it publicly available at that time.

For every finite field $\mathbb{F}$, there is a correspondence between connected $\mathbb{F}$-linear matroids[6] and ideal $\mathbb{F}$-linear secret sharing schemes [BD91]. A matroid $\mathcal{M} = (E, r)$ is entropic if there are some jointly distributed random variables $(S_i)_{i\in E}$ and some constant c such that $r(A) = \frac{1}{c}H((S_i)_{i\in A})$, where H is the entropy function. Connected k-entropic matroids correspond to k-ideal secret sharing schemes [Mat99]. These connections, explained in Section 2.2, are the basis of our characterization of 4-ideal and 6-ideal access structures.

Example 1.6. The uniform matroid $U_{t,n}$ is the matroid on n points, i.e., $E = \{1, \ldots, n\}$, with rank function $r(A) = \min\{t, |A|\}$. The independent sets of $U_{t,n}$ are all subsets of size at most t, the bases are the sets of size t, and the circuits are all sets of size $t+1$. The port of this matroid at point n contains the sets $C \setminus \{n\}$, where C is a circuit, i.e., the sets of size $t+1$, containing n; that is, the port is the $(t, n-1)$-threshold access structure. So, Shamir's secret sharing scheme for a $(t, n-1)$-threshold access structure [Sha79] is a k-ideal linear representation of the matroid $U_{t,n}$, and in particular, a k-entropic one. △

We end this introduction to matroids by presenting three operations that are relevant to this work. The *dual* of a matroid $\mathcal{M}$, denoted by $\mathcal{M}^*$, is the matroid whose bases are the complements of the bases of $\mathcal{M}$, i.e., the bases of $\mathcal{M}^*$ are the sets $E \setminus B$ for bases B of $\mathcal{M}$. The *deletion* and the *contraction* of $\mathcal{M}$ by $F \subset E$ are the matroids $(r_{\setminus F}, E \setminus F)$ and $(r_{/F}, E \setminus F)$ respectively, where $r_{\setminus F}$ is just the restriction of r to $E \setminus F$, and $r_{/F}$ is defined as $r_{/F}(A) = r(A \cup F) - r(F)$ for $A \subseteq E \setminus F$. If a matroid $\mathcal{M}'$ is obtained from $\mathcal{M}$ by applying deletions and contractions, we say that $\mathcal{M}'$ is a *minor* of $\mathcal{M}$.

Example 1.7. Let $\mathcal{M} = (E, r)$ be the matroid defined in Example 1.4. The matroid $\mathcal{M} \setminus \{n\}$ is the one determined by the vectors $v_1, \ldots, v_{n-1}$, and the matroid $\mathcal{M}/\{n\} = (r_{/\{n\}}, \{1, \ldots, n-1\})$, where $r_{/\{n\}}(A) = r(A) - 1$ if $v_n \in \text{span}\{v_1, \ldots, v_{n-1}\}$ and $r_{/\{n\}}(A) = r(A)$ otherwise.

Now, let $U_{t,n}$ be the uniform matroid for some $1 < t \leq n$ presented in Example 1.6. Observe that $U_{t,n} \setminus \{n\} = U_{t,n-1}$, $U_{t,n}/\{n\} = U_{t-1,n-1}$, and $U^*_{t,n} = U_{n-t,n}$. △

Latin squares. A *latin square* of order n is a $n \times n$ array such that each element of $\{0, \ldots, n-1\}$ appears exactly once within any row or column of the array. Two latin squares of order n are said to be *orthogonal* if every ordered pair of symbols occurs exactly once among the n^2 pairs. A set of more than two latin squares with the property that each pair of the set is orthogonal is called *mutually orthogonal latin squares* (MOLS).

Example 1.8. The following tables are latin squares of order 4. The latin square L_1 is the Cayley table of the sum in $\mathbb{Z}_4$, that is, if we index rows and columns

[6] A matroid is connected if, for every two points of the matroid, there is a minimal dependent set containing these points.

by $\{0,1,2,3\}$, the position (i,j) in the table represents $i+j \mod 4$.

$$L_1 = \begin{array}{c} 0\,1\,2\,3 \\ 1\,2\,3\,0 \\ 2\,3\,0\,1 \\ 3\,0\,1\,2 \end{array} \qquad L_2 = \begin{array}{c} 0\,1\,2\,3 \\ 1\,0\,3\,2 \\ 2\,3\,0\,1 \\ 3\,2\,1\,0 \end{array} \qquad L_3 = \begin{array}{c} 0\,1\,2\,3 \\ 2\,3\,0\,1 \\ 3\,2\,1\,0 \\ 1\,0\,3\,2 \end{array}$$

The latin squares L_2 and L_3 are mutually orthogonal latin squares, while the pairs L_1 and L_2 are not orthogonal (e.g., the pair $(1,1)$ appears 4 times). Similarly, L_1 and L_3 are also not orthogonal. △

Latin squares can be generalized to *latin hypercubes* of dimension d by increasing the dimension of the array and obtaining an $n \times \cdots \times n$ array such that each symbol occurs n^{d-t+1} times in each $(d-t)$-dimensional subarray for every $1 \leq t \leq d-1$.

Euler [Eul82], while studying the properties of latin squares, implicitly investigated the characterization of integers k for which there exist k-ideal $(2,n)$-threshold secret sharing schemes. In the language of secret sharing, Euler conjectured that there are no k-ideal $(2,n)$-threshold schemes when $k \equiv 2 \pmod 4$ and $n > 2$. There were no contributions to this conjecture until 1900, when Tarry [Tar00] proved the conjecture to be true for $k = 6$. However, in 1957, Bose, Shrikhande, and Parker [BSP60] proved that the conjecture fails for all other values. For a composite number k, determining the maximum value of n such that there exist k-ideal $(2,n)$-threshold schemes for a given k remains an open problem, even for small values such as $k = 10$. For more details, see [Bla99,Sti04], for example.

Brickell and Davenport [BD91, Section 6] observed that ideal $(2,n)$-threshold schemes can be constructed from n MOLS. This construction was inproved by Matúš [Mat99], who observed that by using the equivalence between ideal threshold schemes and MDS codes of [KGH83] and the fact that MDS are also related to sets of MOLS [Sin64], it is enough to have $n-1$ MOLS to deduce an ideal $(2,n)$-threshold scheme. Next, we detail how to construct an ideal $(2,n)$-threshold secret sharing scheme from a set of $n-1$ MOLS.

Construction 1.9. Let $L_1, \ldots, L_{n-1}$ be a set of $n-1$ MOLS of order k. A k-ideal secret sharing scheme for a $(2,n)$-threshold access structure is constructed as the following:

Let s be a secret and r a random element of a domain S of size k. If $1 \leq i \leq n-1$, the share s_i for the i-th party P_i is the element of the latin square L_i in the position (s,r) (the row s and the column r). While the share s_n for the n-th party P_n is the randomness r.

Privacy Every row of L_i contains all elements of S, and each element appears once. Hence, a single party cannot obtain any information about the secret.

Correctness Consider the two different classes of pairs of parties:

1. P_i and P_j with $1 \leq i,j \leq n-1$. The parties can deduce the secret because there is only one position (s,r) where the pair of shares s_i and s_j appears in the superimposition of the two latin squares L_i and L_j, by orthogonality.

2. P_i and P_n, $1 \leq i \leq n-1$. The parties can obtain the secret because the share s_i appears in a unique position in the r-th column of the latin square L_i, and this position reveals the secret s.

The connection between MOLS and $(2, n)$-threshold schemes was generalized by Martin [Mar91, Theorem 2.4.7] and Dawson, Mahmoodian, and Rahilly [DMR93, Theorem 1], showing the equivalence between (k, n)-threshold ideal schemes and orthogonal arrays (see also [Sti04, Section 11.2]).

Bounds on the share size for general (not necessarily ideal) threshold secret sharing schemes were presented in several subsequent works. Kilian and Nisan [KN90] and Cascudo, Cramer, and Xing [CCX13] showed that for any (t, n)-threshold scheme, the size of the share domain is at least $n - t + 2$, independently of the secret size (e.g., the bound holds even when the domain of secrets is of size 2). In addition, Bogdanov, Guo, and Komargodski [BGK16] showed that the share size must be at least $t + 1$.

Since there is an equivalence between maximal distance separable (MDS) and ideal linear threshold schemes [MS81], the MDS conjecture [Seg55] is highly relevant. In terms of threshold schemes, the conjecture states that for $k < n$ and $1 < t < n$, it is not possible to construct k-ideal linear schemes for (t, n)-threshold access structures, except for the well-known cases where $n = k + 1$, k is a power of 2, and $t = 3$ or $t = k - 1$. Ball [Bal12] proved that the conjecture is true for prime fields.

Ideal Schemes over Small Domains. It is well known that the size of the domain limits the expressivity of secret sharing schemes. The search for the minimum domain size k for which a k-ideal scheme exists for an access structure is a fundamental open problem in combinatorial design theory.

For $k = 2$ and $k = 3$, several works [Mat93,BC94,Gol98] have characterized k-ideal access structures. While the characterization of $\mathbb{F}_2$-linear matroids and their ports, and $\mathbb{F}_3$-linear matroids were already known (for more details, see [Leh64,Sey76a,Sey76b,Oxl11]), they showed that an access structure is 2-ideal (respectively, 3-ideal) if and only if it is a port of a linear matroid over $\mathbb{F}_2$ (respectively, $\mathbb{F}_3$). By known results from matroid theory, these results imply that an access structure is k-ideal for every $k \geq 2$ if and only if it is a port of a matroid that is linear over $\mathbb{F}_2$ and over $\mathbb{F}_3$. An alternative characterization of 2-ideal access structures was presented in [ABI+23].

For $k = 4$, Geelen, Gerards, and Kapoor [GGK00] found a characterization of all $\mathbb{F}_4$-linear matroids. The characterization is presented in terms of their forbidden minors: A matroid is $\mathbb{F}_4$-linear if and only if it excludes $U_{2,6}$, $U_{4,6}$, P_6, F_7^-, $\left(F_7^-\right)^*$, P_8, and P_8'' as minors (see Example 1.6 and Definitions 5.9, 4.5, 5.11, and 5.13 for a definition of these matroids).

For larger prime powers q, characterizations of $\mathbb{F}_q$-linear matroids are not known.

Three of the excluded minors of $\mathbb{F}_4$-representability are already known to be non 4-entropic. First, by the bounds in [KGH83,KN90,CCX13], the $(2, 5)$-

threshold access structure require shares of size at least $k \geq 5$. Since the $(2, 5)$-threshold access structure is a port of $U_{2,6}$, the matroid $U_{2,6}$ is not 4-entropic. Second, by the bound of Bogdanov, Guo, and Komargodski [BGK16], the $(4, 5)$-threshold access structure require shares of size at least $k \geq 5$; consequently, the matroid $U_{4,6}$ is not 4-entropic.

Finally, the non-Fano matroid F_7^- and its dual $\left(F_7^-\right)^*$ are known to be linearly representable over fields of odd characteristic [Oxl11]. Matúš [Mat99] showed that the non-Fano matroid is k-entropic only if k is odd. Therefore, F_7^- is not 4-entropic.

In Section B.1, we provide alternative proofs of the nonexistence of a 4-entropic representation of these three matroids, $U_{2,6}$, $U_{4,6}$, and F_7^-, using the techniques of latin squares and orthogonal arrays developed in this work.

For the rest of the forbidden minors on $\mathbb{F}_4$-representability, the matroids P_6 and P_8'' are known to be q-ideal if q is a prime power $q \geq 5$ (since they are $\mathbb{F}$-linear over any field $|\mathbb{F}| \geq 5$). The matroid P_8 is k-ideal if k is odd since it is $\mathbb{F}$-linear for any field with odd characteristic. Prior to our work, it was not known if P_6, P_8, and P_8'' are 4-entropic.

When increasing the size of k, the first known domain for which there exists a k-ideal secret sharing scheme that is not linear is for $k = 9$, with a multilinear scheme for a port of the Non-Pappus matroid [SA98]. Nevertheless, there is currently no evidence of an ideal access structure that fails to admit multilinear schemes. This motivates the following open problem.

Open Problem 1.10 ([Mat18])**.** *Are there entropic matroids that are not multilinear?*

Rota's conjecture [Rot70] states that for every prime power q, the family of $\mathbb{F}_q$-linear matroids has finitely many excluded minors. In 2014, Geelen, Gerards, and Whittle [GGW14] announced a proof of the conjecture; however, the full version of the proof was not yet published. Furthermore, their proof is non-constructive and does not give a bound on the number excluded minors for a given field. Matúš [Mat18] extended this conjecture to the family of k-entropic matroids:

Conjecture 1.11. *For every $k > 1$, the class of k-entropic matroids has finitely many excluded minors.*

An analogous conjecture can be formulated for the class of multilinear matroids, i.e., matroids that admit ideal multilinear schemes.

1.3 Our Techniques

The characterization of ideal access structures presented in this work is achieved by exploiting the connection between ideal access structures and matroids, and by developing new techniques based on latin squares.

Previous results imply sufficient conditions for the existence of k-ideal schemes for $k = 4$ and $k = 6$; namely, the sufficient condition is that the access structure

is a port of a matroid that does not have certain excluded minors. The primary technical challenge of this work was to prove that these conditions were indeed necessary. For that, we reduced this problem to the impossibility of constructing ideal schemes for some specific access structures. Our main technical contributions are these impossibility results. Specifically, we prove that the matroids associated to these access structures are not k-entropic for the chosen values of k.

The Case $k = 4$. For this case, we built upon the foundational work by Geelen, Gerards, and Kapoor [GGK00], who identified all matroids that admit linear representations over $\mathbb{F}_4$. We conjectured that this class of linear matroids coincides with the class of 4-entropic matroids. Our task was to prove that matroids that are not $\mathbb{F}_4$-linear do not admit any other type of entropic representations. By proving this claim, we arrive at the following characterization.

Theorem 1.12. *An access structure admits a 4-ideal secret sharing scheme if and only if it is a port of a matroid that excludes $U_{2,6}$, $U_{4,6}$, P_6, F_7^-, $\left(F_7^-\right)^*$, P_8, and P_8'' as minors.*

These forbidden minors are well known matroids, and all of them are entropic over other domains. While the impossibility result for $U_{2,6}$, $U_{4,6}$, and F_7^- could be derived from previous works on threshold secret sharing schemes and the work of Matúš [Mat99], the results for the remaining matroids were previously unknown.

To study the dual of the Non-Fano matroid, $\left(F_7^-\right)^*$, we use the techniques developed by Matúš in [Mat99]. This framework allows us to translate the existence of entropic representations into group-theoretic problems. By solving these problems, we show that the matroid is not entropic for $k = 4$. Furthermore, we characterize all the values of k for which it is k-entropic. A key consequence of this result is that the Non-Fano matroid F_7^- and its dual $\left(F_7^-\right)^*$ are entropic over exactly the same domains.

Theorem 1.13. *The matroid $\left(F_7^-\right)^*$ is k-entropic if and only if k is odd.*

For the matroids P_8 and P_8'', we use a completely different approach. We describe the entropic representations of matroids by means of latin squares and latin cubes. Moreover, we use an algebraic description of these combinatorial objects in terms of group operations and permutations. We use special properties of latin squares and cubes of order 4, which cannot necessarily be extended to other orders. Next, we illustrate this by showing different descriptions of a latin square.

Example 1.14. Consider the latin squares

$$L = \begin{array}{c} 0\,1\,2\,3 \\ 1\,0\,3\,2 \\ 2\,3\,0\,1 \\ 3\,2\,1\,0 \end{array} \qquad L' = \begin{array}{c} 0\,1\,2\,3 \\ 2\,3\,0\,1 \\ 1\,0\,3\,2 \\ 3\,2\,1\,0 \end{array}$$

Note that L is the addition table of the Klein group V_4 (i.e., addition in $\mathbb{Z}_2 \times \mathbb{Z}_2$). These latin squares can be described by means of two permutations τ and σ on the set $\{0,1,2,3\}$ and the group operation $\cdot$ of the Klein group V_4. For instance, if we index the rows and columns by $\{0,1,2,3\}$, the latin square L takes the value $L(i,j) = \tau(\sigma(i) \cdot j)$ with $\tau = id$ and $\sigma = id$ at the position (i,j) in the table. While the latin square L' takes the value $L'(i,j) = \tau(\sigma(i) \cdot j)$ with the permutations $\tau = id$ and $\sigma = (0)(12)(3)$ at position (i,j).

Moreover, if we identify the elements $\{0,1,2,3\}$ with the elements of the finite field $\mathbb{F}_4 = \{0,1,\alpha,\alpha+1\}$, we obtain the latin squares

$$L = \begin{array}{cccc} 0 & 1 & \alpha & \alpha+1 \\ 1 & 0 & \alpha+1 & \alpha \\ \alpha & \alpha+1 & 0 & 1 \\ \alpha+1 & \alpha & 1 & 0 \end{array}, \qquad L' = \begin{array}{cccc} 0 & 1 & \alpha & \alpha+1 \\ \alpha & \alpha+1 & 0 & 1 \\ 1 & 0 & \alpha+1 & \alpha \\ \alpha+1 & \alpha & 1 & 0 \end{array}$$

Notice that L is the Cayley table of the sum operation in $\mathbb{F}_4$. That is, if we index rows and columns by $\{0,1,\alpha,\alpha+1\}$, the entry $L(i,j)$ is the sum of the corresponding indices, i.e., $L(i,j) = i+j$. Moreover, the permutations $\tau = id$ and $\sigma = (12)$ of L' can be described as polynomials in $\mathbb{F}_4[x]$ that are the permutation polynomials $\tau(x) = x$ and $\sigma(x) = \alpha x^2$. Therefore, $L'(x,y) = \alpha x^2 + y$. △

Matroids P_8 and P_8'' have rank 4, and the impossibility result is derived by examining all potential 4-entropic representations and finding that none are possible. To achieve this, we describe a 4-entropic representation and deduce a set of latin cubes of order 4 given by the relation detailed in Lemma 2.36, where a correspondence is established between the circuits of an entropic matroid and a latin cube.

Afterwards, we translate the dependence and independence relations of the matroid into some relations of symbol-isotopy and orthogonality between the latin cubes. We apply the characterization of orthogonal latin squares in terms of its algebraic representation.

Example 1.15. Orthogonality of latin squares of order 4 can be described algebraically by means of the permutations σ that determine each latin square. For example, the latin squares

$$L_1 = \begin{array}{c} 0\,1\,2\,3 \\ 1\,0\,3\,2 \\ 2\,3\,0\,1 \\ 3\,2\,1\,0 \end{array} \qquad L_2 = \begin{array}{c} 0\,1\,2\,3 \\ 2\,3\,0\,1 \\ 3\,2\,1\,0 \\ 1\,0\,3\,2 \end{array} \qquad L_3 = \begin{array}{c} 0\,1\,2\,3 \\ 3\,2\,1\,0 \\ 1\,0\,3\,2 \\ 2\,3\,0\,1 \end{array}$$

have $\sigma_{L_1} = id$, $\sigma_{L_2} = (0)(123)$, $\sigma_{L_3} = (0)(132)$ and are mutually orthogonal. The property of being orthogonal corresponds with orthogonality of the σ's (see [Eva89] and Lemma 2.25). In particular, orthogonality of permutations of $\{0,1,2,3\}$ corresponds to having no common values other than 0. Hence, the latin squares L_1, L_2, L_3 define a complete set of MOLS. △

Using the relation illustrated at Example 1.15 and the technical lemmas Lemma 5.5, Lemma 5.6, and Lemma 5.8, we reach a contradiction: we show that it requires a set of more than 3 MOLS of order 4. This directly implies that the proposed configuration is impossible since it is a fundamental result that there exist at most $n-1$ MOLS of order n (Theorem 2.19).

The proof for P_6 follows a similar approach but requires less complex machinery because it is a matroid of rank 3. To prove the impossibility result, we argue by contradiction. We suppose that there exists a 4-entropic representation of P_6 and, from this, we obtain a set of four MOLS. Since there are at most 3 MOLS of order 4 (Theorem 2.19), we find that all 3-element sets are independent, reaching a contradiction.

In Theorem C.12, we present an alternative characterization of 4-ideal access structures in terms of their minors, i.e., we provide a complete list of the forbidden minors of the 4-ideal access structures.

The Case $k = 6$. Since 6 is not a prime power, in this case we cannot consider ideal linear schemes. However, there is a straightforward construction that relies on linear schemes. Namely, if an access structure admits a k_1-ideal scheme and a k_2-ideal scheme, for some coprime integers k_1 and k_2, it is possible to construct a k_1k_2-ideal scheme for the same access structure (via the Chinese Remainder Theorem (CRT)). Because of that, domains of ideal secret sharing schemes are multiplication closed.

Construction 1.16. Let k_1 and k_2 be two coprime integers satisfying $k_1, k_2 \geq 2$, and let Γ be an access structure on a set of parties P. For $i = 1, 2$, let Σ_i be k_i-ideal secret sharing scheme with access structure Γ. We construct a k_1k_2-ideal scheme with access structure Γ as follows.

Sharing: Given a secret $0 \leq s < k_1k_2$, the dealer computes $s_1 = s \mod k_1$ and $s_2 = s \mod k_2$. Then, the dealer shares independently s_1 and s_2 among the set of parties P with the schemes Σ_1 and Σ_2, respectively.

Reconstruction: The parties in an authorized set $A \in \Gamma$ use the reconstruction function of Σ_1 to recover s_1 from their shares, and use the reconstruction function of Σ_2 to recover s_2. Then, they recover s by applying the Chinese Remainder Theorem.

Correctness: Sets that are in Γ can recover both s_1 and s_2 by the correctness of Σ_1 and Σ_2.

Privacy: If a subset is not in Γ, then it does not have any information about s_1 nor s_2 by the privacy properties of Σ_1 and Σ_2. Since s_1 and s_2 are shared independently, a subset that is not in Γ gets no information about s.

Consequently, for $k = 6$, we know that the class of 6-ideal access structures includes the intersection of the 2-ideal and 3-ideal access structures. Our challenge was to determine if the class of 6-ideal access structures contains any additional access structures beyond this intersection. For $k = 10$ (and for many other composite numbers), the answer to the analogous question is known to

be yes: The $(2,3)$-threshold access structure is 10-ideal, even though it is not 2-ideal.

First, we described the intersection of the classes of 2-ideal and 3-ideal access structures by means of the forbidden minors of the associated matroids. A matroid is 2-entropic if and only if it does not contain $U_{2,4}$ as a minor [Mat93,BC94]. A matroid is 3-entropic if and only if it does not contain either $U_{2,5}$, $U_{3,5}$, F_7, or F_7^* as minors [Mat93,BC94]. The intersection of these two classes has only the forbidden minors $U_{2,4}$, F_7, and F_7^*, since $U_{2,4}$ is a minor of $U_{2,5}$ and $U_{3,5}$. We prove that $U_{2,4}$, F_7, and F_7^* are also the unique forbidden minors for 6-ideal access structures. For that, it was enough to prove that these matroids are not 6-entropic.

The impossibility results for $U_{2,4}$ and F_7 can be derived from previous works on threshold secret sharing schemes and the work of Matúš [Mat99]. Hence, it remains to prove that the dual of the Fano matroid, F_7^*, is not 6-entropic. To achieve this, we apply the same techniques we applied in the study of the dual of the Non-Fano matroid. We prove that the dual of the Fano matroid is not 6-entropic. Moreover, we characterize the values of k for which it is k-entropic, showing that the Fano matroid and its dual are entropic exactly over the same domains.

Theorem 1.17. *The matroid F_7^* is k-entropic if and only if $k = 2^\ell$, $\ell > 0$.*

Tutte [Tut58] showed that if a matroid is $\mathbb{F}_2$-linear and $\mathbb{F}_3$-linear, then it is linear for every finite field. Matroids satisfying this property are called *regular* (there are alternative definitions of regular matroids; see [Oxl11] for more details). Hence, as a consequence of our results, we give another characterization of regular matroids in terms of the 6-entropic ones. Since the classes of k-linear and k-entropic matroids coincide for $k = 2$ and $k = 3$, we conclude that a matroid is 6-entropic if and only if it is k-entropic for every $k \geq 2$. In terms of ideal access structures, the result is as follows.

Theorem 1.18. *An access structure admits a 6-ideal secret sharing scheme if and only if it satisfies one of the following equivalent properties:*

(i) It is a port of a matroid that excludes $U_{2,4}$, F_7, and F_7^* as minors.
(ii) It is a port of a regular matroid.
(iii) It is k-ideal for $k = 2$ and $k = 3$.
(iv) It is k-ideal for every $k \geq 2$.

In Theorem C.5, we present an alternative characterization of 6-ideal access structures in terms of their minors.

1.4 Related Work and Open Problems

Ideal Secret Sharing Schemes. For $k = 5$, we are unable to provide any significant contribution. The situation for this domain size is entirely different because the existing knowledge is much more limited. Mayhew and Royle [MR08]

enumerated all matroids on at most nine elements that are not $\mathbb{F}_5$-representable, and Brettell [Bre25] subsequently enumerated the excluded minors on 10 elements. A complete characterization remains out of reach. For all other integers $k > 6$, the characterization of k-ideal access structures is even further from realization.

For $k = 9$ [SA98] and $k = 25$ [BBFP21], there are access structures that admit k-ideal multilinear schemes but fail to admit k-ideal linear schemes. For $k = 8$, it is not known if there are ideal access structures that do not admit ideal $\mathbb{F}_8$-linear schemes.

Other techniques for proving the non-representability of matroids rely on linear information and rank inequalities, which are fundamental to linear programming methods used to bound the information ratio of secret sharing schemes (for example, [BGI+26,BLP08,FKMP20,MPY16,PVY13]). However, a major drawback of these information-theoretic approaches is that they cannot distinguish between different domain sizes, potentially yielding ideal structures that are not useful because they only admit schemes for very large secrets.

Recently, Kühne and Yashfe showed that the problem of determining whether a matroid is entropic or not is undecidable [KY26]. They also proved that determining whether a matroid is multilinear or not is undecidable [KY22].

Extension of Rota's Conjecture. As mentioned above, a fundamental question in matroid theory is whether the number of excluded minors for representability over a given finite field is finite (Rota's Conjecture [Rot70]). In the context of cryptography, we ask if Rota's Conjecture can be extended to other classes of matroids (Conjecture 1.11). Specifically, we ask if there is a finite set of excluded minors that characterizes the matroids possessing an ideal multilinear representation or those that are entropic for a specific domain.

Classes of Secret Sharing Schemes. A challenge in secret sharing involves characterizing the relative expressive power of the primary classes of secret sharing schemes: linear, multilinear, polynomial, and general. There exist access structures that admit ideal multilinear schemes but fail to admit ideal linear schemes [BBFP21,Ben16,SA98]; Furthermore, several works show the advantage of multilinear schemes in the non-ideal case [AA18,AARV21,ABF+19,BF20].

While the total number of access structures grows doubly exponentially with the number of parties, Nelson [Nel18] shows that the number of access structures admitting ideal linear schemes is only exponentially bounded. Therefore, most of the access structures do not admit ideal linear schemes, and most of the access structures require linear schemes with exponential share size [BF20]. This motivates the study of other classes of schemes that reduce the share size of linear constructions. There are no bounds on the number of multilinear matroids; the number can be anywhere between exponential and doubly exponential.

Another open question is whether there exist ideal access structures that do not admit ideal multilinear schemes. This question is closely related to Proposition 1.10 and extends naturally to fixed-domain constraints: specifically, whether

there are k-ideal structures that lack a k-ideal multilinear scheme (for a prime power k). Similarly, the separation between ideal multilinear schemes and ideal polynomial schemes of low degree [PR20,LVW17,BFM25] remains unresolved.

Duality. It is well-known in matroid theory that the dual of a linear or multilinear matroid remains linear or multilinear, respectively. This symmetry extends to the associated cryptographic primitives: the dual of an access structure admitting an ideal linear or multilinear scheme also admits a scheme of the same class. However, whether this duality closure holds for the broader class of all ideal access structures remains a significant open question. The complexity of this relationship is underscored by existing counter-examples in related domains; specifically, it has been proven that duality is not closed for matroids admitting almost entropic representations [Csi19,Kac18], nor for access structures admitting asymptotically ideal statistical schemes [BFM25]. Determining whether the property of admitting k-ideal schemes, or just ideal schemes, is invariant under duality is one of the main open problems in secret sharing.

1.5 Organization

In Section 2, we present some preliminaries on secret sharing schemes, matroids, latin squares, and orthogonal arrays. In Section 3, we prove results for threshold access structures: we prove Theorem 1.3. In Section 4, we study the case $k = 6$, proving Theorem 1.18 and, as a consequence, Theorem 1.2. Moreover, we prove Theorem 1.13 and Theorem 1.17, showing a characterization of the domains in which the Fano Dual and non-Fano Dual matroids are entropic. In Section 5, we consider the case $k = 4$ and prove Theorem 1.1, which is a consequence of Theorem 1.12.

In Appendix A, we present proofs of technical lemmas stated in Section 2.3 and Section 2.4. In Appendix B, we give alternative proofs of the entropic representations of the forbidden minors of 4 and 6 representability based on the techniques developed in this work.

In Appendix C, we provide an alternative characterization of 4-ideal and 6-ideal access structures by determining the forbidden minors of the access structures.

2 Preliminaries

We present preliminaries organized into different subsections. First, we define secret sharing schemes; then, we introduce matroids and discuss their connection with secret sharing schemes. Thereafter, we provide the definitions for orthogonal arrays and latin squares, further elaborating on their generalization into higher-dimensional latin hypercubes.

2.1 Secret Sharing Schemes

In this section, we present the definition of secret sharing schemes (from [Bei25]). Then, we introduce the family of ideal secret sharing schemes, which are the focus of this work.

Definition 2.1 (Access Structures). *Let P be a finite set of parties. A collection $\Gamma \subseteq 2^P$ is monotone if $B \in \Gamma$ and $B \subseteq C$ imply that $C \in \Gamma$. An access structure is a monotone collection $\Gamma \subseteq 2^P$ of non-empty subsets of P. Sets in Γ are called authorized, and sets not in Γ are called unauthorized.*

Definition 2.2 (Secret Sharing Schemes). *Let K be a finite set of secrets, $|K| \geq 2$. A* secret sharing scheme *is a pair $\Sigma = \langle \Pi, \mu \rangle$, where μ is a probability distribution over some finite set R, and Π is a mapping from $K \times R$ to a set of n-tuples $K_0 \times K_1 \times \cdots \times K_n$, where K_i is called the share-domain of player i. A dealer distributes a secret $s \in K$ by first computing a vector of shares $\Pi(s, r) = (\mathsf{sh}_1, \ldots, \mathsf{sh}_n)$, and then giving sh_i to party i. We say that the scheme $\Sigma = \langle \Pi, \mu \rangle$ is a secret sharing scheme realizing an access structure Γ if the following two requirements hold:*

Correctness: *For any authorized set $A \in \Gamma$, there exists a reconstruction function $\textsc{Recon}_A$ such that for every secret $s \in K$,*

$$\Pr[\textsc{Recon}_A(\Pi_A(s, r)) = s] = 1,$$

where $\Pi_A(s, r)$ is the restriction of $\Pi(s, r)$ to its A-entries.

Perfect privacy: *For any forbidden set $B \notin \Gamma$, for every two secrets $a, b \in S$, and for every possible vector of shares sh,*

$$\Pr[\Pi_B(a, r) = \mathsf{sh}_B] = \Pr[\Pi_B(b, r) = \mathsf{sh}_B].$$

where $\mathsf{sh}_B = \langle \mathsf{sh}_j \rangle_{j \in B}$.

In this work, we develop several techniques that conceive secret sharing schemes as tables of shares. Given a scheme $\Sigma = \langle \Pi, \mu \rangle$, it is natural to consider the table with all possible shares of the scheme. That is, a table M with rows indexed by $K_0 \times R$ and columns indexed by $\{0, \ldots, n\}$ that contains all possible shares of the scheme. Each row is a vector in $K_0 \times K_1 \times \cdots \times K_n$ that is the concatenation of $s \in K_0$ and $\Pi(s, r)$ for some $r \in R$. For every $I \subseteq \{0, \ldots, n\}$, we define M_I as the table restricted to the columns I.

Using this representation, the correctness property is as follows: For every set $A \in \Gamma$ and possible sharing sh, all rows whose A's elements match sh_A are indexed by the same secret. When μ, the probability distribution on the random strings, is uniform, the privacy property is as follows: For any set $B \notin \Gamma$, any secrets $s, s' \in K_0$, and any possible sharing sh, the number of rows indexed by s whose B's coordinates are sh_B is equal to the number of rows indexed by s' whose B's coordinates are sh_B. See [BD91] and [Sti92, Section 3] for more details.

This work studies the family of optimal schemes, defined below.

Definition 2.3 (Ideal Secret Sharing Schemes and Ideal Access Structures). *We say that a secret sharing scheme is* k-ideal *if the size of the domain of shares of each party is k and the size of the domain of secrets is k. We say that an access structure is* k-ideal *if there is a k-ideal secret sharing scheme realizing it. We say that a scheme or an access structure is* ideal *if they are k-ideal for some k.*

2.2 Matroids

Here we complement the background on matroid theory presented in Section 1.2. We refer the reader to [Oxl11] for an introduction to matroids. Here we define matroids by their rank function, but there are multiple equivalent definitions.

Definition 2.4 (Matroid). *A matroid is a pair (E, r), where the* ground set *E is a finite set and the* rank *function r is a function $r\colon 2^E \to \mathbb{Z}$, such that the following properties are satisfied for all $X, Y \subseteq E$.*

1. $0 \leq r(X) \leq |X|$.
2. $r(X) \leq r(Y)$ *if* $X \subseteq Y$.
3. $r(X \cap Y) + r(X \cup Y) \leq r(X) + r(Y)$.

Let $\mathcal{M} = (E, r)$ be a matroid. Recall that a set is independent if $r(X) = |X|$. Every subset of an independent set is independent, and the maximal independent sets are called *bases*. All bases have the same number of elements, which equals $r(E)$, the *rank of the matroid*. Next, we provide the definition of ports of matroids.

Definition 2.5 (Ports of matroids). *Let $\mathcal{M} = (E, r)$ be a matroid and $p \in E$. The port of $\mathcal{M}$ at the point p is a collection of subsets of $E \setminus \{p\}$ defined as*

$$\Gamma = \{A \subseteq E \setminus \{p\} : r(A \cup \{p\}) = r(A)\},$$

i.e., $A \in \Gamma$ if and only if adding p to A does not increase its rank.

A port of a connected matroid Γ determines the matroid $\mathcal{M}$, i.e., if Γ is a port of a connected matroid at some point $a \in E$, then there is a unique matroid that satisfies this property. It is a consequence of [Oxl11, Prop. 4.1.2 and Th. 4.3.3].

Theorem 2.6 ([BD91]). *Ideal access structures are matroid ports.*

As a consequence of results in [BD91] and [Mat93], we have the following property.

Theorem 2.7. *Let Σ be an ideal secret sharing scheme with domain of secrets S, let M be the associated table with columns indexed by $E = \{0, \ldots, n\}$, and let $\mathcal{M} = (E, r)$ be its associated matroid. Then*

$$\text{for every } A \subseteq E, \text{ the number of different rows in } \mathsf{M}_A \text{ is } |S|^{r(A)} \tag{1}$$

and each row appears exactly $|S|^{r(E)-r(A)}$ times.

This shows that matroids determined by ideal secret sharing schemes admit a special representation given by the table M. If the domain of secrets is S and $k = |S|$, we say that the matroid is k-*entropic*.

Remark 2.8. Since the work by Brickell and Davenport[BD91], the family of matroids that admit ideal secret sharing schemes has been studied in several areas with different terminology. In 1992, Seymour [Sey92] settled this problem in the context of matroid theory and called secret-sharing matroids to matroids whose ports admit ideal secret sharing schemes. He proved that there exist matroids that are not secret-sharing. Independently, Matúš [Mat93] reached equivalent results by studying families of random variables whose conditional independence structures are determined by matroids. Matúš called these matroids *partition representable* or *p-representable* matroids [Mat99]. Exploring the entropy region, it was found that these matroids play a special role and were also called *entropic*. This notation is motivated by the property presented below. Finally, tables satisfying the properties described in Theorem 2.7 have recently been called *almost affine codes* [SA98] and *variable orthogonal arrays* [CCB25].

Given a secret sharing scheme $\Sigma = \langle \Pi, \mu \rangle$ with secret domain S, we can also define $n+1$ random variables $S_0, \ldots, S_n$ by sampling a uniformly distributed secret s in S, choosing $r \in R$ and computing the share $(\mathsf{sh}_1, \ldots, \mathsf{sh}_n) \leftarrow \Pi(s; r)$; S_0 is a random variable representing the secret s and S_i is a random variable representing the share sh_i for $1 \leq i \leq n$. Furthermore, for a set $A \subseteq E = \{0, \ldots, n\}$ we define $S_A = (S_i)_{i \in A}$. If Σ is an ideal scheme, then the shares S_A are uniformly distributed over a certain size domain $|S|^{r(A)}$. Then the function $r \colon 2^E \to \mathbb{Z}$ defined as

$$r(A) = H(S_A)/H(S) = H(S_A)/\log|S|$$

is the rank function of the associated matroid, where H is the Shannon entropy function. Matroids arising this way are called $|S|$-*entropic* and are equivalent to partition-representable matroids [Mat93].

Theorem 2.9 ([Mat93]). *Let $(S_i)_{i \in E}$ be a sequence of random variables with $H(S_i) = H(S_j)$ for every $i, j \in E$. Let $r : 2^E \to \mathbb{R}$ be the function defined as $r(A) = H(S_A)/H(S)$. If $\mathcal{M} = (E, r)$ is a matroid, then it is partition representable (or $|S|$-entropic).*

We have seen that partition-representable matroids can be equivalently represented by tables and random variables. In this work, we switch between these two representations.

Theorem 2.10. *A connected matroid admits a table M satisfying Equation* (1) *if and only if its ports are ideal access structures.*

Not all ports of matroids admit ideal secret sharing schemes, Vámos matroid is an example of a matroid whose ports do not admit ideal schemes [Sey92], and more examples are given in [Mat99].

Deletions, Contractions, and Minors. Here we see how the entropic representability of matroids behaves with the two most common operations of matroids, which are deletion and contraction (see [Oxl11] for details). Moreover, we see that taking minors preserves k-entropic representability. That is, any minor of a matroid having a k-entropic representation for some k, also admits a k-entropic representation [SA98,Mat93].

Definition 2.11. *Given a matroid $\mathcal{M} = (E, r)$ and $X \subseteq E$, the matroid $\mathcal{M} \setminus X = (E', r')$ with $E' = E \setminus X$ and $r'(A) = r(A)$ for every $A \subseteq E'$ is called the* deletion *of $\mathcal{M}$ by X. And the matroid $(\mathcal{M} \,/\, X) = (E', r')$ with*

$$r'(A) = r(A \cup X) - r(X)$$

for every $A \subseteq E'$ is called the contraction *of X from $\mathcal{M}$. A* minor *of $\mathcal{M}$ is a matroid obtained from $\mathcal{M}$ by applying deletions and contractions.*

For ease of notation, if $a \in E$ and $\mathcal{M}$ is a matroid with ground set E, we write $\mathcal{M} \setminus a$ as the deletion of matroid $\mathcal{M}$ by the singleton $\{a\}$, $\mathcal{M} \setminus \{a\}$. Similarly, we write $\mathcal{M}/i$ as the contraction of the matroid $\mathcal{M}$ by the singleton $\{a\}$, $\mathcal{M}/\{a\}$.

We see that entropic representability is closed under these two operations and we show how to construct such representation using the table of Theorem 2.7.

Let $\mathcal{M} = (E, r)$ be a k-entropic matroid with associated table $\mathsf{M} \subseteq S^E$. Given a set $X \subseteq E$, we define the projection mapping

$$\rho_X \colon S^E \to S^X$$

i.e., the mapping induced by the inclusion $X \subseteq E$. Then, denote M_X as the projection of M to the set X, i.e., $\mathsf{M}_X \colon = \rho_X(\mathsf{M})$. First, define the deletion of M by X, $\mathsf{M} \setminus X := \mathsf{M}_{E \setminus X}$ as the restriction of table M to the columns not in X. Second, given some row a of M_X, we denote $\mathsf{M}_{X:a}$ as the restriction of the fiber of a by the mapping $\rho_X|_{\mathsf{M}} : \mathsf{M} \to \mathsf{M}_X$ to the columns not in X , i.e., the subset

$$\mathsf{M}_{X:a} = \{\rho_{E \setminus X}(r) : r \in \mathsf{M} \text{ such that } \rho_X(r) = a\}.$$

For every choice of $a \in \mathsf{M}_X$, the sets $\mathsf{M}_{X:a}$ are not equal but the matroids determined by the tables $\mathsf{M}_{X:a}$ for every $a \in \mathsf{M}_X$ are the same [SA98]. Hence, we define the contraction of M by X, $\mathsf{M} \,/\, X$ as the table $\mathsf{M}_{X:a}$ for some choice of $a \in \mathsf{M}_X$.

In [SA98], Simonis and Ashikhmin proved that the operations $\mathsf{M} \setminus X$ and $\mathsf{M} \,/\, X$ on the tables give entropic representations for the matroids $\mathcal{M} \setminus X$ and $\mathcal{M} \,/\, X$, respectively.

Proposition 2.12 ([SA98]). *Let $\mathcal{M} = (E, r)$ be a entropic matroid with associated table M and let $X \subseteq E$. Then the deletion of $\mathcal{M}$ by X is entropically represented by the table $\mathsf{M} \setminus X$ and the contraction of $\mathcal{M}$ by X is entropically represented by the table $\mathsf{M} \,/\, X$.*

Another relevant operation is the dual. The dual of a matroid $\mathcal{M} = (E, r)$ is the matroid $\mathcal{M}^* = (E, r^*)$ whose bases are the elements of

$$\mathcal{B}^* = \{E \setminus B : B \text{ is a basis of } \mathcal{M}\}.$$

It is known that the dual of a $\mathbb{F}$-linear matroid is also $\mathbb{F}$-linear, but it is not known if the dual of an entropic matroid is entropic. See [Oxl11] for alternative definitions of the dual of a matroid.

2.3 Orthogonal Arrays

A well-studied structure in combinatorial design theory are the orthogonal arrays. The following definition is from [HSS12].

Definition 2.13. *A $\lambda k^t \times n$ table T with entries in $\mathbb{Z}_k$ is called an orthogonal array of strength t factor n level k and index λ if for each $\lambda k^t \times t$ subtable T' of T, each t-tuple in $\mathbb{Z}_k^t$ occurs in T exactly λ times. We say that T is an $OA(\lambda k^t; t, n, k)$*

Remark 2.14. In this work, we restrict ourselves to the case $\lambda = 1$. This object indeed provides an entropic representation of uniform matroids, and so ideal threshold secret sharing schemes. For a uniform matroid $U_{t,n}$, $t \geq 2$, any circuit has size $t + 1$. Then, if $t \geq 2$, any k-entropic representation of the uniform matroid $U_{t,n}$ is equivalent to an orthogonal array of strength t, factor n, level k and index 1, i.e., an $OA(t, n, k)$. See [Mat99, Example 1.5] for details.

The following result is from [Bus52] and can be found in [DK15].

Lemma 2.15 (Bush bound). *Let $n, t \geq 2$. If there is an $OA(t, n, k)$, then*

$$n \leq \begin{cases} k + t - 1 \text{ if } t \leq k \text{ and } k \text{ is even,} \\ k + t - 2 \text{ if } 3 \leq t \leq k \text{ and } k \text{ is odd,} \\ t + 1 \text{ if } t \geq k. \end{cases}$$

2.4 Latin Squares

Here we provide an introduction to latin squares, with special emphasis on mutually orthogonal latin squares. The notation and most of the results in this section are from [DK15].

Definition 2.16. *A latin square of order k is a $k \times k$ array such that each element of $\{0, \ldots, k-1\}$ appears exactly once within any row or column of the array.*

A latin square of order n can be represented as a table M of 3 columns and k^2 rows, where in every row (i, j, ℓ), the third column takes the value ℓ of the latin square at position (i, j). In this case, we say that the latin square is determined by the table M. This is equivalent to observe that a latin square is an orthogonal array of strength 2, factor 3 and level k.

Definition 2.17. *Two latin squares of order k are said to be* orthogonal *if every ordered pair of symbols occurs exactly once among the k^2 pairs.*

Two orthogonal latin squares of order k with tables M_1 and M_2 satisfy that if we consider the table M with 4 columns and k^2 rows such that each row (i, j, ℓ_1, ℓ_2) is such that (i, j, ℓ_1) is a row of M_1 and (i, j, ℓ_2) is a row of M_2, then this table is an orthogonal array of strength 2, factor 4 and level k. That is, in every 2 column subtable, each row appears once.

A *transversal* of a latin square of order k is a set of k positions, one in each row, one in each column, such that no two of the positions contain the same symbol. Notice that given two orthogonal latin squares L_1 and L_2, the k entries of L_1 corresponding to some entry in L_2 form a transversal of L_1. Then, the characterization of the latin squares that admit orthogonality is given by the following result in [DK15].

Theorem 2.18. *A latin square of order k has an orthogonal mate if and only if it has k disjoint transversals.*

A set of more than two latin squares with the property that each pair of the set is orthogonal is called *mutually orthogonal latin squares* (MOLS).

Theorem 2.19. *There are at most $k-1$ mutually orthogonal latin squares of order k.*

Definition 2.20. *A* quasigroup *is a set Q with a binary operation $\cdot$ such that if $x, z \in Q$, then there exists a unique $y \in Q$ such that $x \cdot y = z$, and if $y, z \in Q$ then there exists a unique $x \in Q$ such that $x \cdot y = z$.*

A latin square can be interpreted as the multiplication table of a quasigroup Q (see [DK15] for more details). We introduce the most used operation between quasigroups that also extends to latin squares properly. Let $(Q, \cdot)$ and $(H, \diamond)$ be two quasigroups. An ordered triple (θ, ϕ, ψ) of one to one mappings from the set Q to the set H is called an *isotopy* of $(Q, \cdot)$ to $(H, \diamond)$ if $\theta(x) \diamond \phi(y) = \psi(x \cdot y)$ for all $x, y \in Q$. The quasigroups $(Q, \cdot)$ and $(H, \diamond)$ are then said to be *isotopic*. An equivalent definition works for latin squares. An *isotopism* between two latin squares L, L' is a permutation of the rows, the columns, and the symbols of L that maps to L'. An *isotopy* class of latin squares is an equivalence class for the isotopy relation. We differentiate *symbol isotopism* as the mapping that only modifies the symbols of a latin square, i.e., (id, id, ψ). Then, we say that the latin squares are *permuted* or *symbol-isotopic*.

The problem of determining whether a latin square has an orthogonal mate or not is open in general, but for the family of group-based latin squares defined below we have additional information about the characterization of the existence of n disjoint transversals, so the existence of orthogonal mates. MOLS determine orthogonal arrays and, as discussed above, guaranty the existence of ideal threshold secret sharing schemes. This property was already observed in [Sin64,Sti92,Mat99].

As a consequence of Construction 1.9 and Lemma 2.22, this result follows.

Theorem 2.21. *The $(2, n)$-threshold access structure admits a k-ideal scheme if and only if there exist $n-1$ MOLS of order k.*

We detailed in Construction 1.9 how to define a k-ideal scheme for a $(2, n)$-threshold access structure given a set of $n-1$ MOLS of order k. We next prove that the converse is also true and deduce the following equivalence.

Lemma 2.22. *Let M be a table in S^E where S is a k-element domain and $E = \{0, \ldots, n\}$. They are equivalent:*

(i) M *is a k-ideal scheme for a $(2, n)$-threshold access structure.*
(ii) M *is a k-entropic representation of the uniform matroid $U_{2,n+1}$.*
(iii) M *determines a set of $n+1-2 = n-1$ orthogonal latin squares of order k as follows:*
Let $B \subseteq \{0, \ldots, n\}$ be a set of size 2. The tables

$$\{\mathsf{M}_{B \cup i} \colon i \in \{0, \ldots, n\} \setminus B\}$$

define a set of $n-1$ MOLS.

Proof. Consider M to be a k-entropic representation of the uniform matroid $U_{2,n+1}$. Let $B \subseteq \{0, \ldots, n\}$ be a set of size 2 and consider the tables $M_{B \cup i}$ consisting on the restriction of M to the columns in $B \cup i$ for every $i \in \{0, \ldots, n\} \setminus B$.

For each table $\mathsf{M}_{B \cup i}$, we consider the square that has in the position (i, j) the value ℓ such that there is a row (i, j, ℓ) in the table $\mathsf{M}_{B \cup i}$. Note that since every pair (i, j) appears once when restricting to every 2-columns of the table $\mathsf{M}_{B \cup i}$, this is well defined and $\mathsf{M}_{B \cup i}$ is a latin square.

Moreover, let $i, j \in \{0, \ldots, n\} \setminus B$, $i \neq j$. Consider the table $\mathsf{M}_{B \cup i \cup j}$ and since M is a k-entropic representation of a uniform matroid of rank 2, this table satisfies that every pair of values appears once when restricting to every 2-columns of the table. Then, if we restrict $\mathsf{M}_{B \cup i \cup j}$ to the columns i and j, every pair of values occurs exactly once. So, the latin squares $\mathsf{M}_{B \cup i}$ and $\mathsf{M}_{B \cup j}$ are orthogonal. □

2.5 Group-Based Latin Squares

When a latin square L is isotopic to the multiplication table (also called the Cayley table) of a group, then we say that the latin square L is *group-based*. In this case, determining whether a latin square admits an orthogonal mate is related with some property of the group.

Group-based latin squares are of special interest in our work. We give some technical results that will be helpful later. Their proofs can be found in Appendix A.

Lemma 2.23. *Let L be a latin square isotopic to the Cayley table of a group $(G, \cdot)$. Then there exist unique permutations τ and σ such that for every $i, j \in G$,*

$$M(i, j) = \tau(\sigma(i) \cdot j).$$

Remark 2.24. Two latin squares L_1, L_2 that are symbol-isotopic, i.e., their isotopism is (id, id, ψ), share the same σ while have different τ. Also note that symbol-isotopism preserves orthogonality.

Let L be the Cayley table of a group $(G, \cdot)$ and some permutation σ of G. We denote L_σ to the latin square obtained by permuting the rows of L. Note that using the notation of Lemma 2.23, it can be expressed with the formula

$$L_\sigma(i, j) = L(\sigma(i), j) = \sigma(i) \cdot j.$$

Next, we relate the orthogonality of permutations of a group with the orthogonality of group-based latin squares.

Let σ_1, σ_2 be permutations of G, following the notation from [Eva89], we say that σ_1 is *orthogonal* to σ_2, $\sigma_1 \perp \sigma_2$, if the mapping $x \mapsto \sigma_1(x)^{-1} \cdot \sigma_2(x)$ is a permutation of G. Note that $\sigma_1 \perp \sigma_2$ iff $\sigma_2 \perp \sigma_1$ since $\sigma_2(x)^{-1} \cdot \sigma_1(x) = (\sigma_1(x)^{-1} \cdot \sigma_2(x))^{-1}$. Then, this notion of orthogonality can be related with orthogonality in latin squares by the following lemma. The proof of Lemma 2.25 is in Section A.1.

Lemma 2.25. *Let L_1 and L_2 be two latin squares isotopic to the Cayley table L of a group $(G, \cdot)$. If L_1 and L_2 are determined by (σ_1, τ_1) and (σ_2, τ_2), respectively, then L_1 is orthogonal to L_2 if and only if $\sigma_1 \perp \sigma_2$.*

2.6 Latin Hypercubes

Latin squares can be generalized by allowing the number of dimensions to increase. If we increase the number of dimensions to three, we obtain a *latin cube*, an object having k^2 rows, k^2 columns, and k^2 layers such that a set of k elements occurs once in each row, column, and layer. For larger dimensions, we define the latin d-hypercubes as follows. See [DK15] for more details.

Definition 2.26. *A* latin hypercube *of order k and dimension d is an array in $\{0, \ldots, k-1\}^{k^d}$ such that each symbol occurs exactly k^{d-t-1} times in each $(d-t)$-dimensional subarray for every $1 \leq t \leq d-1$.*

In particular, a 2-dimensional latin hypercube of order k is a latin square of order k. When considering dimension 3, we say that we have a *latin cube*.

A latin hypercube of order k and dimension d can be represented as a table M of $d+1$ columns and k^d rows, where in every row $(i_1, \ldots, i_d, \ell)$, the last column takes the value ℓ of the latin hypercube at position $(i_1, \ldots, i_d)$. In this case, we say that the latin hypercube is determined by the table M. Note that table M is also a k-entropic representation of the uniform matroid $U_{d,d+1}$. This is equivalent to observe that a latin hypercube is an orthogonal array of strength d, factor $d+1$, and level k.

Example 2.27. An example of a latin hypercube of dimension 3 and order 3 is the $3 \times 3 \times 3$ array that can be represented as the set of the following latin squares

that correspond to the value of the latin hypercube in the position (i, j, k) when $k = 0, 1, 2$:

$$A = \begin{array}{ccc|ccc|ccc} \multicolumn{3}{c|}{k=0} & \multicolumn{3}{c|}{k=1} & \multicolumn{3}{c}{k=2} \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 1 & 2 & 0 & 2 & 0 & 1 & 0 & 1 & 2 \\ 2 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 \end{array}$$

△

The notion of orthogonality in latin squares can be generalized to larger dimensions as follows.

Definition 2.28. *Two latin hypercubes of dimension d and order k are said to be* orthogonal *if, when superimposed, each of the k^2 possible distinct pairs occurs exactly k^{d-2} times.*

Notice that this definition ensures that each ordered pair occurs the same number of times upon superimposition of the hypercubes, but it does not yield any information on the positions of the repeated ordered pairs. For that, we use a more general notion of orthogonality presented in [EM12] that controls the distribution of repeated pairs.

Definition 2.29 ([EM12]). *Two latin hypercubes of dimension d and order k are said to be* strong orthogonal *if, when superimposed, each ordered 2-tuple appears once in any 2-dimensional subarray of the hypercube.*

In particular, two Latin cubes are *strong orthogonal* if in the superimposition of them, each pair appears exactly once in every 2-dimensional subarray. In other words, every pair of latin squares obtained by fixing some layer is orthogonal.

Moreover, we define orthogonality to a set of more than two hypercubes, which we call dimensional orthogonality:

Definition 2.30. *For $d \geq 2$, a set of d hypercubes of order k are said to be d-*orthogonal *if, when superimposed, each of the k^d ordered d-tuples occurs exactly once.*

Notice that if $d = 2$, the definition of dimensional orthogonality corresponds to the standard definitions for orthogonality of latin squares.

Theorem 2.31 ([EM12, Theorem 3.3]). *There are at most $k - 1$ mutually 2-strong orthogonal latin hypercubes of order k and dimension d.*

Example 2.32. The latin cube of Example 2.27 is orthogonal to

$$B = \begin{array}{ccc|ccc|ccc} 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 2 & 0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 \\ 1 & 2 & 0 & 2 & 0 & 1 & 0 & 1 & 2 \end{array}$$

since if we consider the superimposition of the two cubes, every ordered 2-tuple appears 3 times.

$$AB = \begin{array}{ccc|ccc|ccc} 00 & 11 & 22 & 11 & 22 & 00 & 22 & 00 & 11 \\ 12 & 20 & 01 & 20 & 01 & 12 & 01 & 12 & 20 \\ 21 & 02 & 10 & 02 & 10 & 21 & 10 & 21 & 02 \end{array}$$

Note that B it is not strong orthogonal to A since in every row there is some pair that appears 3 times and not one. There are no pairs of strong orthogonal cubes of order 3. This is by Theorem 2.33 and the bound of Theorem 3.1. See an example of strong orthogonal latin cubes of order 4 at the Example A.4. $\triangle$

In [Rao46,Rao47], Rao observed that strong forms of orthogonality of latin hypercubes is related with orthogonal arrays (see [DK15, Section 5.4] for more details). So we can generalize Theorem 2.21 that relates MOLS and ideal schemes for $(2, n)$-threshold access structures to higher dimensions.

Theorem 2.33. *Let $1 \leq n$ and $2 \leq t \leq n$. The (t, n)-threshold access structure admits a k-ideal scheme if and only if there exist $n - t + 1$ mutually strong orthogonal latin hypercubes of dimension t and order k.*

Proof. As we observed previously (Remark 2.14), if $2 \leq t \leq n$, ideal schemes for (t, n)-threshold access structures are equivalent to orthogonal arrays of strength t, factor $n+1$ and level k, i.e., an $OA(t, n+1, k)$. From [DK15], it is deduced that an $OA(t, n + 1, k)$ is equivalent to a set of $n + 1 - t$ mutually strong orthogonal latin hypercubes of dimension t and order k. $\square$

Remark 2.34. A k-ideal scheme for a (t, n)-threshold access structure is equivalent to a k-entropic representation of the uniform matroid $U_{t,n+1}$. Let M be the table corresponding to such representation. Then, they are equivalent:

(i) M is a k-ideal scheme for a (t, n)-threshold access structure with table M.
(ii) M is a k-entropic representation of the uniform matroid $U_{t,n+1}$.
(iii) M determines a set of $n+1-2 = n-1$ 2-strong orthogonal latin hypercubes of order k and dimension t as the following:
Let $B \subseteq \{0, \ldots, n\}$ be a set of size t. For every pair $i, j \in \{0, \ldots, n\} \setminus B$, $i \neq j$, the tables $\mathsf{M}_{B \cup i}$ and $\mathsf{M}_{B \cup j}$ are 2-strong orthogonal latin hypercubes of dimension t and order k.

Remark 2.35. Sets of $n - t + 1$ mutually strong orthogonal latin t-dimensional hypercubes of order k also determine a k-ary code of length $n + 1$ and minimum distance $n-t+1$ (see [EM12] for details). From this observation we can deduce a bound for the size of the domain of a (t, n)-threshold ideal secret sharing scheme which is equivalent to the one stated at Theorem 3.1 for the even case and follows from the sphere-packing bound (or Hamming bound) for k-ary codes, which states that every k-ary code of length n and minimum distance $n - t + 1$ has $t \leq k - 1$.

Concretely, we can deduce that there do not exist pairs of strong orthogonal t-dimensional latin hypercubes of order k if $t > k - 1$.

From Theorem 2.7, every ideal secret sharing scheme defines an entropic representation of a matroid. This representation is given by a table M whose rows are the possible shares of the parties. We can observe that the circuits of entropic matroids define concrete configurations that are related with latin hypercubes.

Lemma 2.36. *Let $\mathcal{M}$ be a k-entropic matroid with associated table M. Then a subset $C \subseteq E$ is a circuit of $\mathcal{M}$ if and only if M_C determines a latin hypercube of dimension $r(C)$, where M_C is the table obtained by restricting to the columns of M labeled by C.*

Proof. Since C is a circuit, the restriction of $\mathcal{M}$ to C is a uniform matroid. That is, the minor is the uniform matroid $U_{t,t+1}$, for $t = r(C)$.

Consider the table M of Theorem 2.7. Denote by M_C the subarray obtained by restricting to the columns labeled by C. Let $t = r(C)$. Then, a k-entropic representation of the uniform matroid $\mathcal{M} \setminus (E \setminus C)$, which is indeed $U_{t,t+1}$, is a latin hypercube of dimension t and order k. □

3 Threshold Access Structures

Bounds on the share size for threshold secret sharing schemes are already known and presented in several works [KGH83,Nis91,CCX13,BGK16]. These bounds work for not-necessarily ideal schemes and are independent of the connection between ideal (t, n)-threshold schemes and orthogonal arrays [Rao46,Rao47,BD91] [Mar91,DMR93].

Orthogonal arrays are a widely studied object in combinatorics theory introduced by Bush [Bus50,Bus52] from which a bound is derived on the number of factors of the array (see Lemma 2.15). Using the connection of orthogonal arrays with k-ideal (t, n)-threshold secret sharing, this bound is translated into the following lower bound on the size of the share domain k in terms of the number of parties n and the threshold t.

Theorem 3.1 (Theorem 1.3 Restated). *Let $n, t \geq 2$, and let Σ be (t, n)-threshold ideal secret sharing scheme over a domain of size k.*

- *If k is even and $t \leq k$, then $k \geq n - t + 2$.*
- *If k is odd and $3 \leq t \leq k$, then $k \geq n - t + 3$.*
- *If $t \geq k$, then $n \leq t$. Equivalently, if $n > t$, then $k \geq t + 1$.*

In [CCX13], Cascudo, Cramer, and Xing show that for any t-threshold access structures of n parties, the size of the share domain is at least $n - t + 2$, independently of the cardinality of the secret space. Moreover, according to the previous remark, the Bush bound implies that if $t \geq 3$ and the secret and shares have domain of size $k \geq t \geq 3$ and k is odd, then k is at least $n - t + 3$. This improves the actual known lower bound for the size of share domain for ideal threshold secret sharing.

Bogdanov, Guo, and Komargodski [BGK16] show that any t-out-of-n secret sharing scheme for one bit secret requires share size at least $t+1$, and the bound holds for ideal schemes too. Notice that the third Bush bound has the same implication.

4 Forbidden Minors for 6-Entropic Matroids and Fano Configurations

This section is dedicated to the proof of Theorem 1.2. We dedicate Section 4.1 to show equivalent conditions for which an access structure admits a 6-ideal scheme, proving Theorem 1.18. This characterization is based on the study of the 6-entropic representations of matroids $U_{2,4}$, F_7 and F_7^*. Although it is well-established that 6-entropic representations of matroids $U_{2,4}$ and F_7 do not exist, in Section 4.2 we provide the characterization of k-entropic representations of the dual of Fano matroid F_7^*, for every $k \geq 2$, following the techniques of [Mat99].

Later, in Section 4.3, we give the characterization of k-entropic representations of the dual of non-Fano matroid $\left(F_7^-\right)^*$, following similar techniques as in Section 4.2. This result will be needed later at Section 5 for the proof of Theorem 1.12.

4.1 Proof of Theorem 1.2

Notice that Theorem 1.2 is a direct implication of the properties (iii) and (iv) of Theorem 1.18. Hence, proving Theorem 1.18 is enough to prove Theorem 1.2.

For the proof of Theorem 1.18, we give a complete characterization of the access structures that admit a 6-ideal secret sharing scheme, providing several equivalent properties.

Theorem 4.1 (Theorem 1.18 Restated). *An access structure admits a 6-ideal secret sharing scheme if and only if satisfies one of the following equivalent properties:*

(i) It is a port of a matroid that excludes $U_{2,4}$, F_7, and F_7^*.
(ii) It is a port of a regular matroid.
(iii) It is k-ideal for $k = 2$ and $k = 3$.
(iv) It is k-ideal for every $k \geq 2$.

Proof. We prove this result as follows. First, we show that if an access structure satisfies (iii), then it is 6-ideal. Then, we prove that if an access structure is 6-ideal, then it satisfies (i). This second implication is the most technically involved, and we dedicate the rest of the section to this proof. The equivalence of items $(i) - (iv)$ is a consequence of the results of Beimel and Chor [BC94], Golić [Gol98], and Matúš [Mat93, Proposition 2], as detailed below.

By Construction 1.16, if an access structure admits a 2-ideal scheme and a 3-ideal scheme, it admits a 6-ideal scheme, proving the first implication.

Now we move to the next step of the proof. To show that a 6-ideal access structure satisfies (i), we prove it by contrapositive: we show that matroids $U_{2,4}$, F_7, F_7^* are not 6-entropic. This implies that any port of a matroid containing these forbidden minors will not be 6-ideal.

The impossibility result for matroids $U_{2,4}$ and F_7 is derived from previous work of Matúš [Mat99]. It remains to prove that the Fano dual matroid is not 6-entropic. The proof is technically involved, and we present it in Section 4.2.

Equivalences $(i) - (iii) - (iv)$ are deduced from the forbidden minor characterization of k-ideal access structures for $k = 2$ and $k = 3$. In terms of matroid theory, we know that a matroid is 2-entropic if and only if it does not contain $U_{2,4}$ as a minor [Gol98,Mat93]. Moreover, a matroid is 3-entropic if and only if it does not contain $U_{2,5}$, $U_{3,5}$, F_7, or F_7^* as minors [Mat93]. Since matroids $U_{2,5}$ and $U_{3,5}$ contain $U_{2,4}$ as a minor, we deduce that every matroid that does not have $U_{2,4}$, F_7, or F_7^* as minors is k-ideal for $k = 2$ and $k = 3$. So, this proves the equivalence between (i) and (iii). Moreover, Beimel and Chor [BC94] prove that these access structures are also k-ideal for every $k \geq 2$, proving the equivalence (i) and (iv).

In addition, matroids that are 2-linear and 3-linear are known to be linearly representable over any field. Moreover, they constitute the class of regular matroids [Oxl11]. Hence, the equivalence between (i) and (ii) follows. □

4.2 The Fano Dual Matroid

Definition 4.2. *The Fano matroid F_7 is a rank 3 matroid on 7 points, where all subsets of size 3 are bases except for the ones connected by a line in Fig. 1 left. The Fano dual matroid F_7^* is a rank-4 matroid on 7 points, where all subsets of size 4 are bases except for those that are connected with a colored line in Fig. 1 right.*

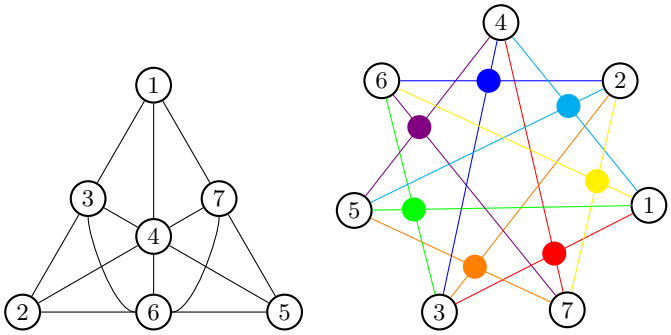


Fig. 1: The matroids F_7 and F_7^*.

Following a similar approach to the characterization of k-entropic representations of F_7 presented in [Mat99], we use that the matroid $M(K_4)$ (Fig. 2) is a minor of F_7^*. Later, in Section 4.3 we also use this approach for the study of $\left(F_7^-\right)^*$.

Theorem 4.3 (Theorem 1.17 Restated). *The F_7^* matroid is k-entropic if and only if $k = 2^t$, $t > 0$.*

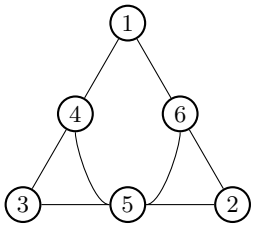


Fig. 2: The matroid $M(K_4)$ of rank 3 and 6 points, where all subsets of size 3 are bases except the ones connected by a line.

Proof. A k-entropic representation of F_7^* is a table M with domain a set S of k elements and 7 columns. Since $r(F_7^*) = 4$, table M has k^4 rows.

The first direction is trivial, as F_7^* is linear over $\mathbb{F}_2$. From this representation, it is standard to build a k-entropic representation on the set $S = \{0, 1\}$ by spanning the rows of this linear representation. Thus, F_7^* is 2-entropic. It follows that F_7^* is k-entropic for every $k = 2^t$, $t > 0$.

In the other direction, we first observe that for every element $i \in E$, the contraction of F_7^* to i, $F_7^* \,/\, i$, is isomorphic to $M(K_4)$. The easiest way to see this is to notice that $F_7 \setminus i = M(K_4)$ and that $M(K_4)$ is self-dual. Hence,

$$F_7^* \,/\, i = (F_7 \setminus i)^* = M(K_4)^* \cong M(K_4).$$

For $a \in S$, let R_a denote the set of rows of M in which the value on the 7th column is a. Thus, M satisfies that for any $a \in S$, the table $\widetilde{\mathsf{M}} := \mathsf{M}_{\{7\}:a}$, i.e., restricting to the first 6 columns and the rows R_a corresponding to the fixed value a of the 7th column c_7, is an entropic representation of the matroid $M(K_4)$.

From the result of Matuš [Mat99], a partition representation of $M(K_4)$ is isotopic to a system of partitions constructed from a finite group G as depicted in Figure 3. To translate this into the language of k-entropic representations, fix some $a \in S$ and denote by $\mathsf{M}_{i,j}$ the cell of M in the ith row and the jth column. The isotopy above means that there exist bijections $\{\psi_i^a \colon S \to G\}$, one for each column c_i, $1 \le i \le 6$, of $\widetilde{\mathsf{M}}$, such that in each row r of $\widetilde{\mathsf{M}}$, we have

$$\begin{aligned}
\psi_4^a\left(\widetilde{\mathsf{M}}_{r,4}\right) &= \psi_3^a\left(\widetilde{\mathsf{M}}_{r,3}\right) \cdot \psi_1^a\left(\widetilde{\mathsf{M}}_{r,1}\right)^{-1}, \\
\psi_6^a\left(\widetilde{\mathsf{M}}_{r,5}\right) &= \psi_2^a\left(\widetilde{\mathsf{M}}_{r,2}\right) \cdot \psi_3^a\left(\widetilde{\mathsf{M}}_{r,3}\right)^{-1}, \\
\psi_6^a\left(\widetilde{\mathsf{M}}_{r,6}\right) &= \psi_1^a\left(\widetilde{\mathsf{M}}_{r,1}\right) \cdot \psi_2^a\left(\widetilde{\mathsf{M}}_{r,2}\right)^{-1},
\end{aligned} \tag{2}$$

where $\cdot$ and $^{-1}$ are the multiplication and inverse operations of G.

Remark 4.4. It is important to note that for each fixed element $a \in S$, restricting the table of M to the first 6 columns and the rows corresponding to $c_7 = a$ is isotopic to $M(K_4)$ for some bijections $\{\psi_i^a\}_{i \in \{1,\ldots,7\}}$. Note that for different values of a, the bijections $\{\psi_i^a\}$ are different. Hence, while the relations in (2)

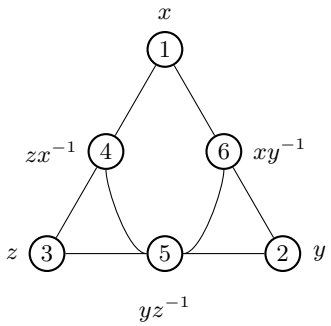


Fig. 3: Entropic representation of $M(K_4)$ via groups

hold for all rows $r \in R_a$, for the rows $r \notin R_a$ these relations generally do not hold.

Fix some $a \in S$ and let $\{\psi_i^a \colon S \to G\}_{i\in\{1,\ldots,6\}}$ be the bijections induced from the isotopy to $M(K_4)$ and $\psi_7^a : S \to G$ be any bijection. We show that the bijections $\{\psi_i^a \colon S \to G\}_{i\in\{1,\ldots,7\}}$ applied to the columns c_i of M give us another entropic representation of F_7^*.

Let $\psi^a(\mathsf{M})$ be the table when ψ_i^a is applied to each column c_i, $i \in E = \{1,\ldots,7\}$. We need to show that for every $X \subseteq E$, the number of different rows in $(\psi^a(\mathsf{M}))_X$ is equal to the number of different rows in M_X.

To see this, it suffices to show that for any set of columns $X \subseteq E$ and for any 2 rows r_1, r_2, it holds that $(\mathsf{M}_{r_1,i})_{i\in X} = (\mathsf{M}_{r_2,i})_{i\in X}$ if and only if $(\psi_i^a(\mathsf{M}_{r_1,i}))_{i\in X} = (\psi_i^a(\mathsf{M}_{r_2,i}))_{i\in X}$. This follows almost immediately from the ψ_i^a's being bijections: If $(\mathsf{M}_{r_1,i})_{i\in X} \neq (\mathsf{M}_{r_2,i})_{i\in X}$ then there exists $j \in X$ such that $\mathsf{M}_{r_1,j} \neq \mathsf{M}_{r_2,j}$, so $\psi_j^a(\mathsf{M}_{r_1,j}) \neq \psi_j^a(\mathsf{M}_{r_2,j})$, and therefore $(\psi_i^a(\mathsf{M}_{r_1,i}))_{i\in X} \neq (\psi_i^a(\mathsf{M}_{r_2,i}))_{i\in X}$; In the other direction, if $(\psi_i^a(\mathsf{M}_{r_1,i}))_{i\in X} \neq (\psi_i^a(\mathsf{M}_{r_2,i}))_{i\in X}$ then there exists $j \in X$ such that $\psi_j^a(\mathsf{M}_{r_1,j}) \neq \psi_j^a(\mathsf{M}_{r_2,j})$, so we infer that

$$\mathsf{M}_{r_1,j} = (\psi_i^a)^{-1}\left(\psi_j^a(\mathsf{M}_{r_1,j})\right) \neq (\psi_i^a)^{-1}\left(\psi_j^a(\mathsf{M}_{r_2,j})\right) = \mathsf{M}_{r_2,j},$$

so $(\mathsf{M}_{r_1,i})_{i\in X} \neq (\mathsf{M}_{r_2,i})_{i\in X}$.

For ease of notation, in the following we assume that the elements of S are the elements of a group G and that when restricting M to the first 6 columns and the rows where $c_7 = a$ for some fixed element a, as above, the columns of the restricted table $\widetilde{\mathsf{M}}$ follow the group operation as depicted in Figure 3. I.e., for every row $r \in \widetilde{\mathsf{M}}$,

$$\widetilde{\mathsf{M}}_{r,1} \cdot \left(\widetilde{\mathsf{M}}_{r,2}\right)^{-1} = \widetilde{\mathsf{M}}_{r,6} \tag{3}$$

$$\widetilde{\mathsf{M}}_{r,2} \cdot \left(\widetilde{\mathsf{M}}_{r,3}\right)^{-1} = \widetilde{\mathsf{M}}_{r,5}, \tag{4}$$

and

$$\widetilde{\mathsf{M}}_{r,3} \cdot \left(\widetilde{\mathsf{M}}_{r,1}\right)^{-1} = \widetilde{\mathsf{M}}_{r,4}. \tag{5}$$

Observe that by definition of $\widetilde{\mathsf{M}}$, the above equations also hold in M for every $r \in R_a$ (i.e., the rows where $c_7 = a$).

Formally, this simply means that we look at $\psi^a(\mathsf{M})$, the entropic representation that results from applying on each column c_i the corresponding ψ_i^a. Note that as $\psi_i^a \colon S \to G$ are bijections, any restriction on the order of G immediately implies the same restriction on the original $|S|$.

Since $\{1,2,3,5\}$ is a base of F_7^*, each of the $|S|^4$ possible combinations appear in columns c_1, c_2, c_3, c_5. In particular, if e is the identity element of G, then for every $g \in G$, there exists a row r_g of M such that

$$\mathsf{M}_{r_g,1} = \mathsf{M}_{r_g,2} = \mathsf{M}_{r_g,3} = e,\ \mathsf{M}_{r_g,5} = g. \tag{6}$$

As $\{1,3,5\}$ is a base of $F_7^* \,/\, 7$, when restricting to the rows R_a, each of the $|S|^3$ possible combinations appears in the columns c_1, c_3, c_5. In particular, there exists a row $r_g^{(1)} \in R_a$ such that

$$\mathsf{M}_{r_g^{(1)},1} = \mathsf{M}_{r_g^{(1)},3} = e,\ \mathsf{M}_{r_g^{(1)},5} = g. \tag{7}$$

Note that since $r_g^{(1)} \in R_a$, these cells are in $\widetilde{\mathsf{M}}$, so by the assumption on $\widetilde{\mathsf{M}}$, we can deduce from Equation (4) that

$$\mathsf{M}_{r_g^{(1)},2} = \mathsf{M}_{r_g^{(1)},5} \cdot \mathsf{M}_{r_g^{(1)},3} = g,$$

and from Equation (3) that

$$\mathsf{M}_{r_g^{(1)},6} = \mathsf{M}_{r_g^{(1)},1} \cdot \left(\mathsf{M}_{r_g^{(1)},2}\right)^{-1} = g^{-1}.$$

Now using the fact that $\{1,3,5,6\}$ is a circuit of F_7^*, we deduce that $\mathsf{M}_{r_g,6} = \mathsf{M}_{r_g^{(1)},6} = g^{-1}$. This follows as $\mathsf{M}_{r_g,1} = \mathsf{M}_{r_g^{(1)},1} = e$, $\mathsf{M}_{r_g,3} = \mathsf{M}_{r_g^{(1)},3} = e$, and $\mathsf{M}_{r_g,5} = \mathsf{M}_{r_g^{(1)},5} = g$. Thus, since $\{1,3,5,6\}$ is a circuit of F_7^*, only $|S|^3$ possible combinations appear in the columns c_1, c_3, c_5, c_6. However, as explained, $|S|^3$ different combinations already appear in these columns in the rows of R_a. Hence, since the values of the columns c_1, c_3 and c_5 in the rows r_g and $r_g^{(1)}$ are equal, it follows that the value on column c_6 in these two rows must also be equal. Hence,

$$\mathsf{M}_{r_g,6} = \mathsf{M}_{r_g^{(1)},6} = g^{-1}. \tag{8}$$

We now proceed in a similar manner and look at the row $r_g^{(2)} \in R_a$ where

$$\mathsf{M}_{r_g^{(2)},2} = \mathsf{M}_{r_g^{(2)},3} = e,\ \mathsf{M}_{r_g^{(2)},6} = g^{-1}.$$

The existence of such a row follows from similar considerations as for Equation (7), since $\{2,3,6\}$ is a base of $F_7^* \,/\, 7$. By the assumption on $\widetilde{\mathsf{M}}$, we can now deduce from Equation (3) that

$$\mathsf{M}_{r_g^{(2)},1} = \mathsf{M}_{r_g^{(2)},6} \cdot \mathsf{M}_{r_g^{(2)},2} = g^{-1}$$

and from Equation (5) that

$$\mathsf{M}_{r_g^{(2)},4} = \mathsf{M}_{r_g^{(2)},3} \cdot \left(\mathsf{M}_{r_g^{(2)},1}\right)^{-1} = g.$$

Next, since $\{2,3,4,6\}$ is a circuit of F_7^* and $\mathsf{M}_{r_g,2} = \mathsf{M}_{r_g^{(2)},2} = e$, $\mathsf{M}_{r_g,3} = \mathsf{M}_{r_g^{(2)},3} = e$, and $\mathsf{M}_{r_g,6} = \mathsf{M}_{r_g^{(2)},6} = g^{-1}$, using similar considerations to those we used for Equation (8), we deduce that

$$\mathsf{M}_{r_g,4} = \mathsf{M}_{r_g^{(2)},4} = g.$$

We follow the same procedure once again, looking at the row $r_g^{(3)} \in R_a$ where

$$\mathsf{M}_{r_g^{(3)},1} = \mathsf{M}_{r_g^{(3)},2} = e,\ \mathsf{M}_{r_g^{(3)},4} = g.$$

The existence of such $r_g^{(3)} \in R_a$ is guaranteed, since $\{1,2,4\}$ is a base of $F_7^* \,/\, 7$. We deduce that

$$\mathsf{M}_{r_g^{(3)},3} = \mathsf{M}_{r_g^{(3)},4} \cdot \mathsf{M}_{r_g^{(3)},1} = g$$

and

$$\mathsf{M}_{r_g^{(3)},5} = \mathsf{M}_{r_g^{(3)},2} \cdot \left(\mathsf{M}_{r_g^{(3)},3}\right)^{-1} = g^{-1} \tag{9}$$

from Equations (5) and (4) by the assumption on $\widetilde{\mathsf{M}}$, and that

$$\mathsf{M}_{r_g,5} = \mathsf{M}_{r_g^{(3)},5} = g^{-1} \tag{10}$$

by the fact that $\{1,2,4,5\}$ is a circuit of $F_7^* \,/\, 7$.

However, we started with $\mathsf{M}_{r_g,5} = g$ by the definition of r_g (Equation (6)), so it follows that $g = g^{-1}$ and so $g^2 = e$, and this holds for all $g \in G$. In addition, G is finite, so it follows that $|G|$ is a power of 2, and, furthermore, $G \cong \Pi_{i=1}^{\log|G|}\mathbb{Z}_2$. Thus, $k = |S| = |G| = 2^t$ for some $t > 0$. □

4.3 The Non-Fano Dual Matroid

Definition 4.5. *The non-Fano Dual matroid, denoted $\left(F_7^-\right)^*$, is a rank-4 matroid with 7 points, whose circuits are the 4-element colored sets of the Fig. 4 right.*

We know that $\left(F_7^-\right)^*$ is linearly representable over a field $\mathbb{F}$ if and only if char $\mathbb{F} \neq 2$. Therefore, for domains of size $k = p^r$ for some odd prime p, there is a linear representation, and thus an entropic one. Since entropic domains are multiplicatively closed, it follows that there exists an entropic representation for every odd $k > 2$. The question was open for domains of even size. We show that $\left(F_7^-\right)^*$ has a k-entropic representation if and only if k is odd.

Theorem 4.6 (Theorem 1.13 Restated). *The dual of non-Fano matroid is k-entropic if and only if k is odd.*

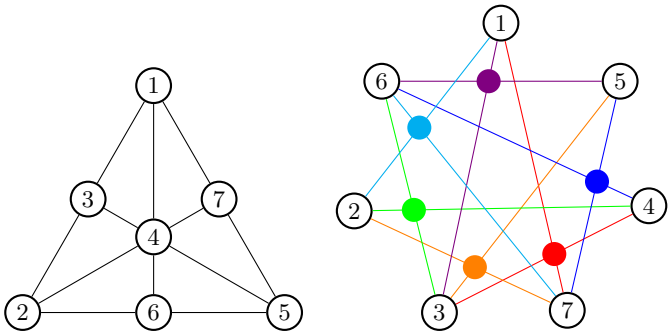


Fig. 4: The non-Fano matroid and non-Fano Dual matroid.

Proof. Observe that, compared with the Fano dual, the set $\{1,2,4,5\}$ is now a base.

In contrast with the dual of the Fano matroid, the dual of the non-Fano is not symmetric. Hence, the result of the contraction depends on the point we are contracting on. If we contract to some element of the new (compared with F_7^*) base, $\{1,2,4,5\}$, for example to 4, then we get

$$\left(F_7^-\right)^* / 4 = \left(F_7^- \setminus 4\right)^* \simeq \left(\mathcal{W}^3\right)^* \simeq \mathcal{W}^3,$$

where $\mathcal{W}^3$ is the Wheel matroid (see [Oxl11] for more details). However, if we contract to some element out of the base $\{1,2,4,5\}$ such as 7, then we again get

$$\left(F_7^-\right)^* / 7 = \left(F_7^- \setminus 7\right)^* \simeq (M(K_4))^* \simeq M(K_4),$$

as in Fig. 5.

Since the only difference between the matroids F_7^* and $\left(F_7^-\right)^*$ is the additional base $\{1,2,4,5\}$, we can follow the proof of Theorem 1.17 up to Equation (9), which still holds also in this case. Equation (10) already relied on the fact that $\{1,2,4,5\}$ was a circuit of F_7^*, when we deduced that $\mathsf{M}_{r_g,5} = \mathsf{M}_{r_g^{(3)},5} = g^{-1}$, but $\{1,2,4,5\}$ is not a circuit of $\left(F_7^-\right)^*$.

Instead, in this case we have that $\{1,2,4,5\}$ is a base, so all k^4 combinations must appear in these columns. In particular, since

$$\mathsf{M}_{r_g,1} = \mathsf{M}_{r_g^{(3)},1} = e,\ \mathsf{M}_{r_g,2} = \mathsf{M}_{r_g^{(3)},2} = e, \text{ and } \mathsf{M}_{r_g,4} = \mathsf{M}_{r_g^{(3)},4} = g,$$

it follows that $\mathsf{M}_{r_g,5} \neq \mathsf{M}_{r_g^{(3)},5}$, unless $r_g \in R_a$, in which case $r_g = r_g^{(3)}$. Observe that in this specific case ($r_g \in R_a$) we can combine Equation (6) with Equation (4) and get that

$$g = \mathsf{M}_{r_g,5} = \widetilde{\mathsf{M}}_{r_g,2} \cdot \left(\widetilde{\mathsf{M}}_{r_g,3}\right)^{-1} = e \cdot (e^{-1}) = e.$$

That is, $r_g \in R_a$ exactly for $g = e$.

As $\mathsf{M}_{r_g,5} = g$ by the definition of r_g (Equation (6)), and $\mathsf{M}_{r_g^{(3)}} = g^{-1}$ by the calculation (Equation (9)), it follows that if $r_g \notin R_a$, then $g \neq g^{-1}$. Since all k^4 combinations must exist, this implies that for every $g \in G$ there exists a row r_g such that $\mathsf{M}_{r_g,5} = g$, but since $\{1,2,3\}$ is a base of $M(K_4)$, exactly one such r_g is in R_a (since there's only a single row $r_a \in R_a$ where $\mathsf{M}_{r_a,1} = \mathsf{M}_{r_a,2} = \mathsf{M}_{r_a,3} = e$, and by (4) for this row $\mathsf{M}_{r_a,5} = \mathsf{M}_{r_a,2} \left(\mathsf{M}_{r_a,3}\right)^{-1} = e$). It follows that $g \neq g^{-1}$ for all but one $g \in G$, which is, as explained, for $g = e$.

Thus, for all $e \neq g \in G$, it must hold that $g^2 \neq e$, so G has no element of order 2. It follows that G is an odd order group, so $k = |S| = |G|$ must be odd. □

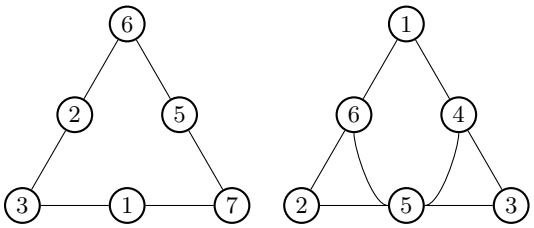


Fig. 5: Geometric representations of $\left(F_7^-\right)^* / 4$ and $\left(F_7^-\right)^* / 7$

5 Forbidden Minors for 4-Entropic Matroids

This section is dedicated to Theorem 1.1. To this end, we take advantage of the forbidden minor characterization of $\mathbb{F}_4$-linear matroids and generalize this characterization to the class of 4-entropic matroids. The characterization of $\mathbb{F}_4$-linear matroids together with Theorem 1.12 proven in Section 5.1 complete the proof of Theorem 1.1.

This proof is based on combinatorial objects such as latin squares and latin cubes of order 4, which we detail in the following subsections in order to complete the proof.

5.1 Proof of Theorem 1.1

A sufficient condition for an access structure to be ideal over a domain of size 4 is to admit a $\mathbb{F}_4$-linear ideal secret sharing scheme, i.e., the access structure is a port of a $\mathbb{F}_4$-linear matroid. Geelen, Gerards, and Kapoor [GGK00] proved that a matroid is $\mathbb{F}_4$-linear if and only if it does not contain as a minor any of the following matroids:

$$U_{2,6}, U_{4,6}, P_6, F_7^-, \left(F_7^-\right)^*, P_8, P_8^{''} \tag{11}$$

In the following theorem, we prove that this condition is also necessary. That is, we show that a matroid port is a 4-ideal access structure if and only if the matroid does not contain any of the minors on the list. With that, we complete the proof of Theorem 1.1.

Theorem 5.1 (Theorem 1.12 Restated). *An access structure admits a 4-ideal secret sharing scheme if and only if it is a port of a matroid that excludes $U_{2,6}$, $U_{4,6}$, P_6, F_7^-, $\left(F_7^-\right)^*$, P_8, and P_8'' as minors.*

Proof. In order to prove this result, we show that all the matroids in (11) are not 4-entropic. Then, since entropic representations are closed by deletion and contraction (Proposition 2.12), this completes the proof of Theorem 1.12.

From previous results, we already know that the minors $U_{2,6}$, $U_{4,6}$ and F_7^- are not 4-entropic [CCX13,BGK16,Mat99]. Also, by Theorem 1.13 we know that $\left(F_7^-\right)^*$ is not 4-entropic. The proofs that P_6, P_8, and P_8'' are not 4-entropic are detailed in Theorem 5.10, Theorem 5.12, and Theorem 5.14, respectively. □

5.2 Latin Squares of Order 4

Our techniques based on latin configurations are focused in small orders and take advantage of the low expressivity that exists when considering small domains. We detail how latin squares and latin hypercubes behave in a domain of four elements, and we characterize orthogonality of latin squares of order four.

While there are only 12 latin squares of order 3, and all are isotopic to the multiplication table of the cyclic group C_3, in order four we can find 576 different latin squares that are classified into two isotopy classes that are determined by two different groups. This implies that latin squares of order 4 admit more expressibility than latin squares of order 3.

Latin squares of order 4 are classified into two isotopy classes that are represented by the latin squares L_V and L_C (see [DK15, Chapter 4] for details).

$$L_V = \begin{matrix} 0\,1\,2\,3 \\ 1\,0\,3\,2 \\ 2\,3\,0\,1 \\ 3\,2\,1\,0 \end{matrix} \qquad L_C = \begin{matrix} 0\,1\,2\,3 \\ 1\,2\,3\,0 \\ 2\,3\,0\,1 \\ 3\,0\,1\,2 \end{matrix}$$

The first square, L_V, is the Cayley table of the Klein group V_4 and the second square, L_C, is the Cayley table of the cyclic group C_4. Hence, we observe that all latin squares of order 4 are group-based and can be characterized by the formula of Lemma 2.23 (see Example 1.14).

Remark 5.2. Note that the additive structure of the finite field $\mathbb{F}_4$ is exactly the Klein group V_4. Then, we can represent the latin squares of order four isotopic to L_V as a 4×4 array of elements in $\mathbb{F}_4$ with the assignment $\{0,1,2,3\}$ to $\{0,1,\alpha,\alpha+1\}$ being α a primitive generator of $\mathbb{F}_4$. This representation connects latin squares to local permutation polynomials [FGU25].

As we saw previously, the property of having an orthogonal mate for latin squares depends on the existence of transversals and is closed under isotopism. A result of [DK15] characterizes the orthogonality of latin squares of order 4 in terms of the isotopy class as follows:

Lemma 5.3 ([DK15]). *The only latin squares of order* 4 *that have an orthogonal mate are those that are isotopic to* L_V*.*

Remark 5.4. While the properties of orthogonality of latin squares of order four are deeply understood, the characterization of latin squares that admit an orthogonal mate remains a long-standing open problem for larger orders. For small orders ($n \leq 5$), the existence of an orthogonal mate is strictly tied to group-based structures; indeed, every latin square of order less than six that possesses an orthogonal mate is isotopic to a Cayley table of a group. Order 6 latin squares do not admit orthogonality, and order 7 is the smallest order for which a non-group-based latin square can admit an orthogonal mate.

Consider $(G, \cdot)$ to be a 4-element set $\{0, 1, 2, 3\}$ with the operation $\cdot$ defined by the Cayley table of V_4. From Lemma 5.3 and Lemma 2.23, we observe that every latin square that admits an orthogonal mate can be represented by Lemma 2.23. This is, for every latin square L isotopic to L_V there are unique permutations τ and σ of G such that the position (i, j) the value of L is $\tau(\sigma(i) \cdot j)$.

We provide two technical results with respect to this isotopy class of latin squares that will be needed later.

Lemma 5.5. *Two latin squares* L_1, L_2 *isotopic to* L_V *are orthogonal if and only if* $\sigma_{L_1}(x) \neq \sigma_{L_2}(x)$ *for every* $x \in \{1, 2, 3\}$*.*

Proof. Say that σ_1 and σ_2 are the permutations determined by L_1 and L_2, respectively.

First, suppose that there is a $i \in G$ such that $\sigma_1(i) = \sigma_2(i)$, then

$$L_1(i, \sigma_1(i)) = \tau_1(\sigma_1(i) \cdot \sigma_1(i)) = \tau_1(0), \quad L_2(i, \sigma_2(i)) = \tau_2(\sigma_2(i) \cdot \sigma_2(i)) = \tau_2(0)$$

but

$$L_1(0, 0) = \tau_1(0), \quad L_2(0, 0) = \tau_2(0).$$

Then, the squares L_1 and L_2 are not orthogonal.

For the converse implication, suppose that L_1 and L_2 are not orthogonal. Recall from Lemma 2.25 that the isotopic group-based latin squares L_1 and L_2 are orthogonal if and only if the permutations σ_1 and σ_2 determined by them are also orthogonal, i.e., they satisfy that $\sigma_1(x)^{-1} \cdot \sigma_2(x)$ is a permutation. Note also that for every x in G, the inverse operation satisfies $x^{-1} = x$. Recall also that the permutations σ_1, σ_2 have 0 as fixed point.

Note also that for every $i, j \in G$, $\sigma(i \cdot j) = \sigma(i) \cdot \sigma(j)$ since the group satisfies the following. If $i \neq j, i, j \neq 0$, then $i \cdot j = k$ where $k \neq i, j$. So for every different $i, j, k \neq 0$

$$\sigma(i \cdot j) = \sigma(k) = \sigma(i) \cdot \sigma(j)$$

and if $i = j$, then

$$\sigma(i \cdot j) = \sigma(0) = \sigma(i) \cdot \sigma(j).$$

Suppose that there are $i, j \in \{1, 2, 3\}$, $i \neq j$, (so $i \cdot j \neq 0$) such that

$$\sigma_1(i)^{-1} \cdot \sigma_2(i) = \sigma_1(j)^{-1} \cdot \sigma_2(j).$$

Since the inverse is the identity,

$$\sigma_1(i) \cdot \sigma_2(i) = \sigma_1(j) \cdot \sigma_2(j)$$

$$\sigma_1(j) \cdot \sigma_1(i) = \sigma_2(j) \cdot \sigma_2(i)$$

$$\sigma_1(j \cdot i) = \sigma_2(j \cdot i)$$

then, we find that σ_1 and σ_2 coincide at some point $j \cdot i \neq 0$. □

Lemma 5.6. *Let L_1, L_2, L_3 be three MOLS of order 4. Then*

$$\sigma_{L_1}(x) \cdot \sigma_{L_2}(x) \cdot \sigma_{L_3}(x) = 0$$

for every $x \in G$.

Proof. Note that if L_1, L_2, L_3 are MOLS, then they are isotopic to L_V. Say that σ_i are the permutations determined by L_i, for $i = 1, 2, 3$, respectively. If $x = 0$, the statement holds since $\sigma_i(0) = 0$, then choose $x \neq 0$. Since L_1, L_2, and L_3 are mutually orthogonal, $\sigma_i(x) \neq \sigma_j(x) \neq 0$ for every $i, j \in \{1, 2, 3\}$, $i \neq j$. By the group operation of V_4, if $\sigma_1(x) \neq \sigma_2(x) \neq 0$, $\sigma_1(x) \cdot \sigma_2(x)$ is the third element of V_4 different from 0, $\sigma_1(x)$, and $\sigma_2(x)$, therefore it is $\sigma_3(x)$. Hence,

$$(\sigma_1(x) \cdot \sigma_2(x)) \cdot \sigma_3(x) = \sigma_3(x) \cdot \sigma_3(x) = 0.$$

□

5.3 Latin Cubes of Order 4

Let C be a latin cube of order 4 with respective table M. By definition, every 2-dimensional subarray is a latin square of order 4 and therefore is a group-based latin square. We consider the contraction of the table M to all three columns $1, 2, 3$. The resulting are latin squares $\mathsf{M}_{1:a}$, $\mathsf{M}_{2:a}$, and $\mathsf{M}_{3:a}$. Since they are group-based latin squares, for every $a \in \{0, 1, 2, 3\}$ there exist permutations $\sigma_{1,a}$, $\sigma_{2,a}$, and $\sigma_{3,a}$ corresponding to Lemma 2.23.

Lemma 5.7. *Let C a latin cube of order 4 with respective table M. Let $\ell \in \{1, 2, 3\}$. If for every $a \in \{0, 1, 2, 3\}$, $\mathsf{M}_{\ell:a}$ is isotopic to L_V, then the layers $\mathsf{M}_{\ell:a}$ are not orthogonal.*

Proof. We proceed by supposing that there are two values $a, b \in \{0,1,2,3\}$ and $\ell \in \{1,2,3\}$ such that $\mathsf{M}_{\ell:a}$ and $\mathsf{M}_{\ell:b}$ are orthogonal.

Take a transversal of the latin square $\mathsf{M}_{\ell:a}$, i.e., the four rows $(r_i, s_i, 0)$, $i = 0,1,2,3$, where $\mathsf{M}_{\ell:a}$ has the value 0 as the 3th column. Since $\mathsf{M}_{\ell:a}$ is orthogonal to $\mathsf{M}_{\ell:b}$, the latin square $\mathsf{M}_{\ell:b}$ has a different value j in every row starting with (r_i, s_i). Then, for one i, say $i = 0$, the latin square $\mathsf{M}_{\ell:b}$ has the row $(r_0, s_0, 0)$.

Note that the existence of the row $(r_0, s_0, 0)$ in both tables $\mathsf{M}_{\ell:a}$ and $\mathsf{M}_{\ell:b}$ implies that the table $\mathsf{M}_{\{0,1,2,3\}\setminus\ell}$ has two identical rows. I.e., in M, there are two rows with values $(r_0, s_0, 0)$ in columns different from ℓ and a and b in column ℓ, respectively. Recall that a latin cube M satisfies that every triplet (r, s, t) appears once in every 3-column subtable. So, the two repeated rows in $\mathsf{M}_{\{0,1,2,3\}\setminus\ell}$ are a contradiction.

□

We now give a relation between the latin squares $\mathsf{M}_{1:0}, \mathsf{M}_{2:0}$ and $\mathsf{M}_{3:0}$ in terms of the permutations determined by them as in Lemma 2.23.

Lemma 5.8. *If C is a latin cube of order 4 with respective table M, then the permutations $\sigma_{1,0}, \sigma_{2,0}, \sigma_{3,0}$ corresponding to the latin squares $\mathsf{M}_{1:0}, \mathsf{M}_{2:0}, \mathsf{M}_{3:0}$ satisfy $\sigma_{1,0} \circ \sigma_{3,0} = \sigma_{2,0}$.*

Proof. In Lemma 2.23, we saw that any group-based latin square L can be written using the formula

$$L(i,j) = \tau(\sigma(i) \cdot j)$$

for some permutations τ and σ of the 4 element set $\{0,1,2,3\}$ with σ satisfying $\sigma(0) = 0$ and $\cdot$ being the respective group operation. Note also that all latin squares L satisfy that for every $i, j \in \{0,1,2,3\}$,

$$L(\sigma^{-1}(j), \sigma(i)) = \tau(\sigma(\sigma^{-1}(j)) \cdot \sigma(i)) = \tau(j \cdot \sigma(i)) = L(i,j)$$

where the last equality holds because V_4 is commutative. In particular, we observe that $L(x,0) = L(0,\sigma(x))$. Now, let C be a latin cube with table M. We consider $C(x,y,z)$ to be the value of the 4th column of the row that starts with (x,y,z).

$$\begin{aligned} C(x,0,0) =& \mathsf{M}_{3:0}(x,0) = \mathsf{M}_{3:0}(0,\sigma_{3,0}(x)) = C(0,\sigma_{3,0}(x),0) = \\ =& \mathsf{M}_{1:0}(\sigma_{3,0}(x),0) = \mathsf{M}_{1:0}(0,\sigma_{1,0}(\sigma_{3,0}(x))) = C(0,0,\sigma_{1,0}(\sigma_{3,0}(x))) \end{aligned}$$

similarly,

$$C(x,0,0) = \mathsf{M}_{2:0}(x,0) = \mathsf{M}_{3:0}(0,\sigma_{2,0}(x)) = C(0,0,\sigma_{2,0}(x)).$$

Then

$$C(x,0,0) = C(0,0,\sigma_{1,0}(\sigma_{3,0}(x))) = C(0,0,\sigma_{2,0}(x))$$

so $\sigma_{1,0} \circ \sigma_{3,0} = \sigma_{2,0}$. □

5.4 Matroid P_6

In this section, we prove that the matroid P_6, defined below, is not 4-entropic.

Definition 5.9. *The matroid P_6 is a matroid of rank 3 on 6 points. Every 3-element set has rank 3, except for one set of size 3 that has rank 2. In Fig. 6, we represent this matroid, and the set of rank 2 is $\{4,5,6\}$.*

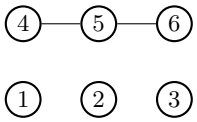


Fig. 6: The matroid P_6.

Theorem 5.10. *The matroid P_6 is not 4-entropic.*

Proof. We suppose that there is a 4-entropic representation and consider the table M satisfying the property of Theorem 2.7. Table M satisfies that for every $A \subseteq \{1,\cdots,6\}$, if M_A is the restriction to the columns in A, each row appears $4^{3-r(A)}$ times in M_A, where r is the rank function of the matroid P_6.

For each $i \in \{4,5,6\}$, we consider the circuit $C_i = \{1,2,3,i\}$ and applying Lemma 2.36 the table M_{C_i} is a latin cube of dimension 3 and order 4.

For every $i \in \{4,5,6\}$ we consider the deletion of the i-th column of the table M, obtaining $\mathsf{M} \setminus \{i\}$. Since $P_6 \setminus \{i\}$ is a uniform matroid $U_{3,5}$, the table $\mathsf{M} \setminus \{i\}$ is a 4-entropic representation of $U_{3,5}$, or a $(3,4)$-threshold ideal scheme. By Theorem 2.33, tables $(\mathsf{M} \setminus \{i\})_{C_j} = \mathsf{M}_{C_j}$ and $(\mathsf{M} \setminus \{i\})_{C_\ell} = \mathsf{M}_{C_\ell}$ constitute pairs of 2-strong orthogonal latin cubes of order 4, for every $j,\ell \in \{4,5,6\}$, $j,\ell \neq i$, $j \neq \ell$. So, M_{C_4}, M_{C_5} and M_{C_6} are pairwise 2-strong orthogonal latin cubes.

In [EM12] they show that if the domain is a prime power, it is possible to extend a pair of 2-strong orthogonal latin cubes to a set of three strong 3-orthogonal latin cubes. Since strong 3-orthogonality implies strong 2-orthogonality, this construction generates a set of 3 mutually strong 2-orthogonal latin cubes.

By Theorem 2.31, there are at most 3 mutually strong 2-orthogonal latin cubes of order 4, so given M_{C_4} and M_{C_5}, there is only one latin cube that is mutually strong 2-orthogonal to M_{C_4} and M_{C_5}. From this uniqueness, the latin cube from the construction of [EM12] must be the M_{C_6} cube, so $\mathsf{M}_{C_4}, \mathsf{M}_{C_5}, \mathsf{M}_{C_6}$ are mutually strong 3-orthogonal.

By Theorem 2.33, table M is the representation of a uniform matroid of rank 3. So $r(\{4,5,6\}) = 3$ contradicts the 3-element circuit of P_6. □

5.5 Matroid P_8

Definition 5.11. *The matroid P_8 is a rank-4 matroid on 8 points whose circuits are the squares $\{1,2,3,4\},\{5,6,7,8\}$ of Fig. 7 and the sets formed by diagonals of one square and the sides of the other square, that are parallel to the diagonal.*

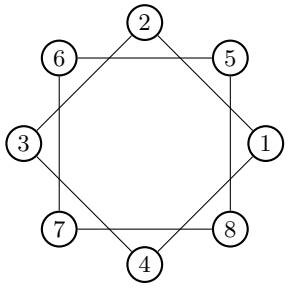


Fig. 7: P_8 matroid

For example, the diagonal $2,4$ and the side $5,8$ form the circuit $\{2,4,5,8\}$. P_8 is known to be $\mathbb{F}$-linear only for odd characteristic fields. Therefore, it is k-entropic for all odd k. Moreover, we show in Section B.4 that it is not multilinear over $\mathbb{F}_2$. In the following result, we see that it does not admit a 4-entropic representation.

Theorem 5.12. *The matroid P_8 is not 4-entropic.*

Proof. Consider a 4-entropic representation of P_8 with table M satisfying the property of Theorem 2.7.

We classify the circuits of rank 3 if the matroid P_8 into two classes:

$$\mathcal{S} = \{\{1,2,6,8\},\{3,4,6,8\},\{2,4,5,8\},\{2,4,6,7\}\} \text{ and}$$

$$\mathcal{T} = \{\{1,2,3,4\},\{5,6,7,8\}\}$$

By Lemma 2.36, for every circuit $C \in \mathcal{S}$ the table M_C, i.e., the restriction of the table M to the columns in the circuit C, is a latin cube of dimension 3 and order 4. For every $i \in \{1,3,5,7\}$, we denote H^i by the latin cube determined by the table M_C, where C is the circuit in $\mathcal{S}$ that contains i. Moreover, for each H^i we can consider the projection to one of its 2-dimensional arrays, which is equivalent to taking the contraction of the table M_C at some column j, if C is the circuit of $\mathcal{S}$ that contains i and $j \in C$. This is, $(\mathsf{M}_C)_{j:a}$ for every $a \in \{0,1,2,3\}$.

Then, for every $i \in \{1,3,5,7\}$ and $j \in \{2,4,6,8\}$ such that j is in the circuit C of $\mathcal{S}$ containing i, four latin squares are deduced

$$\{H^i_{j:0}, H^i_{j:1}, H^i_{j:2}, H^i_{j:3}\}$$

corresponding to the respective tables

$$\{(\mathsf{M}_C)_{j:0}, (\mathsf{M}_C)_{j:1}, (\mathsf{M}_C)_{j:2}, (\mathsf{M}_C)_{j:3}\}$$

First, we observe that all latin squares that come from this setting, i.e. all $H^i_{j:a}$, are isotopic to the Cayley table of the group V_4. We prove this by checking that they are orthogonal to another latin square.

Note that we can only take the contraction to the points in the respective circuit. For example, if $C = \{1, 2, 6, 8\}$, $H^1_{2:a}$ is the latin square determined by the table $(\mathsf{M}_C)_{2:a}$ but $H^1_{4:a}$ is not well defined since the table M_C does not have the column 4.

Claim 1. $H^1_{6:a} \perp H^5_{4:b}$ for all $a, b \in \{0, 1, 2, 3\}$.

Proof. First note that the projection $H^1_{6:a}$ and $H^5_{4:b}$ are well defined since the sets $\{1, 2, 6, 8\}$ and $\{2, 4, 5, 8\}$ are circuits.

Let $c, d \in \{0, 1, 2, 3\}$. We find the positions of the latin squares $H^1_{6:a}$ and $H^5_{4:b}$ such that they take the values c and d, respectively. Since the set $\{1, 4, 5, 6\}$ is independent, there is only one row in M with c, b, d, a values at columns $1, 4, 5, 6$ (Theorem 2.7). Let r, s be the values of the columns 4 and 6 at this row, then, we have that

$$H^1_{6:a}(r, s) = c \text{ and } H^5_{4:b}(r, s) = d.$$

Since the row of M is unique, there is no more position (r', s') such that

$$H^1_{6:a}(r', s') = c \text{ and } H^5_{4:b}(r', s') = d$$

so, $H^1_{6:a}$ and $H^5_{4:b}$ are orthogonal latin squares. □

Following an analogous argument as in Claim 1 and using the fact that the sets $\{1, 4, 5, 6\}$, $\{1, 4, 7, 8\}$, $\{2, 3, 5, 6\}$, and $\{2, 3, 7, 8\}$ are independent, we deduce

$$H^1_{6:a} \perp H^5_{4:b}, \quad H^1_{8:a} \perp H^7_{4:b}, \quad H^3_{6:a} \perp H^5_{2:b}, \quad H^3_{8:a} \perp H^7_{2:b} \tag{12}$$

By Lemma 2.23, for every $i_1 \in \{1, 3, 5, 7\}$, $j_2 \in \{2, 4, 6, 8\}$ and $a \in \{0, 1, 2, 3\}$ such that the square $H^{i_1}_{j_2:a}$ is well defined, there exists a permutation $\sigma_{i_1,j_1,a}$ satisfying that for some τ,

$$H^{i_1}_{j_1:a}(r, s) = \tau(\sigma_{i_1,j_1,a}(r) \circ s).$$

From now on, we fix $a = 0$ and denote $\sigma_{i,j} := \sigma_{i,j,0}$. Therefore, we have the following permutations:

σ	2	4	6	8
1	$\sigma_{1,2}$		$\sigma_{1,6}$	$\sigma_{1,8}$
3		$\sigma_{3,4}$	$\sigma_{3,6}$	$\sigma_{3,8}$
5	$\sigma_{5,2}$	$\sigma_{5,4}$		$\sigma_{5,8}$
7	$\sigma_{7,2}$	$\sigma_{7,4}$	$\sigma_{7,6}$	

By the orthogonality properties described in (12), we deduce the relations

$$\sigma_{1,6} \perp \sigma_{5,4}, \quad \sigma_{1,8} \perp \sigma_{7,4}, \quad \sigma_{3,6} \perp \sigma_{5,2}, \quad \sigma_{3,8} \perp \sigma_{7,2}. \tag{13}$$

Claim 2. $\sigma_{1,2} = \sigma_{3,4}$ and $\sigma_{7,6} = \sigma_{5,8}$.

Proof. Since $\{1,2,3,4\}$ is a circuit, the value of the column 3 is determined by the values of the columns $1,2,4$ in each row of M. Moreover, every 4-tuple in the columns $\{1,2,3,4\}$ appears 4 times.

Consider the four positions (r_i, s_i), $1 \leq i \leq 4$, where the latin square $H^1_{2:0}$ takes the value a. These are in correspondence with the values in columns $6,8$ of the rows in the table M that have values $a,0$ in columns $1,2$. Since $H^1_{2:0}$ is independent of the value of the column 4, we take the four rows that have values $a,0,0$ in columns $1,2,4$, and they have values r_i, s_i in columns $6,8$, for $1 \leq i \leq 4$. Now, since $\{1,2,3,4\}$ is a circuit, all these rows have the same value in the column 3, say b. Note that the values of the columns $6,8$ in these four rows, say r, s are the positions where the latin square $H^3_{4:0}$ has the value b. Hence, for every value a such that $H^1_{2:0}(r,s) = a$, $H^3_{4:0}(r,s) = b$, so $H^1_{2:0}$ and $H^3_{4:0}$ are symbol-isotopic and $\sigma_{1,2} = \sigma_{3,4}$.

An equivalent argument works for the latin squares $H^7_{6:0}$ and $H^5_{8:0}$, deducing that $\sigma_{7,6} = \sigma_{5,8}$. □

Claim 3. $\sigma_{1,8} \circ \sigma_{5,8} \perp \sigma_{3,8}$

Proof. This relation comes from the fact that $\{1,3,5,8\}$ is independent.

Recall from Lemma 5.5 that orthogonality of permutations of 3 elements is equivalent to not having intersection points, i.e. we want that that for all $x \in \{1,2,3\}$, $\sigma_{1,8} \circ \sigma_{5,8}(x) \neq \sigma_{3,8}(x)$.

Suppose that there is some $a \in \{1,2,3\}$ such that

$$\sigma_{1,8} \circ \sigma_{5,8}(a) = \sigma_{3,8}(a). \tag{14}$$

Then, we next proof that there are two rows of the table M such that the columns $1,3,5,8$ take the same value, and by Theorem 2.7 this is a contradiction since $\{1,3,5,8\}$ is independent.

Let $\{j_1, j_2, j_3\} = \{2,4,6,8\} \setminus \{j\}$. Since $\{2,4,6,8\}$ is a basis, there is a row in the table with columns $\{2,4,6,8\}$ taking any value. Take the value a satisfying (14). This is, $\sigma_{1,8}(\sigma_{5,8}(a)) = \sigma_{3,8}(a)$. Consider the row with values in columns j_1, j_2, j_3, j

$$a, \sigma_{5,8}(a), \sigma_{3,8}(a), 0.$$

Note that the sets $\{1,2,6,8\}, \{3,4,6,8\}$, and $\{2,4,5,8\}$ are circuits. Hence, the latin squares $H^i_{8:0}$ are well defined for every $i \in \{1,3,5\}$. Recall from Lemma 2.23 that for every $i \in \{1,3,5\}$, $H^i_{8:0}$ satisfies that

$$H^i_{8:0}(r,s) = \tau_{i,8}(\sigma_{i,8}(r) \cdot s).$$

Then,

$$H^1_{8:0}(\sigma_{5,8}(a), \sigma_{3,8}(a)) = \tau_{1,8}(\sigma_{1,8}(\sigma_{5,8}(a)) \cdot \sigma_{3,8}(a)) = \tau_{1,8}(0),$$
$$H^3_{8:0}(a, \sigma_{3,8}(a)) = \tau_{3,8}(\sigma_{3,8}(a) \cdot \sigma_{3,8}(a)) = \tau_{3,8}(0),$$
$$H^5_{8:0}(a, \sigma_{5,8}(x)) = \tau_{5,8}(\sigma_{5,8}(a) \cdot \sigma_{5,8}(a)) = \tau_{5,8}(0).$$

So the row has values $\tau_{1,8}(0), \tau_{3,8}(0), \tau_{5,8}(0), 0$ at the columns $1, 2, 3, 8$.

Consider also the row with values $0, 0, 0, 0$ in the columns $j_1, j_2, j_3, 8$. Since $H^i_{8:0}(0, 0) = \tau_{i_\ell,8}(0)$ for every $i \in \{1, 3, 5\}$, we have that this row has same values in the columns $1, 3, 5, 8$ than the previous one, but different values at columns j_1, j_2, j_3 since $a, \sigma_{5,8}(a), \sigma_{3,8}(a) \neq 0$. Then, this contradicts the fact that $\{1, 3, 5, 8\}$ is independent. □

From the independence of $\{1, 2, 5, 7\}$, $\{1, 3, 6, 7\}$ and $\{3, 4, 5, 7\}$ and analogous arguments we deduce the relations

$$\begin{aligned} &\sigma_{1,8} \circ \sigma_{5,8} \perp \sigma_{3,8}, && \sigma_{1,2} \circ \sigma_{7,2} \perp \sigma_{5,2}, \\ &\sigma_{1,6} \circ \sigma_{7,6} \perp \sigma_{3,6}, && \sigma_{3,4} \circ \sigma_{7,4} \perp \sigma_{5,4}. \end{aligned} \tag{15}$$

From the properties presented above, we know that

$$\sigma_{5,2} \perp \sigma_{3,6} \quad \text{and} \quad \sigma_{5,2} \perp \sigma_{1,2} \circ \sigma_{7,2}.$$

Composing with $\sigma_{7,6}$ we get

$$\sigma_{5,2} \circ \sigma_{7,6} \perp \sigma_{3,6} \circ \sigma_{7,6} \quad \text{and} \quad \sigma_{5,2} \circ \sigma_{7,6} \perp \sigma_{1,2} \circ \sigma_{7,2} \circ \sigma_{7,6}.$$

Due to Claim 2 and Lemma 5.8, we have that

$$\sigma_{5,2} \circ \sigma_{7,6} = \sigma_{5,2} \circ \sigma_{5,8} = \sigma_{5,4}.$$

Hence,

$$\sigma_{5,4} \perp \sigma_{3,6} \circ \sigma_{7,6}, \quad \sigma_{5,4} \perp \sigma_{1,2} \circ \sigma_{7,2} \circ \sigma_{7,6}, \quad \text{and} \quad \sigma_{5,4} \perp \sigma_{1,6},$$

where the last property is a consequence of Claim 1.

Observe that the orthogonal mates of a permutation σ of 3 elements satisfy that they are identical or orthogonal.

Since there are at most 3 MOLS of order 4, two of the previous permutations coincide. two of the three previous squares that are orthogonal with $\sigma_{5,4}$ coincide. Next we analyze the possible cases.

- If $\sigma_{3,6} \circ \sigma_{7,6} = \sigma_{1,2} \circ \sigma_{7,2} \circ \sigma_{7,6}$ then

  $$\sigma_{3,6} = \sigma_{1,2} \circ \sigma_{7,2} \implies \sigma_{1,2} \circ \sigma_{3,8} = \sigma_{1,2} \circ \sigma_{7,2} \implies \sigma_{3,8} = \sigma_{7,2}$$

  and this contradicts the fact that $\{2, 3, 7, 8\}$ is independent.
- If $\sigma_{3,6} \circ \sigma_{7,6} = \sigma_{1,6}$, this contradicts the independence of $\{1, 3, 6, 7\}$ by (15).
- If $\sigma_{1,2} \circ \sigma_{7,2} \circ \sigma_{7,6} = \sigma_{1,6}$ then since $\sigma_{1,6} = \sigma_{1,2} \circ \sigma_{1,8}$ we have

  $$\sigma_{1,2} \circ \sigma_{1,8} = \sigma_{1,2} \circ \sigma_{7,2} \circ \sigma_{7,6} \implies \sigma_{1,8} = \sigma_{7,2} \circ \sigma_{7,6} = \sigma_{7,4}$$

  and this contradicts the independence of $\{1, 4, 7, 8\}$ by (13).

We have seen that such table M satisfying the independence and dependence relations of the matroid P_8 cannot exist; then P_8 is not 4-entropic. □

5.6 Matroid P_8''

Definition 5.13. *The matroid P_8'' is a rank-4 matroid on 8 points that has all the circuits of the matroid P_8 except for the two 4-element circuits that are disjoint (see Fig. 7).*

It is $\mathbb{F}$-linear only for fields with more than 5 elements. Therefore, the matroid P_8'' is k-entropic for all prime powers k, $k \geq 5$. In Section B.4 we observe that it does not admit a 2-linear representation over $\mathbb{F}_2$. In the following result, we show that it does not admit a 4-entropic representation.

Theorem 5.14. *The matroid P_8'' is not 4-entropic.*

Proof. Consider an entropic representation of P_8'' over the set $\{0,1,2,3\}$ with table M satisfying the property of Theorem 2.7.

In contrast to the matroid P_8, the only circuits of rank 3 that have the matroide P_8'' are those in class $\mathcal{S}$.

$$\mathcal{S} = \{\{1,2,6,8\},\{3,4,6,8\},\{2,4,5,8\},\{2,4,6,7\}\}$$

By Lemma 2.36, for every circuit $C \in \mathcal{S}$ the table M_C, i.e., the restriction of the table M to the columns of the circuit C, is a latin cube of dimension 3 and order 4. For every $i \in \{1,3,5,7\}$ we denote H^i the latin cube determined by the table M_C, where C is the circuit in $\mathcal{S}$ that contains i. Moreover, for each H^i we can consider the projection to one of its 2-dimensional arrays, which is equivalent to taking the contraction of the table M_C at some column j, if C is the circuit of $\mathcal{S}$ that contains i and $j \in C$. This is, $(\mathsf{M}_C)_{j:a}$ for every $a \in \{0,1,2,3\}$.

Then, for every $i \in \{1,3,5,7\}$ and $j \in \{2,4,6,8\}$ such that j is in the circuit C of $\mathcal{S}$ containing i, four latin squares are deduced

$$\{H^i_{j:0}, H^i_{j:1}, H^i_{j:2}, H^i_{j:3}\}$$

corresponding to the respective tables

$$\{(\mathsf{M}_C)_{j:0}, (\mathsf{M}_C)_{j:1}, (\mathsf{M}_C)_{j:2}, (\mathsf{M}_C)_{j:3}\}$$

First, we claim that each latin square $H^i_{j:a}$ is isotopic to V_4.

Note that we can only take the contraction to the points in the respective circuit. For example, if $C = \{1,2,6,8\}$, $H^1_{2:a}$ is the latin square determined by table $(\mathsf{M}_C)_{2:a}$ but $H^1_{4:a}$ is not well defined since the table M_C does not have the column 4.

By Lemma 2.23, for every $i_1 \in \{1,3,5,7\}$ and $j_2 \in \{2,4,6,8\}$ such that the square $H^{i_1}_{j_2:a}$ is well defined, i.e., $\{i_1, j_2, j_3, j_4\}$ is a circuit for some $j_3, j_4 \in \{2,4,6,8\}$, there exists a permutation $\sigma_{i_1 j_1:a}$ satisfying that for some $\tau_{i_1 j_1:a}$,

$$H^{i_1}_{j_1:a}(r,s) = \tau_{i_1 j_1:a}(\sigma_{i_1 j_1:a}(r) \cdot s).$$

Therefore, for every $a \in \{0,1,2,3\}$ we have the following permutations

a	2	4	6	8
1	$\sigma_{12:a}$		$\sigma_{16:a}$	$\sigma_{18:a}$
3		$\sigma_{34:a}$	$\sigma_{36:a}$	$\sigma_{38:a}$
5	$\sigma_{52:a}$	$\sigma_{54:a}$		$\sigma_{58:a}$
7	$\sigma_{72:a}$	$\sigma_{74:a}$	$\sigma_{76:a}$	

Moreover, from Lemma 5.8 we have the following relations:

$$\sigma_{12:a} \circ \sigma_{18:a} = \sigma_{16:a},$$
$$\sigma_{34:a} \circ \sigma_{38:a} = \sigma_{36:a},$$
$$\sigma_{52:a} \circ \sigma_{58:a} = \sigma_{54:a}, \tag{16}$$
$$\sigma_{72:a} \circ \sigma_{76:a} = \sigma_{74:a}. \tag{17}$$

Claim 4. For every a and b,

$$H^1_{2:a} \perp H^3_{4:b} \text{ and } H^7_{6:a} \perp H^5_{8:b}$$

Proof. Take the rows of the table M that have as columns 2 and 4 the values a and b, respectively. Since $\{1,2,3,4\}$ is independent, when looking at the columns $\{1,3\}$, each pair (c,d) appears only once. Note that the columns 1 and 3 of this subtable are indeed the value of the latin squares $H^1_{2:a}$ and $H^3_{4:b}$ respectively. Therefore, each pair (c,d) appears once in the superimposition of the latin squares $H^1_{2:a}$ and $H^3_{4:b}$, hence they are orthogonal. Similarly, taking the rows that have as columns $6,8$ the values a and b, we obtain $H^7_{6:a} \perp H^5_{8:b}$. □

From this we can deduce that $\sigma_{12:0} \perp \sigma_{34:0}$ and $\sigma_{12:a} \perp \sigma_{34:0}$. By Lemma 5.7, $H^1_{2:0}$ and $H^1_{2:a}$ are not orthogonal. But since they are both orthogonal to $H^3_{4:0}$, we can deduce $\sigma_{12:0} = \sigma_{12:a}$. In other words, the latin squares $H^1_{2:0}$ and $H^1_{2:a}$ are symbol isotopic for every $a \in \{1,2,3\}$. Similarly with the latin squares $H^3_{4:0}$ and $H^3_{4:a}$.

Claim 5. $\sigma_{34:0} \circ \sigma_{72:0} \perp \sigma_{52:0}$.

Proof. Since the set $\{2,3,5,7\}$ is dependent, every row that has the same values in columns $2,5,7$ has the same value in column 3. Take the row ω with all 0 in columns $2,4,6,8$, then the values in $3,5,7$ are

$$\tau_{34:0}(0), \quad \tau_{52:0}(0), \quad \tau_{72:0}(0).$$

Now, take another row ω' with values in $\{2,4,6,8\}$, $0, a, \sigma_{72:0}(a), \sigma_{52:0}(a)$, respectively, with $a \in \{1,2,3\}$. Then

$$H^5_{2:0}(a, \sigma_{52:0}(a)) = \tau_{52:0}(\sigma_{52:0}(a) \cdot \sigma_{52:0}(a)) = \tau_{52:0}(0),$$
$$H^7_{2:0}(a, \sigma_{72:0}(a)) = \tau_{72:0}(\sigma_{72:0}(a) \cdot \sigma_{72:0}(a)) = \tau_{72:0}(0).$$

Note that the rows ω and ω' coincide in columns $2,5,7$, so their values in column 3 must coincide. So

$$H^3_{4:a}(\sigma_{72:0}(a), \sigma_{52:0}(a)) = \tau_{34:0}(0). \tag{18}$$

Note that from previous observation, $H^3_{4:0}$ and $H^3_{4:a}$ are symbol isotopic. Hence, there is a fixed point free permutation τ such that for every $r, s \in \{0,1,2,3\}$,

$$H^3_{4:a}(r,s) = \tau(H^3_{4:0}(r,s)).$$

In other words, $H^3_{4:a}(r,s) \neq H^3_{4:0}(r,s)$. If $r = \sigma_{72:0}(a)$ and $s = \sigma_{52:0}(a)$, note from (18) that

$$H^3_{4:a}(r,s) = \tau_{34:0}(0) = H^3_{4:0}(0,0)$$

then, since $H^3_{4:0}(r,s) \neq H^3_{4:0}(0,0)$.

$$H^3_{4:0}(r,s) = \tau_{34:0}(\sigma_{34:0}(\sigma_{72:0}(a)) \cdot \sigma_{52:0}(a)) \neq \tau_{34:0}(0)$$

then

$$\sigma_{34:0}(\sigma_{72:0}(a)) \neq \sigma_{52:0}(a).$$

Since a is any value of $\{1,2,3\}$, we have that the permutations $\sigma_{34:0} \circ \sigma_{72}$ and $\sigma_{52:0}$ do not intersect, hence

$$\sigma_{34:0} \circ \sigma_{72:0} \perp \sigma_{52:0}.$$

□

We can make a similar argument for the circuit 1457:

Claim 6. $\sigma_{12:0} \circ \sigma_{74:0} \perp \sigma_{54:0}$.

Proof. Take the row ω with the value 0 in columns $2,4,6,8$, then the values in $1,5,7$ are

$$\tau_{12:0}(0), \quad \tau_{54:0}(0). \quad \tau_{74:0}(0)$$

Now, take another row ω' with values in $2,4,6,8$: $a, 0, \sigma_{74:0}(a).\sigma_{54:0}(y)$, with $a \in \{1,2,3\}$. Then

$$H^5_{4:0}(a, \sigma_{54:0}(a)) = \tau_{54:0}(\sigma_{54:0}(a) \cdot \sigma_{54:0}(a)) = \tau_{54:0}(0)$$
$$H^7_{4:0}(a, \sigma_{74:0}(a)) = \tau_{74:0}(\sigma_{74:0}(a) \cdot \sigma_{74:0}(a)) = \tau_{74:0}(0)$$

Note that the rows ω and ω' coincide in columns $4,5,7$, so their values in column 1 must coincide. So,

$$H^1_{2:a}(\sigma_{74:0}(a), \sigma_{54:0}(a)) = \tau_{12:0}(0). \tag{19}$$

Note that from previous observation, $H^1_{2:0}$ and $H^1_{2:a}$ are symbol isotopic, so there is a fixed point free permutation τ such that for every $r, s \in \{0,1,2,3\}$,

$$H^1_{2:a}(r,s) = \tau(H^1_{2:0}(r,s))$$

In other words, $H^1_{2:a}(r,s) \neq H^1_{2:0}(r,s)$. If $r = \sigma_{74:0}(a)$ and $s = \sigma_{54:0}(a)$, from (19) we get

$$H^1_{2:a}(r,s) = \tau_{12:0}(0) = H^1_{2:0}(0,0)$$

then, since $H^1_{2:0}(r,s) \neq H^1_{2:0}(0,0)$,

$$H^1_{2:0}(r,s) = \tau_{12:0}(\sigma_{12:0}(\sigma_{74:0}(a)) \cdot \sigma_{54:0}(a)) \neq \tau_{12:0}(0)$$

$$\sigma_{12:0}(\sigma_{74:0}(a)) \neq \sigma_{54:0}(a)$$

Since a is any value of $\{1,2,3\}$, we have that the permutations $\sigma_{12:0} \circ \sigma_{74:0}$ and $\sigma_{54:0}$ do not intersect, hence

$$\sigma_{12:0} \circ \sigma_{74:0} \perp \sigma_{54:0}.$$

□

Note that from the previous claims we deduce

$$\sigma_{12:0} \perp \sigma_{54:0} \circ \sigma^{-1}_{74:0}, \quad \text{and} \quad \sigma_{34:0} \perp \sigma_{52:0} \circ \sigma^{-1}_{72:0}.$$

Since $\sigma_{34:0} \perp \sigma_{12:0}$ and there are at most 3 MOLS of order 4, we find that one of these equalities holds.

$$\sigma_{54:0} \circ \sigma^{-1}_{74:0} = \sigma_{52:0} \circ \sigma^{-1}_{72:0} \tag{20}$$

$$\sigma_{34:0} = \sigma_{54:0} \circ \sigma^{-1}_{74:0} \tag{21}$$

$$\sigma_{12:0} = \sigma_{52:0} \circ \sigma^{-1}_{72:0} \tag{22}$$

We show that none of these options is possible for a 4-entropic representation of the matroid P''_8.

Suppose first that (20) holds, then apply relations (16),(17)

$$\begin{aligned}
\sigma_{54:0} \circ \sigma^{-1}_{74:0} &= \sigma_{52:0} \circ \sigma^{-1}_{72:0} \\
\sigma_{52:0} \circ \sigma_{58:0} &= \sigma_{52:0} \circ \sigma^{-1}_{72:0} \circ \sigma_{72:0} \circ \sigma_{76:0} \\
\sigma_{52:0} \circ \sigma_{58:0} &= \sigma_{52:0} \circ \sigma_{76:0} \\
\sigma_{58:0} &= \sigma_{76:0}.
\end{aligned}$$

Contradicting the fact that the set $\{5,6,7,8\}$ is independent.

Now we show the impossibility of (21) and (22). Take the row ω of the table that has 0 as values in columns $2,4,6,8$. Then, the columns $1,3,5,7$ take values

$$\tau_{12:0}(0), \tau_{34:0}(0), \tau_{52:0}(0), \tau_{72:0}(0)$$

Now, if $a \in \{1,2,3\}$, take the row ω' with values at $2,4,6,8$: $a, 0, \sigma_{74:0}(a), \sigma_{54:0}(a)$, for some $a \in \{1,2,3\}$. Then

$$H^5_{4:0}(a, \sigma_{54:0}(a)) = \tau_{54:0}(0),$$

$$H^7_{4:0}(a, \sigma_{74:0}(a)) = \tau_{74:0}(0).$$

And by circuit $\{1,4,5,7\}$,

$$H^1_{4:0}(\sigma_{74:0}(a), \sigma_{54:0}(a)) = \tau_{12:0}(0).$$

Since $\{1,3,5,7\}$ is independent and the rows ω and ω' coincide in the columns $1,5,7$, the value of the column 3 must differ from $\tau_{34:0}(0)$ and

$$\begin{aligned} H^3_{4:0}(\sigma_{74:0}(a), \sigma_{54:0}(a)) &\neq \tau_{34:0}(0), \\ \tau_{34:0}(\sigma_{34:0}(\sigma_{74:0}(a), \sigma_{54:0}(a)) &\neq \tau_{34:0}(0), \\ \sigma_{34:0}(\sigma_{74:0}(a)) &\neq \sigma_{54:0}(a), \end{aligned}$$

contradicting (21).

Finally, using a similar argument as before, we find that for any $a \in \{1,2,3\}$

$$\sigma_{12:0}(\sigma_{72:0}(a)) \neq \sigma_{52:0}(a).$$

□

AI Use Statement. AI-based tools were used solely for language editing, including improving the clarity and style of the text and correcting grammatical and typographical errors. No AI-based tools were used to develop the ideas, results, or proofs presented in this paper.

References

AA18. Benny Applebaum and Barak Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. In *TCC 2018*, volume 11239 of *LNCS*, pages 317–344, 2018.

AARV21. Benny Applebaum, Barak Arkis, Pavel Raykov, and Prashant Nalini Vasudevan. Conditional disclosure of secrets: Amplification, closure, amortization, lower-bounds, and separations. *SIAM J. Comput.*, 50(1):32–67, 2021.

ABF+19. Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. In *EUROCRYPT 2019*, volume 11478 of *LNCS*, pages 441–471, 2019.

ABI+23. Damiano Abram, Amos Beimel, Yuval Ishai, Eyal Kushilevitz, and Varun Narayanan. Cryptography from planted graphs: Security with logarithmic-size messages. In *TCC 2023*, volume 14365 of *LNCS*, pages 286–315. Springer, 2023.

ABL24. Bar Alon, Amos Beimel, and Or Lasri. Simplified PIR and CDS protocols and improved linear secret-sharing schemes. Technical Report 2024/1599, IACR Cryptology ePrint Archive, 2024.

ABNP20. Benny Applebaum, Amos Beimel, Oded Nir, and Naty Peter. Better secret sharing via robust conditional disclosure of secrets. In *52nd STOC*, pages 280–293, 2020.

AN21. Benny Applebaum and Oded Nir. Upslices, downslices, and secret-sharing with complexity of 1.5^n. In *CRYPTO 2021*, volume 12827 of *LNCS*, pages 627–655, 2021.

AS19. Emmanuel Abbe and Sophie Spirkl. Entropic matroids and their representation. *Entropy*, 21(10), 2019.

Bal12. Simeon Ball. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *Journal of the European Mathematical Society*, 14(3):733–748, 2012.

BBFP20. Michael Bamiloshin, Aner Ben-Efraim, Oriol Farràs, and Carles Padró. Common information, matroid representation, and secret sharing for matroid ports. *Designs, Codes, and Cryptography*, pages 1–24, 2020.

BBFP21. Michael Bamiloshin, Aner Ben-Efraim, Oriol Farràs, and Carles Padró. Common information, matroid representation, and secret sharing for matroid ports. *Des. Codes Cryptogr.*, 89(1):143–166, 2021.

BC94. Amos Beimel and Benny Chor. Universally ideal secret-sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.

BD91. Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.

Bei25. Amos Beimel. Secret-sharing schemes for general access structures: An introduction. Cryptology ePrint Archive, Paper 2025/518, 2025.

Ben16. Aner Ben-Efraim. Secret-sharing matroids need not be algebraic. *Discrete Mathematics*, 339(8):2136–2145, 2016.

BF20. Amos Beimel and Oriol Farràs. The share size of secret-sharing schemes for almost all access structures and graphs. In *TCC 2020*, volume 12552 of *LNCS*, pages 499–529, 2020.

BFM25. Amos Beimel, Oriol Farràs, and Adriana Moya. Polynomial secret sharing schemes and algebraic matroids. In *TCC 2025*, volume 16269 of *LNCS*, pages 428–461. Springer, 2025.

BGI+26. Kristóf Bérczi, Boglárka Gehér, András Imolay, László Lovász, Carles Padró, and Tamás Schwarcz. Interaction between skew-representability, tensor products, extension properties, and rank inequalities. In *Proceedings of SODA 2026*, pages 328–354. SIAM, 2026.

BGK16. Andrej Bogdanov, Siyao Guo, and Ilan Komargodski. Threshold secret sharing requires a linear size alphabet. In Martin Hirt and Adam Smith, editors, *Theory of Cryptography*, pages 471–484, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

BGW88. Michael Ben-Or, Shaffi Goldwasser, and Avi Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computations. In *20th STOC*, pages 1–10, 1988.

BGW99. László Babai, Anna Gál, and Avi Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.

Bla79. George Robert Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, volume 48, pages 313–317, 1979.

Bla99. Simon R. Blackburn. Combinatorial designs and their applications. *Research Notes in Mathematics*, 403:44–70, 1999.

BLP08. Amos Beimel, N. Livne, and C. Padró. Matroids can be far from ideal secret sharing. In R. Canetti, editor, *Proc. of the Fifth Theory of Cryptography Conference – TCC 2008*, volume 4948 of *LNCS*, pages 194–212, 2008.

Bre25. Nick Brettell. The excluded minors for gf(5)-representable matroids on ten elements. *Advances in Applied Mathematics*, 166:102864, 2025.

BSP60. R. C. Bose, S. S. Shrikhande, and E. T. Parker. Further results on the construction of mutually orthogonal latin squares and the falsity of euler's conjecture. *Canadian Journal of Mathematics*, 12:189–203, 1960.

BTW05. Amos Beimel, Tamir Tassa, and Enav Weinreb. Characterizing ideal weighted threshold secret sharing. In *Proc. of the Second Theory of Cryptography Conference – TCC 2005*, volume 3378 of *LNCS*, pages 600–619. Springer-Verlag, 2005.

Bus50. Kenneth A. Bush. *Orthogonal arrays*. PhD thesis, North Carolina State University, 1950.

Bus52. Kenneth A. Bush. Orthogonal arrays of index unity. *Annals of Mathematical Statistics*, 23:426–434, 1952.

CCB25. Qi Chen, Minquan Cheng, and Baoming Bai. Matroidal entropy functions: Constructions, characterizations, and representations. *IEEE Transactions on Information Theory*, 71(4):3237–3249, 2025.

CCD88. David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols. In *20th STOC*, pages 11–19, 1988.

CCX13. Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Bounds on the threshold gap in secret sharing and its applications. *IEEE Trans. Inf. Theory*, 59(9):5600–5612, 2013.

CDG+08. Ronald Cramer, Vanesa Daza, Ignacio Gracia, Jorge Jiménez Urroz, Gregor Leander, Jaume Martí-Farré, and Carles Padró. On codes, matroids, and secure multiparty computation from linear secret-sharing schemes. *IEEE Transactions on Information Theory*, 54(6):2644–2657, 2008.

CDM00. Ronald Cramer, Ivan Damgård, and Ueli Maurer. General secure multiparty computation from any linear secret-sharing scheme. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 316–334. Springer-Verlag, 2000.

Csi19. László Csirmaz. Secret sharing and duality. *Journal of Mathematical Cryptology*, 15:157 – 173, 2019.

DF92. Yvo Desmedt and Yair Frankel. Classification of ideal homomorphic threshold schemes over finite abelian groups. In *Proceedings of the 11th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'92, page 25–34, Berlin, Heidelberg, 1992. Springer-Verlag.

DK15. József Dénes and Anthony D. Keedwell. Latin squares and their applications: Second edition. *Latin Squares and their Applications: Second Edition*, pages 1–424, 01 2015.

DMR93. Ed Dawson, Ebadollah S. Mahmoodian, and Alan Rahilly. Orthogonal arrays and ordered threshold schemes. *Australasian Journal of Combinatorics*, 8:27–44, 1993.

Efr12. Klim Efremenko. 3-query locally decodable codes of subexponential length. *SIAM J. Comput.*, 41(6):1694–1703, 2012.

EM12. John T. Ethier and Gary L. Mullen. Strong forms of orthogonality for sets of hypercubes. *Discrete Mathematics*, 312(12):2050–2061, 2012.

Eul82. Leonhard Euler. Recherches sur un nouvelle espèce de quarrés magiques. *Euler Archive - All Works*, 530, 1782.

Eva89. Anthony B. Evans. Orthomorphisms of groups. *Annals of the New York Academy of Sciences*, 555(1):187–191, 1989.

FGU25. Raúl M. Falcón, Jaime Gutiérrez, and Jorge Jiménez Urroz. An algebraic approach to latin squares of prime power order by local permutation polynomials. Technical report, arxiv.org, 2025.

FKMP20. Oriol Farràs, Tarik Kaced, Sebastià Martín, and Carles Padró. Improving the linear programming technique in the search for lower bounds in

secret sharing. *IEEE Transactions on Information Theory*, 66(11):7088–7100, 2020.

FMP12. Oriol Farràs, Jaume Martí-Farré, and Carles Padró. Ideal multipartite secret sharing schemes. *J. Cryptology*, 25(3):434–463, 2012.

FP12. Oriol Farràs and Carles Padró. Ideal hierarchical secret sharing schemes. *IEEE Transactions on Information Theory*, 58(5):3273–3286, 2012.

FPXY14. Oriol Farràs, Carles Padró, Chaoping Xing, and An Yang. Natural generalizations of threshold secret sharing. *IEEE Transactions on Information Theory*, 60(3):1652–1664, 2014.

GGK00. James F. Geelen, Albertus M. H. Gerards, and Ajai Kapoor. The excluded minors for GF(4)-representable matroids. *Journal of Combinatorial Theory, Series B*, 79(2):247–299, 2000.

GGW14. Jim Geelen, Bert Gerards, and Geoff Whittle. Solving Rota's conjecture. *Notices of the American Mathematical Society*, 61(7):736–743, 2014.

Gol98. Jovan Dj Golić. On matroid characterization of ideal secret sharing schemes. *Journal of Cryptology*, 11(2):75–86, 1998.

GPSW06. Viput Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th CCS*, pages 89–98, 2006.

HSS12. A.S. Hedayat, N.J.A. Sloane, and J. Stufken. *Orthogonal Arrays: Theory and Applications*. Springer Series in Statistics. Springer New York, 2012.

ISN87. Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing schemes realizing general access structure. In *Globecom 87*, pages 99–102, 1987. Journal version: Multiple assignment scheme for sharing secret. *J. of Cryptology*, 6(1), 15-20, 1993.

Kac18. Tarik Kaced. Information inequalities are not closed under polymatroid duality. *IEEE Transactions on Information Theory*, 64(6):4379–4381, 2018.

KGH83. Ehud D. Karnin, Jonathan W. Greene, and Martin E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.

KK26. Mohammad Hossein Kalantari and Shahram Khazaei. Four-entropic matroids are quaternary. Technical Report 2608.20553, 2026. `https://arxiv.org/abs/2608.20553`.

KN90. Joe Kilian and Noam Nisan. Private communication, 1990.

KY22. Lukas Kühne and Geva Yashfe. Representability of matroids by c-arrangements is undecidable. *Israel Journal of Mathematics*, 252(1):95–147, September 2022.

KY26. Lukas Kühne and Geva Yashfe. On entropic and almost multilinear representability of matroids. *Duke Mathematical Journal. Advance publication*, page 1–89, 2026.

Leh64. Alfred Lehman. A solution of the shannon switching game. *Journal of the Society for Industrial and Applied Mathematics*, 12(4):687–725, 1964.

LV18. Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *50th STOC*, pages 699–708, 2018.

LVW17. Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *CRYPTO 2017*, volume 10401 of *LNCS*, pages 758–790, 2017.

Mar91. Keith M. Martin. *Discrete Structures in the Theory of Secret Sharing*. PhD thesis, University of London, 1991.

Mat93. František Matúš. Probabilistic conditional independence structures and matroid theory: Background. *International Journal of General Systems*, 22(2):185–196, 1993.

Mat99. František Matúš. Matroid representations by partitions. *Discrete Mathematics*, 203:169–194, 1999.

Mat18. František Matúš. Classes of matroids closed under minors and principal extensions. *Combinatorica*, 38:935–954, 2018.

MP07. Jaume Martí-Farré and Carles Padró. On secret sharing schemes, matroids and polymatroids. In Salil Vadhan, editor, *Proc. of the Fourth Theory of Cryptography Conference – TCC 2007*, volume 4392 of *LNCS*, pages 253–272. Springer-Verlag, 2007.

MP10. Jaume Martí-Farré and Carles Padró. On secret sharing schemes, matroids and polymatroids. *J. Mathematical Cryptology*, 4(2):95–120, 2010.

MPY16. Sebastià Martín, Carles Padró, and Ann Yang. Secret sharing, rank inequalities, and information inequalities. *IEEE Trans. Inform. Theory*, 62:599–609, 2016.

MR08. Dillon Mayhew and Gordon F. Royle. Matroids with nine elements. *Journal of Combinatorial Theory, Series B*, 98(2):415–431, 2008.

MS81. R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, 24:583–584, September 1981.

Nel18. Peter Nelson. Almost all matroids are nonrepresentable. *Bulletin of the London Mathematical Society*, 50(2):245–248, 2018.

Nis91. Noam Nisan. Lower bounds for non-commutative computation. In *Proc. of the 23th ACM Symp. on the Theory of Computing*, pages 410–418, 1991.

Oxl11. James G. Oxley. *Matroid theory*. Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, second edition, 2011.

PG06. Carles Padró and Ignacio Gracia. Representing small identically self-dual matroids by self-dual codes. *SIAM J. Discrete Math.*, 20(4):1046–1055, 2006.

PR20. Anat Paskin-Cherniavsky and Artiom Radune. On polynomial secret sharing schemes. In *ITC 2020*, volume 163 of *LIPIcs*, pages 12:1–12:21, 2020.

PVY13. Carles Padró, Leonor Vázquez, and An Yang. Finding lower bounds on the complexity of secret sharing schemes by linear programming. *Discrete Applied Mathematics*, 161:1072–1084, 2013.

Rao46. Calyampudi Radhakrishna Rao. Difference sets and combinatorial arrangements derivable from finite geometries. *Proceedings of the National Institute of Sciences of India*, 12:123–135, 1946.

Rao47. C. Radhakrishna Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *Supplement to the Journal of the Royal Statistical Society*, 9(1):128–139, 1947.

RBG01. Lajos Rónyai, László Babai, and Murali K. Ganapathy. On the number of zero-patterns of a sequence of polynomials. *Journal of the AMS*, 14(3):717–735, 2001.

Rot70. Gian-Carlo Rota. Combinatorial theory, old and new. In *Actes du Congres International des Mathématiciens (Nice, 1970)*, volume 3, pages 229–233, 1970.

SA98. Juriaan Simonis and Alexei Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179–197, 1998.

Seg55. Beniamino Segre. Curve razionali normali e k-archi negli spazi finiti. *Ann. Mat. Pura Appl.*, 39(4):357–379, 1955.

Sey76a. P. D. Seymour. The forbidden minors of binary clutters. *Journal of the London Mathematical Society*, s2-12(3):356–360, 1976.

Sey76b. Paul D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.*, 27:407–413, 1976.

Sey92. Paul D. Seymour. On secret-sharing matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.

Sha79. Adi Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

Sin64. Richard C. Singleton. Maximum distance q -nary codes. *IEEE Trans. Inf. Theory*, 10:116–118, 1964.

Sti92. Douglas R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2:357–390, 1992.

Sti04. Douglas R. Stinson. *Combinatorial designs: constructions and analysis*. Springer, New York, NY, USA, 2004.

Tar00. Gaston Tarry. *Le problème des 36 officiers*. Secrétariat de l'Association française pour l'avancement des sciences, 1900.

Tut58. William T. Tutte. A homotopy theorem for matroids i,ii. *Transactions of the American Mathematical Society*, 88:144–160,161–174, 1958.

Wat11. Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 53–70. Springer-Verlag, 2011.

appendices

A Technical Proofs on Latin Squares and Orthogonal Arrays

In this appendix, we provide the formal proofs for the technical lemmas utilized throughout the paper.

Corollary A.1. *If $n \geq 2$, there do not exist $OA(t, n, k)$ if $n \geq t + k$.*

Proof. The Bush bound on Othogonal Arrays says that if the level n is greater than the strength t, then the factor n is bounded by

- If $k \leq t$ then $n \leq t + 1$
- If $k > t$ then $n \leq k + t - 1$ if n is even.
- If $k > t$ then $n \leq k + t - 2$ if n is odd.

Since $k + t > \max(t + 1, k + t - 1)$, the factor $n = k + t$ is too small to permit the existence of an orthogonal array with such parameters. □

Proof (Proof of Lemma 2.23). Let L be the Cayley table of $(G, \cdot)$. Since M is isotopic to L, then there exist three permutations of G (θ, ϕ, ψ) such that

$$M(i, j) = \psi(\theta(i) \cdot \phi(j)).$$

Let $\tau = \psi\phi$ and $\sigma = \phi^{-1}\theta$ then

$$M(i, j) = \psi\theta(i) \cdot \psi\phi(j) = \psi\phi(\phi^{-1}\theta(i) \cdot j) = \tau(\sigma(i) \cdot j)$$

Let 0 be the identity element of G, and we label $1, \ldots, n - 1$ for the rest of elements of G. Observe that τ is the permutation that maps $L(0, j)$ to $M(0, j)$ since $\tau(L(0, j)) = \tau(0 \cdot j) = M(0, j)$ and that σ is the permutation that maps the positions of the first row of M to the position occupying the first column since $M(0, \sigma(j)) = \tau(\sigma(j)) = M(j, 0)$. Note from this observation that the pair (τ, σ) is unique and that σ has 0 as fixed point since $M(0, \sigma(0)) = M(0, 0)$. □

A.1 Proof of Lemma 2.25

Lemma A.2. *Let L_1 and L_2 be two latin squares isotopic to the Cayley table L of a group $(G, \cdot)$. If L_1 and L_2 are determined by (σ_1, τ_1) and (σ_2, τ_2), respectively, then L_1 is orthogonal to L_2 if and only if $\sigma_1 \perp \sigma_2$.*

Recall that the orthogonality of permutations of groups is defined as follows. Let σ_1, σ_2 be permutations of G, following the notation from [Eva89], we say that σ_1 is *orthogonal* to σ_2, $\sigma_1 \perp \sigma_2$, if the mapping $x \mapsto \sigma_1(x)^{-1} \cdot \sigma_2(x)$ is a permutation of G. Then, we prove Lemma 2.25, which states that this notion of orthogonality can be related with orthogonality in latin squares. First, see Lemma A.3 proven in [Eva89], while Lemma 2.25 is a generalization proven in the following.

Lemma A.3. *Let L be the multiplication table of a group $(G, \cdot)$ and σ_1, σ_2 be permutations of G. Let L_σ be the latin square L permuting its rows by σ, i.e., $L_\sigma(i,j) = \sigma(i) \cdot j$. Then L_{σ_1} is orthogonal to L_{σ_2} if and only if $\sigma_1 \perp \sigma_2$.*

Proof (Proof of Lemma 2.25). Let L_1 and L_2 two latin squares isotopic to the Cayley table L of a group $(G, \cdot)$. By Lemma 2.23, there exist unique permutations (τ_1, σ_1), (τ_2, σ_2) such that

$$L_1(i,j) = \tau_1(\sigma_1(i) \cdot j), \quad L_2(i,j) = \tau_2(\sigma_2(i) \cdot j).$$

Define L_σ as in Lemma A.3, $L_\sigma(i,j) = \sigma(i) \cdot j$, then observe that.

$$L_1(i,j) = \tau_1(L_{\sigma_1}(i,j)), \quad L_2(i,j) = \tau_2(L_{\sigma_2}(i,j))$$

Since orthogonality of latin squares is preserved by permutations, L_1 and L_2 are orthogonal if and only if L_{σ_1} and L_{σ_2} are orthogonal. Finally, Lemma A.3 implies that

$$L_1 \perp L_2 \iff L_{\sigma_1} \perp L_{\sigma_2} \iff \sigma_1 \perp \sigma_2.$$

□

A.2 Latin Hypercubes of order 4

To clarify the definition of strong orthogonality with respect to orthogonality, we saw in Example 2.27 and Example 2.32 a pair of latin cubes of order 3 that are orthogonal but not strong orthogonal. Now we see an example of a pair of latin cubes of order 4 that are strong orthogonal, and as a consequence they are also orthogonal. Moreover, we also show a pair of latin cubes of order 4 that are not strong orthogonal. And these three cubes are a complete set of mutually orthogonal latin squares.

Example A.4. Consider the latin cube of order 4

$$C_1 = \begin{array}{c|c|c|c} 0\,1\,2\,3 & 1\,0\,3\,2 & 2\,3\,0\,1 & 3\,2\,1\,0 \\ 1\,0\,3\,2 & 0\,1\,2\,3 & 3\,2\,1\,0 & 2\,3\,0\,1 \\ 2\,3\,0\,1 & 3\,2\,1\,0 & 0\,1\,2\,3 & 1\,0\,3\,2 \\ 3\,2\,1\,0 & 2\,3\,0\,1 & 1\,0\,3\,2 & 0\,1\,2\,3 \end{array}$$

A strong orthogonal latin cube with C_1 is

$$C_2 = \begin{array}{c|c|c|c} 0\,2\,3\,1 & 1\,3\,2\,0 & 2\,0\,1\,3 & 3\,1\,0\,2 \\ 3\,1\,0\,2 & 2\,0\,1\,3 & 1\,3\,2\,0 & 0\,2\,3\,1 \\ 1\,3\,2\,0 & 0\,2\,3\,1 & 3\,1\,0\,2 & 2\,0\,1\,3 \\ 2\,0\,1\,3 & 3\,1\,0\,2 & 0\,2\,3\,1 & 1\,3\,2\,0 \end{array}$$

And a latin cube C_3 that is not strong orthogonal with C_1 but the set C_1, C_2, C_3 is 3-orthogonal is

$$C_3 = \begin{array}{c|c|c|c} 0\,1\,2\,3 & 1\,0\,3\,2 & 2\,3\,0\,1 & 3\,2\,1\,0 \\ 3\,2\,1\,0 & 2\,3\,0\,1 & 1\,0\,3\,2 & 0\,1\,2\,3 \\ 1\,0\,3\,2 & 0\,1\,2\,3 & 3\,2\,1\,0 & 2\,3\,0\,1 \\ 2\,3\,0\,1 & 3\,2\,1\,0 & 0\,1\,2\,3 & 1\,0\,3\,2 \end{array}$$

The reason that C_3 is not strong orthogonal with C_1 is that the squares defined by the first row of the cubes are not orthogonal, i.e. they are

$$\begin{array}{cccc} 0\,1\,2\,3 & & & 0\,1\,2\,3 \\ 1\,0\,3\,2 & & & 1\,0\,3\,2 \\ 2\,3\,0\,1 & & \text{and} & 2\,3\,0\,1 \\ 3\,2\,1\,0 & & & 3\,2\,1\,0 \end{array}$$

and therefore there are pairs in the superimposition of these 2-subarrays that are repeated. However, if we look at the superimposition of the three cubes, every very triple appears only once and then they are 3-orthogonal. △

B Alternative Proofs of Forbidden Minors

B.1 Uniform Matroids $U_{2,n}$ and $U_{4,6}$

There are two uniform forbidden minors for $\mathbb{F}_4$-linear representability: $U_{2,6}$ and $U_{4,6}$. We show that they are not 4-entropic.

For the first one, $U_{2,6}$ we use that for $k \geq 2$, the uniform matroid $U_{2,k+2}$ is not k-entropic. This follows from Theorem 2.21 and the fact that there are at most $k-1$ MOLS of order k. Hence, we have the following result:

Proposition B.1. *The matroids $U_{2,n}$ are not 4-entropic if $n \geq 6$.*

An alternative proof for this result can be found in [AS19]. Moreover, using the equivalence of the entropic representations of uniform matroids with orthogonal arrays, a k-entropic representation of $U_{2,n}$ implies the existence of a set of $n-1$ MOLS of order k. The Bush Bound Lemma 2.15 states that if an $OA(2,n,k)$ exists, then $n \leq k+1$, so $n \leq 5$.

For the matroid $U_{4,6}$ we use bounds on ideal schemes for threshold access structures of Theorem 3.1 that follow from the Bush bound.

Theorem B.2. *The matroid $U_{4,6}$ is not 4-entropic.*

Proof. A 4-entropic representation of $U_{4,6}$ is equivalent to a 4-ideal scheme for a 4-out-of-5 access structure. By Theorem 3.1, an ideal scheme for this access structure needs a domain size greater than or equal to 5, so it cannot exist. □

Note that Remark 2.35 gives an alternative proof for the nonexistence of an ideal secret sharing scheme for the $(4,5)$-threshold access structure, or in terms of matroid theory, the fact that the matroid $U_{4,6}$ is not entropic.

B.2 Matroid P_6

Remark B.3. Notice that working with higher order latin cubes, there are more than 3 possible cubes that satisfy that the latin squares are mutually orthogonal, but the cubes are not orthogonal. Then, there is a possible entropic representation of the matroid P_6 in fields of higher order.

For example, when considering order 5, there are sets of three cubes that are not orthogonal, but the latin squares defined by fixing some coordinate are mutually orthogonal. More concretely, an example of three latin cubes of order 5 that have orthogonal latin squares but are not orthogonal are:

$$H_4 = \left(\begin{array}{ccccc|ccccc|ccccc|ccccc|ccccc}
0&1&2&3&4&3&4&0&1&2&1&2&3&4&0&4&0&1&2&3&2&3&4&0&1\\
3&4&0&1&2&1&2&3&4&0&4&0&1&2&3&2&3&4&0&1&0&1&2&3&4\\
1&2&3&4&0&4&0&1&2&3&2&3&4&0&1&0&1&2&3&4&3&4&0&1&2\\
4&0&1&2&3&2&3&4&0&1&0&1&2&3&4&3&4&0&1&2&1&2&3&4&0\\
2&3&4&0&1&0&1&2&3&4&3&4&0&1&2&1&2&3&4&0&4&0&1&2&3
\end{array}\right)$$

$$H_5 = \left(\begin{array}{ccccc|ccccc|ccccc|ccccc|ccccc}
0&4&3&2&1&1&0&4&3&2&2&1&0&4&3&3&2&1&0&4&4&3&2&1&0\\
3&2&1&0&4&4&3&2&1&0&0&4&3&2&1&1&0&4&3&2&2&1&0&4&3\\
1&0&4&3&2&2&1&0&4&3&3&2&1&0&4&4&3&2&1&0&0&4&3&2&1\\
4&3&2&1&0&0&4&3&2&1&1&0&4&3&2&2&1&0&4&3&3&2&1&0&4\\
2&1&0&4&3&3&2&1&0&4&4&3&2&1&0&0&4&3&2&1&1&0&4&3&2
\end{array}\right)$$

$$H_6 = \left(\begin{array}{ccccc|ccccc|ccccc|ccccc|ccccc}
0&3&1&4&2&1&4&2&0&3&2&0&3&1&4&3&1&4&2&0&4&2&0&3&1\\
2&0&3&1&4&3&1&4&2&0&4&2&0&3&1&0&3&1&4&2&1&4&2&0&3\\
4&2&0&3&1&0&3&1&4&2&1&4&2&0&3&2&0&3&1&4&3&1&4&2&0\\
1&4&2&0&3&2&0&3&1&4&3&1&4&2&0&4&2&0&3&1&0&3&1&4&2\\
3&1&4&2&0&4&2&0&3&1&0&3&1&4&2&1&4&2&0&3&2&0&3&1&4
\end{array}\right)$$

Then, if X_1, X_2, X_3 are independent random variables uniformly distributed in $\mathbb{F}_5$ and X_4, X_5, X_6 are uniformly distributed in the elements of the latin cubes H_4, H_5, H_6, respectively, then the vector $(X_1, \ldots, X_6)$ defines an entropic representation of the matroid P_6 in $\mathbb{F}_5$. Indeed, this corresponds to the linear representation defined by the matrix

$$\begin{pmatrix}
1&0&0&3&3&1\\
0&1&0&1&3&4\\
0&0&1&1&2&3
\end{pmatrix}$$

B.3 Non-Fano and Non-Fano Dual Matroids

The non-Fano matroid F_7^- and its dual $\left(F_7^-\right)^*$ admit a linear representation only over fields with off characteristic. They can be represented by the graphs shown in Fig. 8.

Matúš showed that F_7^- is only representable by partitions over domains of odd order [Mat99, Proposition 4.1], i.e. only k-entropic for odd k.

In Theorem B.4 and Theorem B.6, we show an alternative proof that F_7^- and $(F_7^-)^*$ are not 4-entropic that uses the techniques of latin squares and orthogonality, independent of the work of Matúš.

Theorem B.4. *The matroid F_7^- is not 4-entropic.*

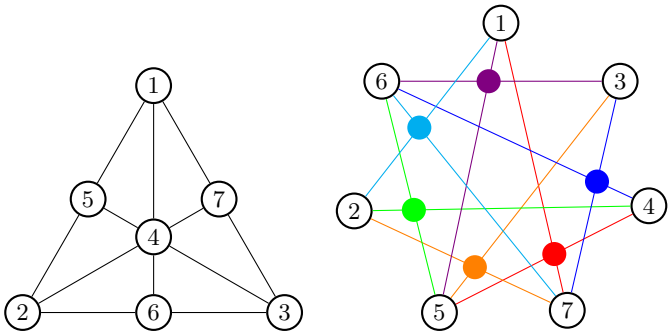


Fig. 8: non-Fano Matroid and Dual of non-Fano

Proof. Consider the circuits $\{1,2,3,4\}$, $\{1,2,3,5\}$, $\{1,2,3,6\}$, and $\{1,2,3,7\}$, and their associated latin cubes of dimension 3 and order 4, H_4, H_5, H_6, H_7.

For every latin cube, we can take the projection to one of its 2-dimensional arrays, which is equivalent to taking the contraction of H^i at some point j for some value $a \in \{0,1,2,3\}$. We denote $H^i_{j:a}$ as the latin square corresponding to this contraction.

We now observe that for every $a \in \{0,1,2,3\}$ each latin square $H^i_{j:a}$ is isotopic to V_4.

Let $i_1, i_2 \in \{4,5,6,7\}$. If $\{1, i_1, i_2\}$ is a base, each row of $\mathsf{M}_{\{1,i_1,i_2\}}$ occurs once. Then, the projections of the cubes H^{i_1} and H^{i_2} to each value a of the column 1 are orthogonal latin squares.

From the relations $\{1,5,6\}, \{1,6,7\}, \{1,4,5\}, \{1,4,7\}$ we deduce that

$$H^5_{1:a} \perp H^6_{1:a}, \quad H^6_{1:a} \perp H^7_{1:a}, \quad H^4_{1:a} \perp H^5_{1:a}, \quad H^4_{1:a} \perp H^7_{1:a}$$

Note that for every $i_1 \in \{4,5,6,7\}$ and $j \in \{1,2,3\}$ there is a $i_2 \in \{4,5,6,7\}$ such that $\{j, i_1, i_2\}$ is a base. Then, for every $a \in \{0,1,2,3\}$, $H^{i_1}_{j:a}$ has an orthogonal mate and is therefore isotopic to the Cayley table of V_4.

By Lemma 2.23, for every $i \in \{4,5,6,7\}$ and every $j \in \{1,2,3\}$, there exist permutations $\sigma_{i,j,a}$ and τ such that

$$H^i_{j:a}(r,s) = \tau(\sigma_{i,j,a}(r) \cdot s)$$

We will hereafter consider a fixed value and denote $\sigma_{i,j} := \sigma_{i,j,a}$.

Next, we deduce some relations of the latin squares from the circuits of the matroid.

Claim 7. If $i_1, i_2 \in \{4,5,6,7\}$, $j \in \{1,2,3\}$ are such that $C = \{j, i_1, i_2\}$ is a circuit, $\sigma_{i_1,j} = \sigma_{i_2,j}$.

Proof. Consider a circuit $C = \{j, i_1, i_2\}$ with $i_1, i_2 \in \{4,5,6,7\}$ and $j \in \{1,2,3\}$. Each row of M_C occurs 4 times. Consider a value of $a \in \{0,1,2,3\}$, for every position of $H^{i_1}_{j:a}$ such that it takes a fixed value, the square $H^{i_2}_{j:a}$ will take the same value. This means that $H^{i_1}_{j:a}$ and $H^{i_2}_{j:a}$ are symbol-isotopic and then $\sigma_{i_1,j} = \sigma_{i_2,j}$.

Then, the circuits $\{1,4,6\}$, $\{1,5,7\}$, $\{2,4,7\}$, $\{2,5,6\}$, $\{3,4,5\}$ and $\{3,6,7\}$ imply that

$$\begin{aligned} \sigma_{4,1} &= \sigma_{6,1}, \ \ \sigma_{5,1} = \sigma_{7,1} \\ \sigma_{4,2} &= \sigma_{7,2}, \ \ \sigma_{5,2} = \sigma_{6,2} \\ \sigma_{4,3} &= \sigma_{5,3}, \ \ \sigma_{6,3} = \sigma_{7,3} \end{aligned} \tag{23}$$

Recall from Lemma 5.8 the relation of the permutations of the three projections of a latin cube $\sigma_{i,1}, \sigma_{i,2}$ and $\sigma_{i,3}$:

$$\sigma_{i,2} = \sigma_{i,1} \circ \sigma_{i,3}$$

Since $\sigma_{4,2} = \sigma_{7,2}$ and $\sigma_{5,2} = \sigma_{6,2}$, we have

$$\sigma_{4,1} \circ \sigma_{4,3} = \sigma_{7,1} \circ \sigma_{7,3} \tag{24}$$

$$\sigma_{5,1} \circ \sigma_{5,3} = \sigma_{6,1} \circ \sigma_{6,3} \tag{25}$$

Applying (23) to (24) we get

$$\sigma_{6,1} \circ \sigma_{5,3} = \sigma_{5,1} \circ \sigma_{6,3}$$

Hence,

$$\sigma_{6,1} = \sigma_{5,1} \circ \sigma_{6,3} \circ \sigma_{5,3}^{-1}$$

and applying this to (25) we get

$$\begin{aligned} \sigma_{5,1} \circ \sigma_{5,3} &= \sigma_{5,1} \circ \sigma_{6,3} \circ \sigma_{5,3}^{-1} \circ \sigma_{6,3} \\ \sigma_{5,3} &= \sigma_{6,3} \circ \sigma_{5,3}^{-1} \circ \sigma_{6,3} \\ \sigma_{6,3}^{-1} \circ \sigma_{5,3} &= \sigma_{5,3}^{-1} \circ \sigma_{6,3} = (\sigma_{6,3}^{-1} \circ \sigma_{5,3})^{-1} \end{aligned}$$

Note that this implies that if $\pi = \sigma_{6,3}^{-1} \circ \sigma_{5,3}$, then $\pi^{-1} = \pi$. Since π is a 3-element permutation, this implies that π has a fixed point, i.e. there is a $b \in \{1,2,3\}$ such that $\pi(b) = b$. Therefore,

$$\sigma_{6,3}^{-1} \circ \sigma_{5,3}(b) = b \implies \sigma_{5,3}(b) = \sigma_{6,3}(b)$$

Observe that this contradicts the independence of the set $\{3,5,6\}$ since the latin squares $H_{3:a}^5$ and $H_{3:a}^6$ are orthogonal, and then $\sigma_{5,3} \perp \sigma_{6,3}$. By Lemma 5.5, the permutations $\sigma_{5,3}$ and $\sigma_{6,3}$ must not have fixed points. □

Remark B.5. This argument doesn't work over a domain of 3 elements because there are permutations of 2 elements π satisfying $\pi^{-1} = \pi$ but not having any fixed point.

The dual of non-Fano matroid, $\left(F_7^-\right)^*$ is the matroid that has as circuits the complements of the hyperplanes of F_7^-, i.e. maximal sets of F_7^- with rank 2. So circuits of $\left(F_7^-\right)^*$ are the colored sets in Fig. 8 and all four elements are independent sets.

Theorem B.6. *The matroid* $\left(F_7^-\right)^*$ *is not* 4*-entropic.*

Proof. Consider a 4-entropic representation of $\left(F_7^-\right)^*$ with table M satisfying the property of Theorem 2.7.

Sets $\{1,2,3,4,i\}$ with $i=5,6,7$ are circuits of rank 4, and by Lemma 2.36 the restriction to the columns $\{1,2,3,i\}$ is an hypercube of dimension 4, which we denote H^i, for every $i=5,6,7$.

For every latin hypercube H^i, $i\in\{5,6,7\}$ and every $j\in\{1,2,3,4\}$, we consider the latin cubes $H^i_{j:0}$,$H^i_{j:1}$,$H^i_{j:2}$,$H^i_{j:3}$ obtained when fixing the column j to the values $0,1,2,3$, respectively. Moreover, if $j_1,j_2\in\{1,2,3,4\}$ and $a,b\in\{0,1,2,3\}$, we denote $H^i_{j_1,j_2:a,b}$ the latin square obtained when fixing the two columns j_1,j_2 of the latin hypercube H^i to the values a and b, respectively.

First, note that if a set $\{1,2,i_1,i_2\}$ is independent for some $i_1,i_2\in\{5,6,7\}$, then the squares $H^{i_1}_{1,2:a,b}$ and $H^{i_2}_{1,2:a,b}$ are orthogonal for all values of $a,b\in\{0,1,2,3\}$. Indeed, we can show that, if they are not orthogonal, then there is a repeated pair in the superimposition and this would imply a repeated row in the table $\mathsf{M}_{\{1,2,i_1,i_2\}}$.

Observe that for every $j_1,j_2\in\{1,2,3,4\}$ and every $i\in\{5,6,7\}$ there is a $\ell\in\{5,6,7\}$ such that the set $\{j_1,j_2,i,\ell\}$ is independent. So, all projections $H^i_{j_1,j_2:a,b}$ are squares orthogonal to some other latin square, so by Lemma 5.3 they must be isotopic to the multiplication table of the group V_4, L_V, and can be characterized by the formula of Lemma 2.23.

Since we observed that all latin squares $H^i_{j_1,j_2:a,b}$ are isotopic to L_V, by Lemma 5.7, for every $i\in\{5,6,7\}$, $j_1,j_2\in\{1,2,3,4\}$, and $a,b\in\{0,1,2,3\}$ there exists a permutation $\sigma_{i;j_1,j_2:a,b}$ satisfying for some τ

$$H^i_{j_1,j_2:a,b}(r,s)=\tau(\sigma_{i;j_1,j_2:a,b}(r)\cdot s).$$

For ease of notation, we fix $a=b=0$ for the remainder of the proof and denote $\sigma_{i;j_1j_2}:=\sigma_{i;j_1,j_2:0,0}$.

By applying Lemma 5.8 to the latin cubes $H_{i,1}$,$H_{i,2}$,$H_{i,3}$,$H_{i,4}$ for $i\in\{5,6,7\}$, we deduce the relations:

$$\begin{aligned}\sigma_{i;12}\circ\sigma_{i;14}&=\sigma_{i;13},\\ \sigma_{i;12}\circ\sigma_{i;24}&=\sigma_{i;23},\\ \sigma_{i;13}\circ\sigma_{i;34}&=\sigma_{i;23},\\ \sigma_{i;14}\circ\sigma_{i,34}&=\sigma_{i;24}\end{aligned}\tag{26}$$

Now we study the dependency relations determined by the matroid and deduce the implications on the σ's.

Let $i_1,i_2\in\{5,6,7\}$ and $j_1,j_2\in\{1,2,3,4\}$. If a set $\{i_1,i_2,j_1,j_2\}$ is a circuit, then the latin squares $H^{i_1}_{j_1,j_2}$ and $H^{i_2}_{j_1,j_2}$ are dependent, i.e., all the positions where $H^{i_1}_{j_1,j_2}$ takes a fixed value, and the square $H^{i_2}_{j_1,j_2}$ takes the same value. This is, that $H^{i_1}_{j_1,j_2}$ and $H^{i_2}_{j_1,j_2}$ are symbol-isotopic. Therefore, the circuits $\{1,3,5,6\}$, $\{2,4,5,6\}$, $\{2,3,5,7\}$, $\{1,4,5,7\}$, $\{1,2,6,7\}$, $\{3,4,6,7\}$ imply the following relations:

$$\begin{aligned}&\sigma_{5;13}=\sigma_{6;13},\ \sigma_{5;14}=\sigma_{7;14},\ \sigma_{6;34}=\sigma_{7;34}\\ &\sigma_{5;24}=\sigma_{6;24},\ \sigma_{5;23}=\sigma_{7;23},\ \sigma_{6;12}=\sigma_{7;12}\end{aligned}\tag{27}$$

The independence relations

$$\{1,2,5,6\},\{1,2,5,7\},\{2,3,6,7\}$$
$$\{2,3,5,6\},\{1,3,5,7\},\{1,4,6,7\}$$
$$\{1,4,5,6\},\{2,4,5,7\},\{2,4,6,7\}$$
$$\{3,4,5,6\},\{3,4,5,7\},\{1,3,6,7\}$$

imply the following relations of orthogonality:

$$\sigma_{5;12} \perp \sigma_{6;12},\ \sigma_{5;12} \perp \sigma_{7;12},\ \sigma_{6;23} \perp \sigma_{7;23}$$
$$\sigma_{5;23} \perp \sigma_{6;23},\ \sigma_{5;13} \perp \sigma_{7;13},\ \sigma_{6;14} \perp \sigma_{7;14}$$
$$\sigma_{5;14} \perp \sigma_{6;14},\ \sigma_{5;24} \perp \sigma_{7;24},\ \sigma_{6;24} \perp \sigma_{7;24}$$
$$\sigma_{5;34} \perp \sigma_{6;34},\ \sigma_{5;34} \perp \sigma_{7;34},\ \sigma_{6;13} \perp \sigma_{7;13}$$

If we call $\sigma_{\cdot,\cdot} = \sigma_{5;\cdot,\cdot}$, and $\sigma'_{\cdot,\cdot}$ an orthogonal permutation of $\sigma_{\cdot,\cdot}$, then all these relations can be organized as follows:

Using the relations in (26) applied at equalities of (27), we have

$$\sigma_{5;13} = \sigma_{6;13} \implies \sigma_{5;12} \circ \sigma_{5;14} = \sigma_{6;12} \circ \sigma_{6;14} \tag{28}$$

$$\begin{aligned} \sigma_{5;23} = \sigma_{7;23} \implies \sigma_{5;12} \circ \sigma_{5;24} &= \sigma_{7;12} \circ \sigma_{7;12} \\ \sigma_{5;12} \circ \sigma_{5;14} \circ \sigma_{5;34} &= \sigma_{7;12} \circ \sigma_{7;14} \circ \sigma_{7,34} \end{aligned} \tag{29}$$

$$\sigma_{5;24} = \sigma_{6;24} \implies \sigma_{5;14} \circ \sigma_{5;34} = \sigma_{6;14} \circ \sigma_{6;34} \tag{30}$$

From (28) and (29) we deduce that

$$\sigma_{6;12} \circ \sigma_{6;14} \circ \sigma_{5;34} = \sigma_{7;12} \circ \sigma_{7;14} \circ \sigma_{7,34}$$

then using $\sigma_{6;12} = \sigma_{7;12}$ we get

$$\sigma_{6;14} \circ \sigma_{5;34} = \sigma_{7;14} \circ \sigma_{7,34}$$
$$\sigma_{7;14}^{-1} \circ \sigma_{6;14} = \sigma_{7;34} \circ \sigma_{5;34}^{-1}$$

By (30),

$$\sigma_{5;34} \circ \sigma_{6;34}^{-1} = \sigma_{5;14}^{-1} \circ \sigma_{6;14}$$

And applying $\sigma_{5;14} = \sigma_{7;14}$ and $\sigma_{6;34} = \sigma_{7;34}$ we get

$$\sigma_{5;34} \circ \sigma_{7;34}^{-1} = \sigma_{7;14}^{-1} \circ \sigma_{6;14}$$

Hence,

$$\sigma_{5;34} \circ \sigma_{7;34}^{-1} = \sigma_{7;34} \circ \sigma_{5;34}^{-1} = (\sigma_{5;34} \circ \sigma_{7;34}^{-1})^{-1}$$

So $\sigma_{5;34} \circ \sigma_{7;34}^{-1}$ has order 2. Since every order 2 permutation of 3 elements has a fixed point, there is some $b \in \{1,2,3\}$ such that

$$\sigma_{5;34} \circ \sigma_{7;34}^{-1}(b) = b \implies \sigma_{5;34}(c) = \sigma_{7;34}(c)$$

for some $c \in \{1,2,3\}$. This contradicts the fact that the set $\{3,4,5,7\}$ is independent. □

B.4 P_8 and P_8'' are not Multilinear

Using techniques of pivoting matrices in $\mathcal{M}_{2\times 2}(\mathbb{F}_2)$ of [BBFP20], it can be seen that there are no 2×2 matrices A, B, C, D, E that deduce a 2-linear representation of the matroid P_8:

$$\begin{array}{cccccccc} 2 & 4 & 6 & 8 & 3 & 1 & 5 & 7 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & D \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & A & 1 & 0 & E \\ 0 & 0 & 0 & 1 & B & 1 & C & 0 \end{array}$$

Again, pivoting techniques on the matrices A, B, C, D, E, lead to deduce the impossibility of a 2-linear representation of the matroid P_8''.

C Forbidden Minors For Access Structures

In this section, we provide an alternative characterization of 4-ideal and 6-ideal access structures by determining the forbidden minors of the access structures.

These results take advantage of the characterization of matroid ports by Seymour [Sey76b]. He provided a characterization in terms of the forbidden minors of the access structure. That is, he presented a (small) list of access structures and proved that an access structure Γ is a matroid port if and only if none of the minors of Γ are in the list.

The access structures in the list are P_4, Q_4, $b(Q_4)$ and J_k for $k \geq 3$. These access structures can be easily represented by graphs and hypergraphs as shown in Fig. 9: The nodes are the participants and the minimal authorized subsets are the graph edges and the colored hyperedges. For example, the minimal authorized subsets of P_4 are $\{1, 2\}$, $\{2, 3\}$, and $\{3, 4\}$. For every $k \geq 2$, we define J_k as the access structures with minimal authorized subsets $\{\{1, \ldots, k\}\} \cup \{\{0, i\} : i = 1, \ldots, k\}$.

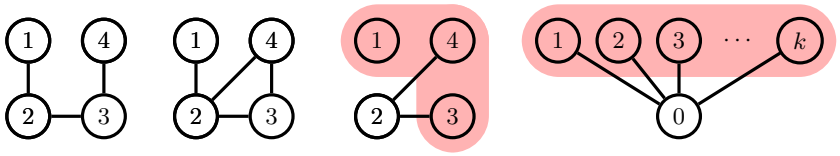


Fig. 9: Representation of the access structures P_4, Q_4, $b(Q_4)$, and J_k for $k \geq 2$.

Theorem C.1 ([Sey76b]). *An access structure is a matroid port if and only if none of its minors are P_4, Q_4, $b(Q_4)$ nor J_k for any $k \geq 3$.*

Thirty years later, Martí-Farré and Padró [MP07] revisited [Sey76b]. From the optimal information ratio of these access structures, they discovered properties of the information ratio of matroid ports.

In [Sey76a] and [Sey76b], Seymour provided a characterization of access structures that admit 2-ideal linear secret sharing schemes, advancing the work by Lehman [Leh64]. Taking into account that 2-ideal access structures admit 2-ideal linear schemes [BC94], [Sey76b, Corollary] provides the following characterization of 2-ideal access structures.

Theorem C.2. *An access structure admits a 2-ideal scheme if and only if it contains neither P_4 nor J_k (for any $k \geq 2$) as a minor.*

In the rest of the section, we provide an alternative characterization of k-ideal access structures for $k = 3, 4, 6$. We provide these results in Theorem C.4, Theorem C.12, and Theorem C.5, respectively.

C.1 3-Ideal and 6-Ideal Access Structures

We denote the (t, n)-threshold access structure as $\Gamma_{t,n}$, which is the matroid port of the uniform matroid $U_{t,n+1}$ to some of its points. This is well defined since uniform matroids are symmetric. We define Γ_{F_7} as the Fano matroid port to some of its points and $\Gamma^*_{F_7}$ as its dual.

Observation C.3. *Following the labels of Fig. 10, The Fano access structure Γ_{F_7} can be described as the set of participants $P = \{a_0, a_1, b_0, b_1, c_0, c_1\}$ where the minimal authorized sets are*

$$\min \Gamma_{F_7} = \{\{a_0, a_1\}, \{b_0, b_1\}, \{c_0, c_1\}\} \cup \{\{a_i, b_j, c_k\} : i + j + k \equiv 0 \pmod 2\}$$

The Fano Dual access structure $\Gamma^*_{F_7}$ can be described as the set of participants $P = \{a_0, a_1, b_0, b_1, c_0, c_1\}$ with minimal authorized sets

$$\min \Gamma_{F_7^*} = \{\{a_i, b_j, c_k\} : i + j + k \equiv 0 \pmod 2\}.$$

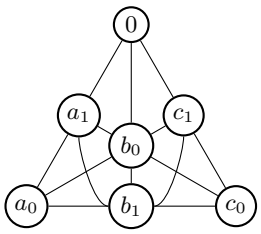


Fig. 10: The matroid F_7, with the labels used to determine its matroid port.

Then, the characterization of 3-ideal access structures is:

Theorem C.4. *An access structure is* 3*-ideal if and only if none of its minors are* P_4*,* Q_4*,* $b(Q_4)$*,* $\Gamma_{2,4}$*,* $\Gamma_{3,4}$*,* Γ_{F_7}*,* $\Gamma^*_{F_7}$*, nor* J_k *for any* $k \geq 3$*.*

And, using our result Theorem 1.2 we can deduce the following characterization of 6-ideal access structures:

Theorem C.5. *An access structure admits a* 6*-ideal scheme if and only if none of its minors are* P_4*,* J_k *for* $k \geq 2$*,* $\Gamma_{3,4}$*,* Γ_{F_7}*, nor* $\Gamma^*_{F_7}$*.*

Proof. Γ is a port of a matroid if and only if it does not contain P_4, Q_4, $b(Q_4)$ or J_k, $k \geq 3$. The structures Q_4 and $b(Q_4)$ contain J_2 as minor, so if Γ does not contain the minor J_2, then neither Q_4 nor $b(Q_4)$. So, it is a port of a matroid. Moreover, since it does not contain J_2 as minor, the matroid does not contain the uniform $U_{2,4}$ as a minor and then Γ admits a 2-ideal scheme. Similarly, since it does not contain the minor J_2, the minor $\Gamma_{2,4}$ is not in Γ and by the characterization of 3-ideal schemes, Γ admits a 3-ideal scheme. Therefore, it admits a 6-ideal scheme.

Conversely, if Γ admits a 6-ideal scheme, in particular it is a matroid port and so it does not contain the minors P_4 nor J_k $k \geq 3$. By Theorem 1.2, the matroid does not contain minors $U_{2,4}$, $U_{3,4}$, F_7 nor F_7^* as any of its ports, therefore Γ does not have minors J_2, $\Gamma_{3,4}$, Γ_{F_7} or $\Gamma^*_{F_7}$. □

C.2 4-Ideal Access Structures

Next, we show a characterization of 4-ideal access structures by their forbidden minors. For that, we need a description of the ports of all the involved matroids.

Lemma C.6. *The matroid ports of* P_6 *are the access structures on* 5 *points* $\Gamma^1_{P_6}$ *and* $\Gamma^2_{P_6}$ *with*

$$\Gamma^1_{P_6} = \{A \subseteq \{1,2,3,4,5\} : |A| \geq 3, A \neq \{3,4,5\}\} = \Gamma_{3,5} \setminus \{3,4,5\}.$$

$$\Gamma^2_{P_6} = \{A \subseteq \{1,2,3,4,5\} : |A| \geq 3\} \cup \{\{4,5\}\}.$$

Proof. The matroid P_6 has every 3-element set of rank 3 except for one set that has rank 2 (see Fig. 11).

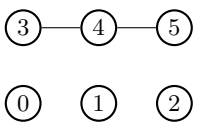


Fig. 11: The matroid P_6.

First, the ports of P_6 at the points $0, 1, 2$ are the same since the matroids are equivalent when relabeling the points $0, 1, 2$. We denote the port of P_6 at the

point 0 by $\Gamma^1_{P_6}$. Elements of $\Gamma^1_{P_6}$ are those subsets A of $\{1,2,3,4,5\}$ that $r(A) = r(A \cup \{0\})$. Note that since every 3-element set has rank 3 except for the set $\{3,4,5\}$, the unique 3-element set not containing 0 that does not satisfy $r(A) = r(A \cup \{0\})$ is $\{3,4,5\}$. So,

$$\Gamma^1_{P_6} = \Gamma_{3,5} \setminus \{3,4,5\}.$$

Second, the ports of P_6 at the points $3,4,5$ are the same since the matroids are equivalent when relabeling the points $3,4,5$. We denote $\Gamma^2_{P_6}$ to the port of P_6 at point 5. All 2-element sets A of $\{0,1,2,3,4\}$ satisfy that

$$r(A) = 2 \quad \text{and} \quad r(A \cup \{5\}) = 3$$

except for $A = \{3,4\}$. So $\{3,4\} \in \Gamma^2_{P_6}$. Every 3-element set A not containing 5 satisfies that

$$r(A) = 3 = r(A \cup \{5\})$$

therefore, $\Gamma^2_{P_6} = \Gamma_{3,5} \cup \{\{3,4\}\}$. □

Lemma C.7. *The matroid ports of F_7^- are the access structures $\Gamma^1_{F_7^-}$ and $\Gamma^2_{F_7^-}$ on the set $\{a_0,a_1,b_0,b_1,c_0,c_1\}$ with*

$$\Gamma^1_{F_7^-} = \Gamma_{F_7} \cup \{\{a_1,b_1,c_1\}\}, \qquad \Gamma^2_{F_7^-} = \Gamma_{F_7} \setminus \{b_0,b_1\},$$

$$(\Gamma^1_{F_7^-})^* = \Gamma^*_{F_7} \setminus \{a_0,b_0,c_0\}, \qquad (\Gamma^2_{F_7^-})^* = \Gamma^*_{F_7} \cup \{\{a_0,a_1,c_0,c_1\}\}.$$

Proof. The matroid F_7^- has points contained in 3 circuits and points contained only in 2 circuits. These two types of points define two non-equivalent matroid ports

First, we consider one of the vertices of the triangle. We denote the port of F_7^- by this point by $\Gamma^1_{F_7^-}$. Then we label the other points as in Fig. 12 left and observe that all authorized sets are as in Γ_{F_7},

$$\Gamma_{F_7} = \{\{a_0,a_1\},\{b_0,b_1\},\{c_0,c_1\}\} \cup \{\{a_i,b_j,c_k\} : i+j+k \equiv 0 \pmod 2\}$$

and the set $\{a_1,b_1,c_1\}$, which is unauthorized in the Fano configuration. So,

$$\Gamma^1_{F_7^-} = \Gamma_{F_7} \cup \{\{a_1,b_1,c_1\}\}.$$

Note that if we consider the port by the point in the center, we obtain the same access structure $\Gamma^1_{F_7^-}$.

Now, consider one of the points that is contained only in 2 circuits and denote the port of the matroid by this point by $\Gamma^2_{F_7^-}$. We label the other points as in Fig. 12 right. The authorized sets are again all the sets in Γ_{F_7} except for the set $\{b_0,b_1\}$ that is unauthorized. Therefore,

$$\Gamma^2_{F_7^-} = \Gamma_{F_7} \setminus \{b_0,b_1\}.$$

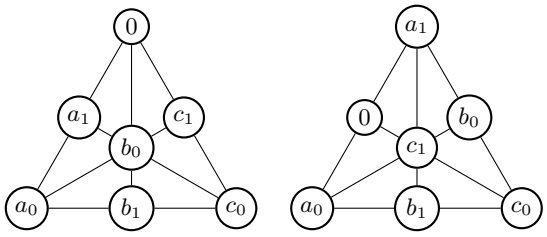


Fig. 12: Matroid F_7^- represented with two different labellings. Ports at zero provide the two possible ports of F_7^-.

The other ports of F_7^- over the other two points contained in only 2 circuits are the same as $\Gamma^2_{F_7^-}$.

For the duals, we use the definition

$$\Gamma^* = \{E \setminus B : B \notin \Gamma\}.$$

Since $\Gamma^1_{F_7^-} = \Gamma_{F_7} \cup \{\{a_1, b_1, c_1\}\}$ and $\Gamma^2_{F_7^-} = \Gamma_{F_7} \setminus \{b_0, b_1\}$, we have that

$$(\Gamma^1_{F_7^-})^c = (\Gamma_{F_7})^c \setminus \{a_1, b_1, c_1\}, \quad (\Gamma^2_{F_7^-})^c = (\Gamma_{F_7})^c \cup \{\{b_0, b_1\}\}.$$

Hence,

$$\begin{aligned}(\Gamma^1_{F_7^-})^* =& \{E \setminus B : B \in (\Gamma_{F_7})^c \setminus \{a_1, b_1, c_1\}\} = \Gamma^*_{F_7} \setminus \{a_0, b_0, c_0\}, \text{ and}\\ (\Gamma^2_{F_7^-})^* =& \{E \setminus B : B \in (\Gamma_{F_7})^c \cup \{\{b_0, b_1\}\}\} = \Gamma^*_{F_7} \cup \{\{a_0, a_1, c_0, c_1\}\}.\end{aligned}$$

□

Lemma C.8. *The matroid port of P_8 over any of its points is the access structure Γ_{P_8} on the set $E = \{1, 2, 3, 4, 5, 6, 7\}$ defiend as follows,*

$$\begin{aligned}\Gamma_{P_8} =& \{\{5, 6, 7\}, \{1, 2, 6\}, \{3, 4, 6\}, \{2, 4, 5\}, \{1, 3, 7\}\}\\ &\cup \{B \subseteq E : B \textit{ base of } P_8\} \cup \Gamma_{5,7}.\end{aligned}$$

Proof. First, observe that all the ports of the matroid P_8 are the same, since it is symmetric. There are no rank-2 dependent sets in P_8 and $r(P_8) = 4$, so sets $A \subseteq E$ such that $r(A) = r(A \cup \{8\})$ have rank at least 3.

Rank-3 authorized sets are obtained by the circuits of P_8 containing 8. If P_8 is labeled as in Fig. 13, the rank-3 authorized sets are:

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

Rank-4 authorized sets are $A \subseteq E$ with $r(A) = 4$, and they are all. If A has 4-elements, then it is independent. Note that since there are no circuits of size 3, a 4-element set is a circuit or a base. There are 35 4-element sets in E, 5 of

them are circuits and the other 30 are bases. So, A is one of the following 30 sets:

$$\{B \subseteq E : B \text{ base of } P_8\}.$$

The other rank-4 sets are sets with more than 4 elements, i.e., $\Gamma_{5,7}$. □

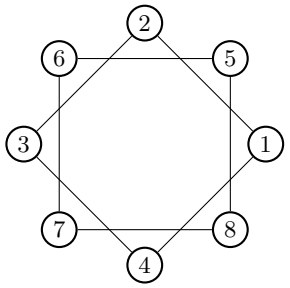


Fig. 13: P_8 matroid

Observation C.9. *A list of minimal authorized sets of Γ_{P_8} is given by the following 3-element sets:*

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

and 10 of the 30 bases not containing 8 (that are those that do not contain any of the five sets above). Namely, they are:

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

Lemma C.10. *The matroid port of P_8'' over any of its points is the access structure $\Gamma_{P_8''}$ on the set $E = \{1,2,3,4,5,6,7\}$:*

$$\Gamma_{P_8''} = \{\{1,2,6\},\{3,4,6\},\{2,4,5\},\{1,3,7\}\} \cup \{B \subseteq E : B \text{ base of } P_8''\} \cup \Gamma_{5,7}.$$

Proof. The matroid P_8'' differs from P_8 by the two disjoint circuits, $\{1,2,3,4\}$ and $\{5,6,7,8\}$. So the 3-element authorized sets are

$$\{1,2,6\},\{3,4,6\},\{2,4,5\},\{1,3,7\}$$

and the 4-element authorized sets are again the bases of P_8'' not containing 8:

$$\{B \subseteq E : B \text{ base of } P_8''\}.$$

Observe that they are 31, the same 30 as in Γ_{P_8} plus the base $\{1,2,3,4\}$. Again, since we are listing the authorized sets and not only the minimal ones, all sets at least 5 elements are authorized, i.e., $\Gamma_{5,7}$. □

Observation C.11. *The list of minimal authorized sets of* $\Gamma_{P_8''}$ *is given by the following* 3*-element sets:*

$$\{1,2,6\},\{3,4,6\},\{2,4,5\},\{1,3,7\}$$

and 15 *of the* 31 *bases not containing* 8 *(that are the ones that do not contain any of the four sets above). Namelu, they are:*

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

Theorem C.12. *An access structure admits a* 4*-ideal scheme if and only if its minors are different from* P_4, Q_4, $b(Q_4)$, $\Gamma_{2,5}$, $\Gamma_{4,5}$, $\Gamma^1_{P_6}$, $\Gamma^2_{P_6}$, $\Gamma^1_{F_7^-}$, $\Gamma^2_{F_7^-}$, $\Gamma^{*1}_{F_7^-}$, $\Gamma^{*2}_{F_7^-}$, Γ_{P_8}, $\Gamma_{P_8''}$, *and* J_k *for* $k \geq 3$.

Proof. This follows by Theorem 1.1 and Theorem C.1. □