

Entropic matroids and their representation

Emmanuel Abbe
EPFL, Department of Mathematics, Lausanne 1015, CH

and

Sophie Spirkl
Princeton University, Princeton, NJ 08540, USA

September 27, 2019

Abstract

This paper investigates *entropic matroids*, that is, matroids whose rank function is given as the Shannon entropy of random variables. In particular, we consider *p-entropic matroids*, for which the random variables each have support of cardinality p . We draw connections between such entropic matroids and secret-sharing matroids and show that entropic matroids are linear matroids when $p = 2, 3$ but not when $p = 9$. Our results leave open the possibility for p -entropic matroids to be linear whenever p is prime, with particular cases proved here. Applications of entropic matroids to coding theory and cryptography are also discussed.

1 Introduction

Matroid theory generalizes the notion of independence and rank beyond vector spaces. In a graphical matroid, for example, the rank of a subset of edges is the size of an acyclic spanning set of edges; analogous to the rank of a subset of vectors, which is the size of a spanning set of linearly independent vectors. It is natural to ask whether such combinatorial structures can also be obtained from probabilistic notions of independence, based on random variables. In particular, the entropy can be used to measure dependencies between random variables and it can be used to define a matroid rank function as discussed below. One can then investigate how such entropic matroids relate to other matroids, in particular whether they admit linear representations as graphical matroids do. Before giving formal definitions of such entropic matroids, we give some general definitions for matroids.

1.1 Definitions

We recall a few standard definitions related to matroids, see, for example, Oxley [1]. A *matroid* is a pair $M = (E, r)$, where the ground set E is a finite set (typically $E = [m]$, $m \in \mathbb{Z}_+$) and where the rank function $r : 2^E \rightarrow \mathbb{Z}_+$ satisfies

1. For any $A \subseteq E$, $r(A) \leq |A|$ (*normalization*);
2. For any $A \subseteq B \subseteq E$, $r(A) \leq r(B)$ (*monotonicity*);
3. For any $A, B \subseteq E$, $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ (*submodularity*).

The submodularity property can be interpreted as a diminishing return property: for every $A \subseteq B$ and $x \in E$,

$$r(A \cup x) - r(A) \geq r(B \cup x) - r(B), \quad (1)$$

that is, the larger the set, the smaller the increase in rank when adding a new element. Independent sets in a matroid are the subsets $S \subseteq E$ such that $r(S) = |S|$ and maximal independent sets are called *bases*, whereas minimal dependent sets are called *circuits*.

A matroid $M = (E, r)$ is *linear* if there is a vector space V and a map $f : E \rightarrow V$ such that $r(S) = \text{rank}(f(S))$ for all $S \subseteq E$, where *rank* denotes the rank function of V , that is, $\text{rank}(f(S)) = \dim \text{span}(f(S))$. We say that a matroid is \mathbb{F} -*representable* if in addition, V can be chosen as a vector space over the field \mathbb{F} .

Given a matroid M , a *minor* of $M = (E, \mathcal{F})$ is a matroid that can be obtained from M by a finite sequence of the following two operations:

1. *Restriction*: Given $A \subseteq E$, we define the matroid $M|A = (A, \mathcal{F} \cap 2^A)$.
2. *Contraction*: Given an independent set $A \in \mathcal{F}$, we define the matroid $M/A = (E \setminus A, \{B \subseteq E \setminus A : B \cup A \in \mathcal{F}\})$.

We define the *dual* $M^* = (E, r^*)$ of a matroid $M = (E, r)$ is defined by letting $r^*(A) = r(E \setminus A) + |A| - r(E)$ for all $A \subseteq E$. A matroid property is a *dual property* if M has the property if and only if M^* does.

Theorem 1 (Woodall [2]). *Being an \mathbb{F} -representable matroid is a dual property, that is, M is \mathbb{F} -representable if and only if M^* is.*

1.2 Entropic Matroids

One may expect that matroids could also result from probabilistic structures. Perhaps the first possibility would be to define a matroid to be ‘probabilistic’ if its elements can be represented by random variables (with a joint distribution on some domain), such that a subset S is independent if the random variables indexed by S are mutually independent. This, however, does not necessarily give a matroid. For example, let X_1 and X_2 be independent random variables (for example, normally distributed) and let $X_3 = X_1 + X_2$. Let $A = \{3\}$, $B = \{1, 3\}$ and $x = \{2\}$. Then $r(A \cup x) - r(A) = 0$ since X_2 and X_3 are dependent but $r(B \cup x) - r(B) = 1$ since $B \cup x = \{1, 2, 3\}$ contains two independent random variables. So this violates the submodularity requirement.

On the other hand, it is well known that the entropy function satisfies the monotonicity and submodularity properties [3, 4]. Namely, for a probability measure μ on a discrete set \mathcal{X} , the *entropy of μ in base q* is defined by

$$H(\mu) = - \sum_{x \in \mathcal{X}} \mu(x) \log_q \mu(x). \quad (2)$$

For two random variables X and Y with values in \mathcal{X} and \mathcal{Y} respectively and with joint distribution μ , we define the *conditional entropy*

$$H(X|Y) = \sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \mu(x, y) \log \frac{\mu(x, y)}{\sum_{u \in \mathcal{X}} \mu(u, y)}. \quad (3)$$

In particular, we have the chain rule of entropy $H(X|Y) = H(X, Y) - H(Y)$. We also define the *Hamming distance* of two vectors x and y as $d(x, y) = |\{1 \leq i \leq n : x_i \neq y_i\}|$ and the *Hamming ball* of radius r around x as $B_r(x) = \{y : d(x, y) \leq r\}$.

Furthermore, for a probability measure μ of m random variables defined each on a domain \mathcal{X} , that is, for a probability distribution μ on \mathcal{X}^m , one can define the function

$$r(S) = H(\mu_S), \quad S \subseteq [m], \quad (4)$$

where μ_S is the *marginal* of μ on S , that is,

$$\mu_S(x[S]) = \sum_{x_i \in [q] : i \notin S} \mu(x), \quad x[S] = \{x_i : i \in S\}. \quad (5)$$

By choosing the base q for the entropy in (4) to be $|\mathcal{X}|$, we also get that $r(S) \leq |S|$, with equality for uniform measures. Therefore, the above r satisfies the three axioms

of a rank function, with the exception that r is not necessarily integral. In fact this defines a polymatroid (and r is also called a β -function [5]) and entropic polymatroids (i.e., polymatroids derived from such entropic β -functions) have been studied extensively in the literature; see References [6, 8, 9, 7] and references therein. Using the Shannon entropy to study matroid structures already emerged in the works [10, 11], where the family of pairs of sets (i, j) and K such that $K \subseteq [m]$, $i, j \in [m] \setminus K$ is called probabilistically representable if there exist random variables $\{X_k\}_{k \in [m]}$ such that X_i and X_j are conditionally independent given X_K , with the latter expressed in terms of the Shannon entropy as $r(i, K) + r(j, K) - r(i, j, K) - r(K) = 0$.

However, we can also investigate what happens if this function r is in fact integral. This is the object of study in this paper.

Definition 2. Let $q \in \mathbb{Z}_+$. A matroid $M = ([m], r)$ is q -entropic if there is a probability distribution μ on $[q]^m$ such that for any $S \subseteq [m]$,

$$r(S) = H(\mu_S), \quad (6)$$

where μ_S is the marginal of μ on S and H is the Shannon entropy in base q .

Note that the entropy does not depend on the support of the random variables but only on their joint distribution. For this reason, the restriction that μ is taking values in $[q]^m$ is in fact equivalent to requiring that each random variable has a support of cardinality at most q . When working with the m underlying random variables X_1, \dots, X_m distributed according to μ , we write $H(S) = H(X[S]) = H(X_i : i \in S) = H(\mu_S)$.

With the integrality constraint, the random variables representing a q -entropic matroid must be marginally either uniformly distributed or deterministic, each pair of random variables must be either independent or a deterministic function of each other, and so on. These represent therefore extremal dependencies. As discussed in Section 8, such distributions (with extremal dependencies) have recently emerged in the context of polarization theory and multi-user polar codes [12], which has motivated in part this paper. In Section 4, we also comment on the connection between secret sharing from cryptography.

It is well-known and easy to check that entropic matroids generalize linear matroids, see, for example, References [13, 7]. For completeness we recall the proof, making explicit the dependency on the field size.

Lemma 3. *Let \mathbb{F} be a finite field. If a matroid is \mathbb{F} -representable then it is $|\mathbb{F}|$ -entropic.*

Proof. Let M be an \mathbb{F} -representable matroid and A be a matrix in $\mathbb{F}^{|E| \times n}$ whose rows correspond to elements of E so that a subset of rows is linearly independent in \mathbb{F}^n if and only if the corresponding subset of E is independent in M . Let Y_1, \dots, Y_n be mutually independent and uniformly distributed random variables over \mathbb{F} and let $Y = (Y_1, \dots, Y_n)$. Then the vector of random variables $(X_1, \dots, X_{|E|}) = A \cdot Y$ satisfies that for any $B \subseteq E$, $H(\{X_i : i \in B\}) = \text{rank } \{A_i : i \in B\}$. Thus the entropy function on $X_1, \dots, X_{|E|}$ recovers the rank function of M and M is $|\mathbb{F}|$ -entropic. \square

Our main goal throughout the remainder of this paper is to investigate whether entropic matroids are always representable over fields. As discussed in next section, we will approach this question by checking whether the forbidden minors of representable matroids are entropic or not. This strategy is justified by the fact that for the Shannon entropy, entropic matroids are a minor-closed class, as we will show in Lemma 4.

1.3 Results

We prove that for every p , a matroid is p -entropic if and only if it is secret-sharing with a ground set of size p , which is equivalent to being the matroid of an almost affine code with alphabet size p . Furthermore, we prove that for every p , being p -entropic is closed under taking matroid minors.

We give alternative proofs that for $p = 2$ and $p = 3$, being p -entropic is equivalent to being \mathbb{F}_p -representable by examining known forbidden minor characterizations. We also

make some partial progress towards proving the same for other primes p . In the final section of the paper, we mention some applications of entropic matroids in coding.

2 Further Related Literature

Matroid representations and forbidden minors were studied in Reference [14] for $\text{GF}(3)$, Reference [16, 15] for $\text{GF}(4)$ and some results for general fields were obtained in References [17, 18, 19]. Linear representable matroids are also intimately related to linear solutions to network coding problems, in particular in Reference [20], in which a network-constrained matroid enumeration algorithm is developed, as well as Reference [21] that considers integer-valued polymatroids and representable polymatroids in References [22, 23]. Matroids minors and the connection to Zhang-Yeung inequality was discussed in Reference [24], which shows in particular that almost entropic matroids have infinitely many excluded minor. Matroids, secret sharing and linearity are also discussed in several papers as mentioned in part earlier. Reference [25] gave the first example of an access structure (i.e., the parties that can recover the secret from their share) induced by a matroid, namely the Vamos matroid, that is non-ideal (a measure of optimality of the secret shares lengths); Reference [26] presented the first non-trivial lower bounds on the size of the domain of the shares for secret-sharing schemes realizing an access structure induced by the Vamos matroid and this is later improved in Reference [27] using non-Shannon inequalities for the entropy function. As mentioned earlier, an important line of work is also dedicated to understanding the representation of entropic polymatroids for a fixed ground set cardinality [9], which is well-understood for cardinality 2 and 3 and more complicated for larger cardinality with the non-Shannon inequalities emerging.

3 Minors of Entropic Matroids

In this section, we prove the following:

Lemma 4. *Let M be an entropic matroid on random variables X_1, \dots, X_m with values in \mathbb{F}_p and with entropy H and joint distribution μ .*

- (i) *For any $A \subseteq \{X_1, \dots, X_m\}$, $M|A$ is entropic.*
- (ii) *For any $X_i \in \{X_1, \dots, X_m\}$ with $H(X_i) = 1$, $M/\{X_i\}$ is entropic.*
- (iii) *For any independent set A , M/A is entropic.*

Proof. For each of the claims, we construct random variables and a probability distribution whose entropy agrees with the rank function of the matroid in question.

To prove (i), we consider the variable set A with the marginal distribution given by μ . Then H is integral on any subset of A , since it is integral on any subset of $\{X_1, \dots, X_m\}$. This implies (i).

To prove (ii), we consider two cases. If for any $B \subseteq \{X_1, \dots, X_m\}$ with $X_i \notin B$ we have $H(X_i, B) = H(B) + 1$, then X_i is independent of all other variables. In particular, any set is independent in M if and only if its union with $\{X_i\}$ is. Therefore, $M/\{X_i\} = M| \{X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_m\}$ in this case and the result follows from (i).

Otherwise, we define a distribution on $\{X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_m\}$ by fixing any value x for X_i with $\mathbb{P}[X_i = x] > 0$ and considering the probability distribution obtained by conditioning on the event $\{X_i = x\}$. Now let $A \subseteq \{X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_m\}$. There are two cases. If there is no circuit C with $X_i \in C$ such that A contains $C \setminus \{X_i\}$ as a subset, then $H(A) + 1 = H(A, X_i) = H(A) + H(X_i|A)$, therefore $H(X_i|A) = 1$ and so X_i and A are independent. In this case, $H(A|X_i = x) = H(A)$, thus H agrees with the rank function of $M/\{X_i\}$.

If adding X_i to A creates a circuit, then $H(A, X_i) = H(A)$ and $H(A|X_i) = H(A) - 1$. Let $X(A)$ denote the vector with components $X_j, j \in A$ and let $\mathcal{Y} = \mathbb{F}_p^A$ denote the set of possible values of $X(A)$.

Suppose first that $H(A|X_i = k) < H(A) - 1$ for some $k \in \mathbb{F}$. Now let B be a basis in A , that is, $|B| = H(B) = H(A)$. We have that $H(A|X_i = k) = H(B|X_i = k) + H(A|B, X_i = k)$ and $H(A|B, X_i = k) \leq H(A, X_i|B) = H(A|B) = 0$. Therefore, $H(B|X_i = k) < |B| - 1$.

Now let C be the unique circuit in $B \cup \{i\}$. It follows that $H(C) = H(C \setminus \{X_i\}) = |C| - 1$ and $H(B \setminus C|C) = H(B) - H(C) = |B \setminus C|$. In particular, the variables in $B \setminus C$ are independent of X_i in the marginal distribution on B and thus

$$H(B|X_i = k) = H(B \setminus C) + H(C \setminus \{X_i\}|X_i = k, B \setminus C) = |B \setminus C| + H(C|X_i = k).$$

This implies that $H(C|X_i = k) < |B| - |B \setminus C| - 1 = |C| - 2$. But $\mathbb{P}[X_i = k|X(C \setminus \{X_i\}) = c] \in \{0, 1\}$ and $\mathbb{P}[X(C \setminus \{X_i\}) = c] = p^{-|C|+1}$, which implies that $\mathbb{P}[X(C) = c] \in \{0, p^{-|C|+1}\}$ and $\mathbb{P}[X(C \setminus \{X_i\}) = c|X_i = k] \in \{0, p^{-|C|+2}\}$. Since these probabilities add up to one, it follows that exactly $p^{|C|-2}$ of them are non-zero, which yields

$$\begin{aligned} H(C|X_i = k) &= \sum_c \mathbb{P}[X(C \setminus \{X_i\}) = c|X_i = k] \log_p \left(\frac{1}{\mathbb{P}[X(C \setminus \{X_i\}) = c|X_i = k]} \right) \\ &= p^{|C|-2} \left(p^{-|C|+2} \log_p \left(\frac{1}{p^{-|C|+2}} \right) \right) \\ &= |C| - 2, \end{aligned}$$

a contradiction to the assumption $H(C) < |C| - 2$.

This implies that $H(A|X_i = k) \geq H(A) - 1$ for all A . Since

$$\begin{aligned} H(A) - 1 &= H(A|X_i) = \sum_{k=0}^{p-1} \mathbb{P}[X_i = k] H(A|X_i = k) \\ &= \sum_{k=0}^{p-1} \frac{1}{p} H(A|X_i = k) \geq p \cdot \frac{1}{p} (H(A) - 1) = H(A) - 1, \end{aligned}$$

it follows that we have $H(A|X_i = k) = H(A) - 1$ for all summands. This implies that the entropy of the conditional distribution yields the entropic matroid $M/\{X_i\}$ and this proves (ii).

Finally, (iii) follows by applying (ii) repeatedly. \square

This lemma proves that the property of being an entropic matroid is closed under taking minors. This means that in order to show entropic matroids belong to a minor-closed class of matroids, it suffices to show that the forbidden minors of this class are not entropic.

4 Secret-Sharing and Almost Affine Matroids

Secret-sharing matroids were introduced in Reference [28]. These matroids are motivated by the problem of secret-sharing in cryptography [29, 30], which refers to distributing a secret among a collection of parties via secret shares such that the secret can be reconstructed by combining a sufficient number (of possibly different types) of secret shares, while individual shares being of no use on their own.

We use the following definitions from Reference [25]: Let $A \in S^{I \times E}$ be a matrix, where S, I and E are finite sets. For $i \in I, e \in E$ and $Y \subseteq E \setminus \{e\}$, we define $n(i, e, Y) = \{a_{je} : j \in I, a_{jy} = a_{iy} \text{ for all } y \in Y\}$. Then A is a *secret-sharing matrix* if for $e \in E$ and $Y \subseteq E \setminus \{e\}$, either $n(i, e, Y) = S$ for all $i \in I$ or $|n(i, e, Y)| = 1$ for all $i \in I$. Any secret-sharing matrix induces a *secret-sharing matroid* with ground set E and rank function $r(Y)$ the logarithm with base $|S|$ of the number of distinct rows of the submatrix $A[Y] = (a_{ij} : i \in I, j \in Y)$ of A . In particular, Y is independent if and only if $A[Y]$ contains all vectors in S^Y .

The interpretation is as follows. Suppose some row $i \in I$ has been chosen in A but its value has been kept secret. Knowing A , one wishes to determine as much as possible

about the values $a_{ie}, e \in E$, without knowing which row has been selected. If by some means one has been able to determine the values a_{if} for all $f \in Y \subseteq E$. Then the possible values of a_{ie} for some $e \in E \setminus Y$, consistent with the available information, are precisely the members of $n(i, e, Y)$ (and this set can be determined despite not knowing i).

Secret-sharing matroids were connected to entropy rank functions in Reference [31], as further discussed below. We now formally connect the two classes of matroids.

Lemma 5. *If a matroid is p -entropic, then it is a secret-sharing matroid with a ground set of size p .*

Proof. Given a p -entropic matroid M with ground set E and rank (entropy) function H , we let A be the matrix containing all vectors in \mathbb{Z}_p^E which correspond to outcomes of positive probability in M . For every set Y of variables, $A[Y]$ contains the possible outcomes of these variables. These outcomes are all equally likely and the number of distinct outcomes with positive probability is $p^{H(Y)}$. This implies that to prove that M is a secret-sharing matroid, it suffices to prove that A is a secret-sharing matrix.

Let $e \in E$ and $Y \subseteq E \setminus \{e\}$. Then $n(i, e, Y)$ is the number of possible values of the random variable $X_e \in E$ associated with e when Y is fixed to its values in outcome i . But $H(X_e|Y) \in \{0, 1\}$ and if $H(X_e|Y) = 0$ then X_e is determined by the values of Y and $|n(i, e, Y)| = 1$ for all i ; if $H(X_e|Y) = 1$ then X_e is independent of the values of the variables in Y and thus $n(i, e, Y) = \mathbb{Z}_p$. This proves that A is a secret-sharing matrix. \square

Note that this proof remains true for any $p \in \mathbb{N}_{\geq 1}$, that is, it does not require the ground set to be a field. The converse of Lemma 5 is true as well: every secret-sharing matroid is p -entropic for some p . This was observed in Reference [31] and we include a proof for completeness. Together, this observation and Lemma 5 provide an alternative characterization of entropic matroids as secret-sharing matroids.

Lemma 6. *Every secret-sharing matroid with ground set S is $|S|$ -entropic.*

Proof. Let M be a secret-sharing matroid and A a secret-sharing matrix inducing M . Without loss of generality, we may assume that A does not contain two identical rows, since this does not affect the structure of the matroid. The definition of secret-sharing matroids implies that the number of rows of A is a power $|S|^r$ of $|S|$. We define a probability distribution on the set of random variables $\{X_e : e \in E\}$ by setting the probability that $(X_e)_{e \in E} = a$ as $|S|^{-r}$ for every row a of A .

We proceed by induction on $|E \setminus Y|$ to show that $H(Y)$ (with the Shannon entropy with base $|S|$) is integral for every $Y \subseteq E$ and moreover, that the resulting probability distribution on Y is the uniform distribution on the distinct rows of $A[Y]$. This is clearly true for $Y = E$, since $H(E) = r$. Let $Y \subset E$ and let $e \in E \setminus Y$, then by the induction hypothesis, $H(Y \cup \{e\}) = k \in \mathbb{N}$. The matrix $A[Y \cup \{e\}]$ has $|S|^k$ distinct rows and each distinct row has the same probability $|S|^{-k}$. If $H(X_e|Y) = 0$, then $H(Y) = k$ and distinct rows in $A[Y \cup \{e\}]$ are distinct rows of $A[Y]$ and thus the distribution of the variables in Y is the same as for the variables of $Y \cup \{e\}$. Therefore, we may assume that fixing the values of the variables in Y does not always determine X_e . This means that $n(i, e, Y) = |S|$ for all i . In particular, every distinct row of $A[Y]$ gives rise to $|S|$ distinct rows in $A[Y \cup \{e\}]$ and thus $A[Y]$ has $|S|^{k-1}$ distinct rows. Each distinct row has the same multiplicity $|S|^{r-k}$ in $A[Y \cup \{e\}]$ by the induction hypothesis and thus each distinct row of $A[Y]$ has multiplicity $|S|^{r-k+1}$. Now the resulting distribution of the variables in Y is a uniform distribution with $|S|^{k-1}$ distinct outcomes, therefore $H(Y) = k - 1$. Clearly, $r_M(Y) = k - 1$ and therefore this induction allows us to conclude that the rank in M coincides with the entropy of the constructed distribution. This implies the result. \square

Seymour [25] proved that the Vamos matroid is not a secret sharing matroid. This implies that it is not an entropic matroid for any p .

Moreover, there is a secret-sharing matroid which is not representable over the corresponding field (with $|S|$ elements) and which has been discovered by Simonis and

Ashikhmin [32]. This example is the non-Pappus matroid, shown in Figure 1. This matroid has nine elements $\{1, \dots, 9\}$ as its ground set E and each $X \subseteq E$ has rank $\min(|X|, 3)$ with the exception of the eight 3-elements sets shown as colored lines, which each have rank 2. Pappus' theorem proves that this matroid is not representable over any field.

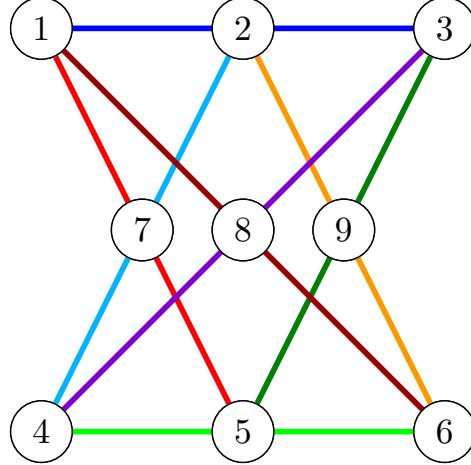


Figure 1: The non-Pappus matroid.

Simonis and Ashikhmin [32] show that the row space of the matrix

$$\begin{bmatrix} 10 & 10 & 00 & 10 & 00 & 10 & 10 & 10 & 00 \\ 01 & 01 & 00 & 01 & 00 & 01 & 01 & 01 & 00 \\ 00 & 00 & 00 & 10 & 10 & 21 & 01 & 10 & 10 \\ 00 & 00 & 00 & 02 & 01 & 20 & 12 & 02 & 01 \\ 00 & 10 & 10 & 01 & 00 & 01 & 00 & 11 & 10 \\ 00 & 01 & 01 & 21 & 00 & 21 & 00 & 10 & 01 \end{bmatrix}$$

is a secret-sharing matrix, where each entry of the matrix is considered as an element of \mathbb{F}_3^2 . They introduce another definition of entropic matroids via codes: a code (subset) $\mathcal{C} \subseteq S^E$ is *almost affine* if $r(Y) := \log_{|S|}(|\mathcal{C}_Y|) \in \mathbb{N}_0$ for all $Y \subseteq E$, where \mathcal{C}_Y denotes the projection of \mathcal{C} to the variables in Y . The corresponding matroid M with ground set E and rank function r is called an *almost affine matroid*. It is not hard to see that this definition coincides with secret-sharing matroids by using the codewords in C as the rows of the secret-sharing matrix A and vice versa. These results show that not all entropic matroids are representable by giving a 9-entropic matroid which is not representable over any field.

5 The Case $p = 2$

An \mathbb{F}_2 -representable matroid is called *binary*. The goal of this section is to prove the following.

Theorem 7. *Every 2-entropic matroid is binary.*

To prove this, we use the characterization of binary matroids proved by Tutte [33] stating that a matroid is binary if and only if it has no $U_{2,4}$ -minor. $U_{2,4}$ is the uniform matroid of rank two on four elements: $E = [4]$ and \mathcal{F} consists of all subsets of E of cardinality at most two. Using Tutte's characterization, the theorem follows from the next lemma.

Lemma 8. *$U_{2,4}$ is not 2-entropic.*

Proof. Suppose for a contradiction that μ is a probability distribution on four random variables X_1, \dots, X_4 whose entropy is the rank function of $U_{2,4}$, then $H(X_i) = 1$ for all i

and $H(X_i, X_j) = 2$ for all $i \neq j$; furthermore $H(X_1, X_2, X_3, X_4) = 2$. This implies that $\mathbb{P}[X_i = a, X_j = b] = \frac{1}{4}$ for all $i \neq j$ and $a, b \in \mathbb{F}_2$, because the marginal distribution of X_i and X_j has to be the product of two independent $\text{Ber}(\frac{1}{2})$ distributions to achieve an entropy of two.

Furthermore, $H(X_i, X_j | X_k, X_l) = 0$ for $\{i, j, k, l\} = [4]$ by the chain rule and therefore $\mathbb{P}[X_1 = a, X_2 = b, X_3 = c, X_4 = d] \in \{0, \frac{1}{4}\}$ for all a, b, c, d . Without loss of generality, we may assume that $\mathbb{P}[X_1 = 0, X_2 = 0, X_3 = 0, X_4 = 0] = \frac{1}{4}$ but then every other event in which at least two different variables X_i and X_j are zero must have probability zero, since $\mathbb{P}[X_i = 0, X_j = 0] = \frac{1}{4}$. Since $\mathbb{P}[X_i = 0, X_j = 1] = \frac{1}{4}$, it follows that all outcomes with three ones have probability $\frac{1}{4}$. Now $\frac{1}{4} = \mathbb{P}[X_1 = 1, X_2 = 1] \geq \mathbb{P}[X_1 = 1, X_2 = 1, X_3 = 0, X_4 = 1] + \mathbb{P}[X_1 = 1, X_2 = 1, X_3 = 1, X_4 = 0] = \frac{1}{2}$, a contradiction. \square

6 The Case $p = 3$

An \mathbb{F}_3 -representable matroid is called *ternary*. The following structure theorem has been proved independently by Seymour [34] and Bixby [35], who attributed it to Reid.

Theorem 9 (Seymour [34], Bixby [35]). *A matroid is ternary if and only if it contains no minor isomorphic to $U_{2,5}$, $U_{3,5}$, the Fano plane F_7 or its dual.*

The Fano plane, shown in Figure 2, has a ground set $E = [7]$ and can be represented over \mathbb{F}_2 by the column vectors of the matrix $\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$, that is, a set is independent if and only if it contains at most three vectors and it does not contain all three vectors on any line (including the circle).

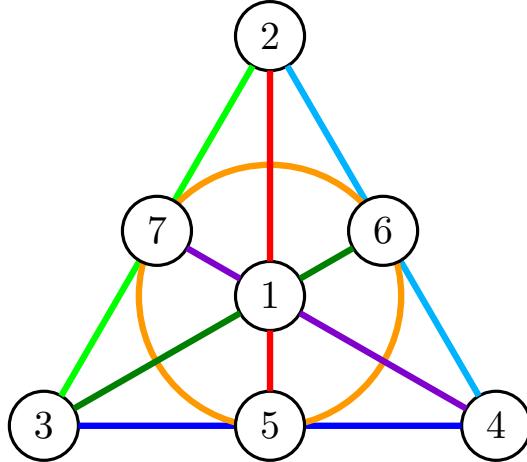


Figure 2: The Fano plane.

Lemma 10. $U_{2,5}$ is not 3-entropic.

Proof. Suppose for a contradiction that there exist $X = (X_1, \dots, X_5)$ such that $H(A) = \min\{|A|, 2\}$ for all $A \subseteq \{X_1, \dots, X_5\}$. Then, for any choice of $\{a, b, c, d, e\} = \{1, 2, 3, 4, 5\}$, we have that $H(X_a, X_b, X_c | X_d, X_e) = 0$ and thus for any vector $x \in \mathbb{F}_3^5$,

$$\mathbb{P}[X_a = x_a, X_b = x_b, X_c = x_c | X_d = x_d, X_e = x_e] \in \{0, 1\}$$

and $\mathbb{P}[X = x] \in \{0, \frac{1}{9}\}$.

As in the proof for $U_{2,4}$, we may assume that $\mathbb{P}[X = 0] = \frac{1}{9}$ but then any other event with at least two zeros must have probability 0. This leaves six events, five with one zero and one with no zeros; but each of them has probability at most $\frac{1}{9}$, thus the total probabilities add up to at most $\frac{7}{9}$, a contradiction. \square

Lemma 11. $U_{3,5}$ is not 3-entropic.

Proof. As before, we suppose for a contradiction that there is a vector $X = (X_1, \dots, X_5)$ of random variables such that $H(A) = \min\{|A|, 3\}$ for all $A \subseteq \{X_1, \dots, X_5\}$.

Every three distinct variables are independent and they determine the other two variables. It follows that, for every event, its probability is either zero or $\frac{1}{27}$. But there are only 81 outcomes and 27 of them occur with positive probability. Each of those 27 must differ from the others in at least three places, because if two outcomes are equal in three positions, the other two are determined and thus equal. This means that the Hamming balls of radius 1 around the outcomes with positive probability are disjoint. Each of these Hamming balls contains 11 elements: the outcome with positive probability and the outcomes in which one variable is flipped to one of the two other possible values. Therefore, we have at least $27 \cdot 11 = 297$ outcomes, a contradiction. \square

Lemma 12. The Fano plane is not 3-entropic.

Proof. Suppose for a contradiction that the Fano plane is 3-entropic and that $X = \{X_1, \dots, X_7\}$ is a set of random variables whose entropy corresponds to their rank in the Fano matroid as shown in Figure 2. Since the maximum size of an independent set in the Fano matroid is three, any three independent variables determine the values of all the others; in particular, there are at most 27 outcomes with positive probability, which we denote by their values on the independent set X_1, X_2, X_3 . Since $H(X_1, X_2, X_3) = 3$, each of these outcomes has probability $\frac{1}{27}$, whereas all other outcomes have probability zero. It follows that we have a map $f: \mathbb{F}_3^3 \rightarrow \mathbb{F}_3^4$ mapping the values on X_1, X_2, X_3 to the values on X_4, \dots, X_7 , where X_2 and X_3 determine X_7 , X_1 and X_2 determine X_5 and X_3 and X_1 determine X_6 but every change of one of X_1, X_2, X_3 must change X_4 .

We consider the set of nine assignments of X_1, X_2, X_3 for which $X_4 = 0$. If every two of these have pairwise distance at least three, we can only have three distinct assignments. This implies that we may assume that there are two assignments with distance two. Furthermore, if we fix any two digits, exactly one choice is valid for the remaining digit. Therefore, up to isomorphism (exchanging symbols), the set looks as follows: $\{000, 012, 021, 102, 111, 120, 201, 210, 222\}$; and thus $X_4 = X_1 + X_2 + X_3$.

The random variables X_2, X_3, X_4 determine X_5, X_6, X_7 and X_1 . In particular, both of the pairs $X_1, X_1 + X_2 + X_3$ and X_2, X_3 determine X_7 .

Changing X_1 does not change X_7 and neither does simultaneously adding k to X_2 and subtracting k from X_3 . Therefore, keeping $X_2 + X_3$ constant will keep X_7 constant and $H(X_7|X_2+X_3) = 0$, and $H(X_2+X_3|X_7) = 0$. This implies that there is a one-to-one correspondence between X_7 and $X_2 + X_3$ and similarly between X_6 and $X_2 + X_4$ and between X_5 and $X_3 + X_4$. But then X_5, X_6, X_7 allow us to find $X_2 + X_3, X_2 + X_4$ and $X_3 + X_4$ and thus $2X_2 + 2X_3 + 2X_4$ and $X_2 + X_3 + X_4$ (since $2 \neq 0$ in \mathbb{F}_3), which is X_1 . This shows that $H(X_1|X_5, X_6, X_7) = 0$ and thus $3 = H(X_1, X_5, X_6, X_7) = H(X_5, X_6, X_7) = 2$, a contradiction. \square

The above proof actually shows that the Fano plane is not p -entropic for any $p > 2$, which gives an alternative proof that it is not \mathbb{F}_p -representable for $p > 2$ either.

The dual F_7^* of the Fano plane is \mathbb{F}_2 -representable and a representation is given by

$$\text{the columns of the matrix } \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \text{. This shows that every 3-element set}$$

is independent in F_7^* , thus its circuits are exactly the complements of the three-element circuits of the Fano plane. To give a better understanding of these matroids, we expanded the symmetrical representation of F_7 given in Reference [36] and shown in Figure 3a to F_7^* . The result is shown in Figure 3b. Each color connects the elements of a circuit in one figure and the corresponding circuit given by its complement in the other figure. The cyclical order of the nodes in Figure 3a yields a rainbow Hamilton cycle (one edge of each color) in Figure 2.

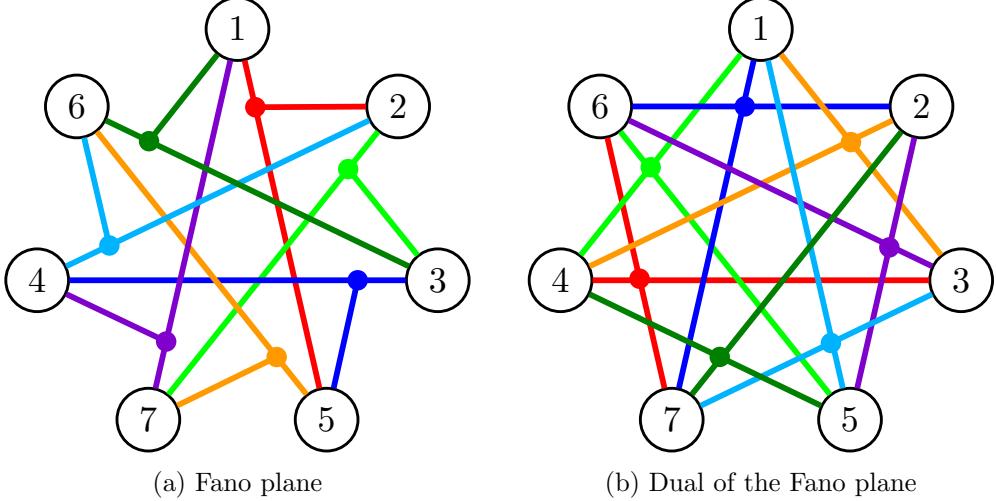


Figure 3: A symmetrical view of the circuits of the Fano plane and its dual.

Lemma 13. *The dual of the Fano plane is not 3-entropic.*

Proof. Suppose for a contradiction that $X = (X_1, \dots, X_7)$ is a vector of random variables whose entropy coincides with the rank function of F_7^* . Since $H(X_2, X_3, X_4, X_5) = 4$ and $H(X) = 4$, $\mathbb{P}[X = x] \in \{0, \frac{1}{81}\}$ for all $x \in \mathbb{F}_3^7$. We refer to the events with positive probability as outcomes.

By permuting the symbols, we may assume that 0000000 is a possible outcome. We consider the other outcomes (X_1, X_6, X_7) for $X_2 = 0$. No two of these outcomes can have distance one, because X_1, X_2, X_6, X_7 is a cycle, so for fixed X_2 , any two distinct possible outcomes must have distance at least two on their restriction to (X_1, X_6, X_7) . In the proof of the previous lemma, we have already shown that by switching digits, we may assume that the set of images is $\{000, 012, 021, 102, 111, 120, 201, 210, 222\}$. As shown in Figure 4, this also determines the other two sets (but not necessarily which of them is which). This shows that $X_1 + X_6 + X_7$ is sufficient to determine X_2 and vice versa; by flipping symbols 1 and 2 for X_2 , we may assume that $X_1 + X_6 + X_7 = X_2$.

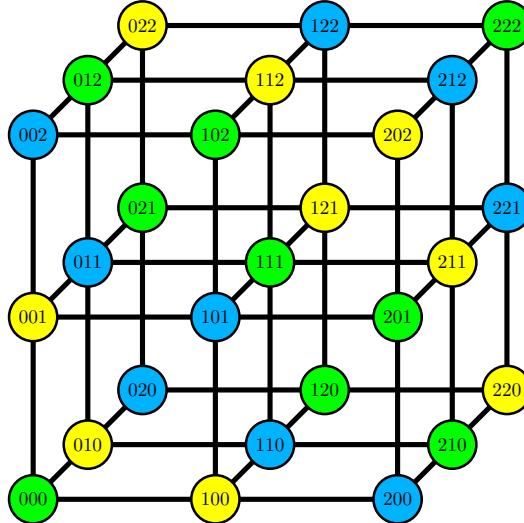


Figure 4: Values of (X_1, X_6, X_7) colored by corresponding value of X_2 .

We now fix X_3 . Then X_4 is determined by either $X_1, X_2 = X_1 + X_6 + X_7$ or X_6, X_7 and thus changing X_1 or adding k to X_6 and subtracting it from X_7 does not change X_4 . This implies that X_4 depends only on $X_6 + X_7$ (and X_3) and thus $H(X_3, X_4, X_6 + X_7) = 2$.

Analogously, $H(X_3, X_5, X_1 + X_7) = 2$ and $H(X_4, X_5, X_1 + X_6) = 2$. Therefore, X_3, X_4 and X_5 determine $X_6 + X_7 + X_1 + X_7 + X_1 + X_6 = 2(X_1 + X_6 + X_7) = 2X_2$ and since $2 \neq 0$ in \mathbb{F}_3 , this shows that $H(X_2, X_3, X_4, X_5) = 3$, contradicting the assumption that X had the entropy function given by the rank in F_7^* . \square

Combining these four lemmas with the characterization of ternary matroids, we have proved the following theorem (the interesting part being the only if part).

Theorem 14. *A matroid is 3-entropic if and only if it is \mathbb{F}_3 -representable.*

7 Comments for General Primes p

For ground sets of arbitrary size p , being p -representable is a stronger assumption than being p -entropic as the example of Simonis and Ashikhmin [32] of the non-Pappus matroid (see Figure 1) shows. However, no counterexamples exist in the case where the ground set has prime order.

In this section, we show that for primes p , every p -entropic matroid of rank at most two is linear, that is, let M be an entropic matroid with ground set E and $H(E) \leq 2$, then M is linear. If $H(E) < 2$, this is true since any basis has at most one element. Furthermore, we may assume that every $X \in E$ satisfies $H(X) = 1$, for otherwise X is deterministic and is represented by the zero vector in every linear representation.

Lemma 15. *Let M be a p -entropic matroid of rank 2. If there are two elements X and Y in the ground set E with $H(X, Y) = 1$, then M is \mathbb{F}_p -linear if and only if $M \setminus \{X\}$ is.*

Proof. If M is \mathbb{F}_p -representable, then so is $M \setminus \{X\}$, since it is a minor-closed property. Suppose that $M \setminus \{X\}$ is representable and let $f: E \setminus \{X\} \rightarrow V$ be a representation and let $g: E \rightarrow V$ be defined as $f(Z)$ for $Z \neq X$ and $f(X) = f(Y)$. Let $S \subseteq E$. Then $\dim(\text{span}(g(S))) = H(S)$ for $X \notin S$. If $X \in S$ but $Y \notin S$, then $\dim(\text{span}(g(S))) = \dim(\text{span}(f(S \cup \{Y\}))) = H(S \cup \{Y\})$ and

$$\begin{aligned} H(S \cup \{Y\}) &= H(S) + H(Y|S) \\ &= H(S) + H(X|S) + H(X, Y|S) - H(X|S) + H(Y|S) - H(X, Y|S) \\ &= H(S) + H(X|S) + H(Y|X, S) - H(X|Y, S) = H(S \cup \{X\}). \end{aligned}$$

If $X, Y \in S$, then $\dim(\text{span}(g(S))) = \dim(\text{span}(f(S \setminus \{X\}))) = H(S \setminus \{X\}) = H(S)$ by applying submodularity to the sets $\{X, Y\}$ and $S \setminus \{X\}$. This proves that g is an \mathbb{F}_p -representation of M . \square

With the above lemma, we have reduced the problem to considering uniform matroids. For any prime p , the uniform matroid $U_{2,p+1}$ is \mathbb{F}_p -representable by choosing the images of E as

$$(0, 1), (1, 0), (1, 1), (1, 2), \dots, (1, p-1) \in \mathbb{F}_p^2.$$

Each pair of these $p+1$ vectors is independent and a basis of \mathbb{F}_p^2 , thus they represent $U_{2,p+1}$. The following lemma shows that any larger uniform matroid is neither p -entropic nor \mathbb{F}_p^2 -representable.

Lemma 16. *The uniform matroid $U_{2,p+2}$ is not p -entropic for any $p \in \mathbb{N}_{\geq 2}$.*

Proof. Suppose not and let C denote the set of possible outcomes for a probability distribution on $p+2$ variables representing $U_{2,p+2}$. By changing symbols, we may assume that $(0, \dots, 0)$ is a possible outcome. Furthermore, there are p^2 outcomes and hence p of them begin with a zero. These p outcomes have the same value at the first coordinate X_1 but all other values are distinct (i.e., each X_i for $i > 1$ takes all of its p possible values exactly once among these p outcomes, including value zero for outcome $(0, \dots, 0)$). Therefore, we can simultaneously change the other symbols so that these p outcomes become $(0, 0, \dots, 0), (0, 1, \dots, 1), (0, 2, \dots, 2), \dots, (0, p-1, \dots, p-1)$. But then any other outcome not starting with zero satisfies that X_2, \dots, X_{p+2} all take different values in \mathbb{Z}_p . Since there are only p values but $p+1$ variables, this is a contradiction. \square

This shows that line matroids, which are among the forbidden minors of binary and ternary matroids, are p -entropic if and only if they are \mathbb{F}_p -linear.

8 Application: Entropic Matroids in Coding

We recall here a result proved in Reference [12] that makes entropic matroids emerge in a probabilistic context and which gives further motivations to studying entropic matroids. The result gives in particular a rate-optimal code for compressing correlated sources, similarly to the channel counter-part developed in Reference [37].

Let $X^n = (X_1, \dots, X_n)$ be an i.i.d. sequence of discrete random variables taking values in \mathcal{X}^m . That is, X^n is an $m \times n$ random matrix with i.i.d. columns of distribution μ on \mathcal{X}^m . One can assume that the support of \mathcal{X} is finite (countable supports can be handled with truncation arguments) and to further simplify, we assume that \mathcal{X} is binary, associating each element in the binary field, that is, $\mathcal{X} = GF(2)$.

Due to the i.i.d. nature of the sequence, the entropy of X^n is the sum of each components' entropies $H(\mu)$, i.e.,

$$H(X^n) = nH(\mu). \quad (7)$$

The next result shows that it is possible to transform the sequence X^n with an invertible map that extracts the entropy in subsets of the components. In words, the transformation takes the i.i.d. vectors under an arbitrary μ to a sequence of distributions that correspond in the limit to entropic matroids.

Theorem 17 (Abbe [12]). *Let m be a positive integer, n be a power of 2 and X^n be an $m \times n$ random matrix with i.i.d. columns of distribution μ on \mathbb{F}_2^m . Let $Y^n = X^n G_n$ over \mathbb{F}_2 , where $G_n = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{\otimes \log_2(n)}$. For any $\varepsilon = O(2^{-n^\beta})$, $\beta < 1/2$, we have*

$$|\{i \in [n] : H(Y_i[S]|Y^{i-1}) \notin \mathbb{Z} \pm \varepsilon, \text{ for any } S \subseteq [m]\}| = o(n). \quad (8)$$

In other words, one starts with an i.i.d. sequence of random vectors under a distribution μ that defines an *entropic polymatroid* $[m] \supseteq S \mapsto H(S)$ and after the transformation G_n , one obtains a sequence of random vectors which is no longer i.i.d. but where each random vector given the past defines an *entropic matroid* in the limit. Having a matroid structure is of course much easier to handle for compression purposes, one simply has to pick a basis for each matroid, store the components in that basis and the other components are fully dependent on these so they can be recovered without being stored. Of course, in practice n is large but finite, and each random vector defines a polymatroid that is *close* to a matroid but a continuity argument allows to show that the components outside of the bases can still be recovered but only *with high probability*. Since a compression code is allowed to fail with a low probability of error, this is not an issue. Understanding the structure of these entropic matroids allows then one to better understand how the stored components can be allocated over the different components—see Reference [12] for further details.

9 Acknowledgements

This research was partly funded by NSF grant CIF-1706648.

References

- [1] Oxley, J.G. *Matroid Theory*; Oxford University Press: Oxford, UK, 2006; Volume 3.
- [2] Woodall, D.R. Matroid Theory: Types of Matroids Lecture Notes. Available online: <https://www.maths.nottingham.ac.uk/personal/drw/PG/matroid.ch3.pdf>.

- [3] Fujishige, S. Polymatroidal dependence structure of a set of random variables. *Inf. Control* **1978**, *39*, 55–72.
- [4] Lovász, L. Submodular functions and convexity. In *Mathematical Programming—The State of the Art*; Bachem, A., Grötschel, M., Korte, B., Eds.; Springer: Berlin, Germany, 1982; pp. 234–257.
- [5] Edmonds, J. *Submodular Functions, Matroids and Certain Polyhedra*; Lecture Notes in Computer Science; Springer: Berlin, Germany, 2003.
- [6] Han, T.S. A uniqueness of shannon’s information distance and related nonnegativity problems. *J. Comb. Inf. Syst. Sci.* **1981**, *6*, 320–331.
- [7] Li, C.; Walsh, J.M.; Weber, S. Matroid bounds on the region of entropic vectors. In Proceedings of the 2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2–4 October 2013; pp. 796–803.
- [8] Zhang, Z.; Yeung, R. On characterization of entropy function via information inequalities. *IEEE Trans. Inf. Theory* **1998**, *44*, 1140–1452.
- [9] Yeung, R.W. *Information Theory and Network Coding*; Springer: Berlin, Germany, 2008.
- [10] Matúš, F. On Equivalence of Markov Properties over Undirected Graphs. *J. Appl. Probab.* **1992**, *29*, 745–749.
- [11] Matúš, F. Probabilistic conditional independence structures and matroid theory: Background. *Int. J. Gen. Syst.* **1994**, *22*, 185–196.
- [12] Abbe, E. Randomness and dependencies extraction via polarization, with applications to Slepian-Wolf coding and secrecy. *IEEE Trans. Inf. Theory* **2015**, *61*, 2388–2398.
- [13] Abbe, E. Mutual information, matroids and extremal dependencies. *arXiv* **2010**, arXiv:1012.4755.
- [14] Kahn, J.; Seymour, P. On forbidden minors for GF(3). *Proc. Am. Math. Soc.* **1988**, *102*, 437–440.
- [15] Geelen, J.F.; Gerards, A.; Kapoor, A. The excluded minors for GF(4)-representable matroids. *J. Comb. Theory Ser. B* **2000**, *79*, 247–299.
- [16] Kahn, J. On the uniqueness of matroid representations over GF(4). *Bull. Lond. Math. Soc.* **1988**, *20*, 5–10.
- [17] Kung, J.P.; Oxley, J.G. Combinatorial geometries representable over GF(3) and GF(q). ii. dowling geometries. *Gr. Comb.* **1988**, *4*, 323–332.
- [18] Kung, J.P. Combinatorial geometries representable over GF(3) and GF(q). i. the number of points. *Discret. Comput. Geom.* **1990**, *5*, 83–95.
- [19] Whittle, G. On matroids representable over GF(3) and other fields. *Trans. Am. Math. Soc.* **1997**, *349*, 579603.
- [20] Apte, J.; Li, C.; Walsh, J.M. Algorithms for computing network coding rate regions via single element extensions of matroids. In Proceedings of the 2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA , 29 June–4 July 2014; pp. 2306–2310.
- [21] Salimi, A.; Médard, M.; Cui, S. On the representability of integer poly- matroids: Applications in linear code construction. In Proceedings of the 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Aller- ton), Monticello, IL, USA, 29 September–2 October 2015; pp. 504–508.
- [22] Chan, T.; Grant, A.; Kern, D. Existence of new inequalities for representable polymatroids. In Proceedings of the 2010 IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; pp. 13641368.
- [23] Chan, T.; Grant, A.; Pfluger, D. Truncation technique for characterizing linear polymatroids. *IEEE Trans. Inf. Theory* **2011**, *57*, 6364–6378.

- [24] Matúš, F. Classes of matroids closed under minors and principal extensions. *Combinatorica* **2018**, *38*, 935–954.
- [25] Seymour, P. On secret-sharing matroids. *J. Comb. Theory Ser. B* **1992**, *56*, 69–73.
- [26] Beimel, A.; Livne, N.; Padro, C. Matroids can be far from ideal secret sharing. In *Theory of Cryptography Conference*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 194–212.
- [27] Martin, S.; Padro, C.; Yang, A. Secret sharing, rank inequalities, and information inequalities. *IEEE Trans. Inf. Theory* **2015**, *62*, 599–609.
- [28] Brickell, E.F.; Daniel, M.D. On the classification of ideal secret sharing schemes. *J. Cryptol.* **1991**, *4*, 123–134.
- [29] Blakley, G.R. Safeguarding Cryptographic Keys. In Proceedings of the 1979 AFIPS National Computer Conference, Monval, NJ, USA, 1979; Volume 48, pp. 313–317.
- [30] Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613.
- [31] Martí-Farré, J.; Padró, C. On secret sharing schemes, matroids and polymatroids. In *Theory of Cryptography Conference*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 273–290.
- [32] Simonis, J.; Alexei, A. Almost affine codes. *Des. Codes Cryptogr.* **1998**, *14*, 179–197.
- [33] Tutte, W.T. A homotopy theorem for matroids II. *Trans. Am. Math. Soc.* **1958**, *88*, 144–174.
- [34] Seymour, P. Matroid representation over $GF(3)$. *J. Comb. Theory Ser. B* **1979**, *26*, 159–173.
- [35] Bixby, R.E. On Reid’s characterization of the ternary matroids. *J. Comb. Theory Ser. B* **1979**, *26*, 174–204.
- [36] Pegg Jr., E. Math Games: The Fano Plane. Available online: http://www.mathpuzzle.com/MAA/47-Fano/mathgames_05_30_06.html.
- [37] Abbe, E.; Telatar, E. Polar codes for the m-user multiple access channel. *IEEE Trans. Inf. Theory* **2012**, *58*, 5437–5448.