Matroids Can Be Far From Ideal Secret Sharing

Amos Beimel[1,⋆], Noam Livne[2,⋆⋆], and Carles Padró[3,⋆⋆⋆]

[1] Dept. of Computer Science
Ben-Gurion University
Beer-Sheva, Israel
beimel@cs.bgu.ac.il
[2] Weizmann Institute of Science
Rehovot, Israel
noam.livne@weizmann.ac.il
[3] Dept. of Applied Mathematics 4
Universitat Politècnica de Catalunya
Barcelona, Spain
cpadro@ma4.upc.edu

Abstract. In a secret-sharing scheme, a secret value is distributed among a set of parties by giving each party a share. The requirement is that only predefined subsets of parties can recover the secret from their shares. The family of the predefined authorized subsets is called the access structure. An access structure is ideal if there exists a secret-sharing scheme realizing it in which the shares have optimal length, that is, in which the shares are taken from the same domain as the secrets. Brickell and Davenport (J. of Cryptology, 1991) proved that ideal access structures are induced by matroids. Subsequently, ideal access structures and access structures induced by matroids have received a lot of attention. Seymour (J. of Combinatorial Theory, 1992) gave the first example of an access structure induced by a matroid, namely the Vamos matroid, that is non-ideal. Beimel and Livne (TCC 2006) 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.

In this work, we substantially improve those bounds by proving that the size of the domain of the shares in every secret-sharing scheme for those access structures is at least $k^{1.1}$, where k is the size of the domain of the secrets (compared to $k + \Omega(\sqrt{k})$ in previous works). Our bounds are obtained by using non-Shannon inequalities for the entropy function. The importance of our results are: (1) we present the first proof that there exists an access structure induced by a matroid which is not nearly ideal, and (2) we present the first proof that there is an access structure whose information rate is strictly between 2/3 and 1. In addition, we present a better lower bound that applies only to *linear* secret-sharing schemes realizing the access structures induced by the Vamos matroid.

⋆ Partially supported by the Frankel Center for Computer Science at the Ben-Gurion University.

⋆⋆ Partially supported by the Israel Science Foundation (grant No. 460/05).

⋆⋆⋆ Partially supported by the Spanish Ministry of Education and Science under project TSI2006-02731.

1 Introduction

1.1 Ideal Secret-Sharing Schemes and Matroids

Secret-sharing schemes, which were introduced by Shamir [31] and Blakley [5] nearly 30 years ago, are nowadays used in many cryptographic protocols. In these schemes there is a finite set of parties, and a collection $\mathcal{A}$ of subsets of the parties (called the access structure). A secret-sharing scheme for $\mathcal{A}$ is a method by which a dealer distributes shares of a secret value to the parties such that (1) any subset in $\mathcal{A}$ can reconstruct the secret from its shares, and (2) any subset not in $\mathcal{A}$ cannot reveal any partial information about the secret in the information-theoretic sense. Clearly, the access structure $\mathcal{A}$ must be monotone, that is, all supersets of a set in $\mathcal{A}$ are also in $\mathcal{A}$.

Ito, Saito, and Nishizeki [18] proved that there exists a secret-sharing scheme for every monotone access structure. Their proof is constructive, but the obtained schemes are very inefficient: the ratio between the length in bits of the shares and that of the secret is exponential in the number of parties. Nevertheless, some access structures admit secret-sharing schemes with much shorter shares. A secret-sharing scheme is called *ideal* if the shares of every participant are taken from the same domain as the secret. As proved in [20], this is the optimal size for the domain of the shares. The access structures which can be realized by ideal secret-sharing schemes are called *ideal access structures*.

The exact characterization of ideal access structures is a longstanding open problem, which has interesting connections to combinatorics and information theory. The most important result towards giving such characterization is by Brickell and Davenport [8], who proved that every ideal access structure is induced by a matroid, providing a necessary condition for an access structure to be ideal. A sufficient condition is obtained as a consequence of the linear construction of ideal secret-sharing schemes due to Brickell [7]. Namely, an access structure is ideal if it is induced by a matroid that is representable over some finite field. However, there is a gap between the necessary condition and the sufficient condition. Seymour [30] proved that the access structures induced by the Vamos matroid are not ideal. Other examples of non-ideal access structures induced by matroids have been presented by Matúš [26]. Hence, the necessary condition above is not sufficient. Moreover, Simonis and Ashikmin [33] constructed ideal secret-sharing schemes for the access structures induced by the non-Pappus matroid, which is not representable over any field. This means that the sufficient condition is not necessary. Therefore, the study of the access structures that are induced by matroids is useful in the search of new results about the characterization of ideal access structures.

Another motivation in studying access structures induced by matroids arises from the separation result of Martí-Farré and Padró [24]. Namely, by using an old result by Seymour [29], they generalized the result by Brickell and Davenport [8], proving that in every secret-sharing scheme whose access structure is *not* induced by a matroid there is at least one participant whose domain of shares has size at least $k^{1.5}$, where k is the size of the domain of secrets. In other words, by proving that an access structure is not induced by a matroid, we prove a lower bound of $k^{1.5}$ for the size of the shares' domain. Therefore, the access structures that are not induced by matroids are clearly far from being ideal.

We rephrase the above result using the notion of information rate of [9]. The *information rate* of a secret-sharing scheme is $\log k/\log s$, where k is the size of the domain of the secrets and s is the maximum size of the domains of shares. That is, the information rate is the relation between the length in bits of the secret and the maximum length of the shares. Ideal secret-sharing schemes are those having information rate equal to 1. The information rate of an access structure $\mathcal{A}$ is the supermum of the information rates of all secret-sharing schemes realizing the access structure with a finite domain of shares. Stating the aforementioned result in the new notation, if $\mathcal{A}$ is not induced by a matroid, the information rate of every secret-sharing scheme for $\mathcal{A}$ is at most 2/3, hence the information rate of $\mathcal{A}$ is at most 2/3. This is not the case for the non-ideal access structures induced by matroids, which can be very close to ideal. An access structure $\mathcal{A}$ is *nearly ideal* if its information rate is 1. A non-ideal but nearly-ideal access structure is presented in [22, 27].

At this point, two natural open questions arise. First, which matroids induce ideal access structures? And second, what can be said about the optimal size of the shares' domain for access structures induced by matroids?

Even though several interesting results have been given in [33, 26, 27], the first question is far from being solved. Since an ideal secret-sharing scheme can be seen as a representation of the corresponding matroid, this question can be thought of as a representability problem. Very little is known about the second question. For instance, the only known non-trivial lower bound on the optimal size of the shares' domain for access structures induced by matroids has been presented by Beimel and Livne [2]. Specifically, for an access structure induced by the Vamos matroid, they prove a lower bound of $k + \Omega(\sqrt{k})$, where k is the size of the domain of the secrets.

The best constructions of secret-sharing realizing access structures induced by matroids are the constructions for general access structures, e.g., in [4, 32, 7, 19]; in these constructions most access structures induced by matroids require shares of exponential length. However, prior to this work, even the following question was open.

Question 1 *Does there exist a matroid such that its induced access structures are not nearly ideal?*

Observe that the lower bound given in [2] for an access structure induced by the Vamos matroid does not imply that it is not nearly ideal. For comparison, for general access structures the best known lower bound is given by Csirmaz [13] who proves that for every n there is an access structure $\mathcal{A}_n$ with n participants such that for every secret-sharing scheme realizing $\mathcal{A}_n$ there is at least one participant whose share has length at least $(n/\log n)\log k$.

Moreover, the following open problem, which was posed by Martí-Farré and Padró [23], was unsolved.

Question 2 *Does there exist an access structure whose optimal share size is $\Theta(k^{\alpha})$ for some constant $1 < \alpha < 3/2$?*

That is, Martí-Farré and Padró ask if there is an access structure whose information rate is strictly between 2/3 and 1. As a consequence of the result of [24], if such an access structure exists, it must be induced by a matroid.

1.2 Our Results

In this paper we answer the above two questions about access structures induced by matroids. Specifically, we prove new lower bounds on the size of the domains of shares in secret-sharing schemes for the access structures induced by the Vamos matroid, substantially improving the bound given in [2]. The Vamos matroid induces two non-isomorphic access structures. We prove for them lower bounds on the size of the domains of shares of, respectively, $k^{10/9}$ and $k^{11/10}$, where k is the size of the domain of the secrets (compared to $k + \Omega(\sqrt{k})$ in [2]).

Therefore, we present here the first examples of access structures induced by matroids that are not nearly ideal, resolving Question 1. Moreover, we solve Question 2 in the affirmative: As a consequence of our lower bound and the upper bound of $k^{4/3}$ that was proved in [25], the access structures induced by the Vamos matroid are the required examples.

The interest of our result is increased by the use of the so called non-Shannon inequalities in our proof. By using the basic properties of the entropy function, namely, the so-called Shannon inequalities, Csirmaz [13] proved the best known lower bounds for secret-sharing schemes mentioned above. On the negative side, Csirmaz proved that using only Shannon inequalities one cannot improve his lower bounds by a factor larger than $\log n$. More relevant to this work, several bounds on the joint entropy of the shares of subsets of parties for access structures induced by matroids were proved in [2] using Shannon inequalities (see Theorem 14 and Theorem 15 in Section 2 below). However, these bounds are only on the joint entropy of the shares and the authors of [2] could not use them to prove lower bounds for access structures induced by matroids. This is not a coincidence as in [24] it is proved that it is not possible to obtain bounds for access structures induced by matroids by using only this technique (since the rank function of the matroid satisfies the Shannon inequalities).

Nevertheless, there exist several inequalities for the entropies of a set of random variables that cannot be deduced from the Shannon inequalities. These are the so-called non-Shannon inequalities. The first examples of such inequalities were given by Zhang and Yeung [36], and other examples have been found subsequently [15]. In this paper, we combine the entropy inequalities of [2] and the non-Shannon inequality of Zhang and Yeung [36] to obtain a simple and elegant proof of our result. The inequality of [36] was previously used related to the Vamos matroid in [16] for proving lower bounds for network coding and in [27] for proving that this matroid is not asymptotically entropic (the latter result gives an alternative proof that the access structures induced by the Vamos matroid are not ideal). We believe that non-Shannon inequalities will be used for proving new lower bounds for secret-sharing schemes, possibly improving the best known lower bound given by Csirmaz [13].

In addition, by applying a similar technique to the Ingleton's inequality [17, 28], which applies only to linear random variables, we obtain a lower bound of $k^{5/4}$ for the size of the shares' domains for *linear* secret-sharing schemes whose access structures are induced by the Vamos matroid.

2 Preliminaries

In this section we define secret-sharing schemes, review some background on matroids, and discuss the connection between secret-sharing schemes and matroids. The definition of secret-sharing presented in this paper uses the entropy function; in the appendix we review the relevant definitions from information theory.

2.1 Secret Sharing

Definition 1 (Access Structure). *Let P be a finite set of parties. A collection $\mathcal{A} \subseteq 2^P$ is* monotone *if $B \in \mathcal{A}$ and $B \subseteq C$ imply that $C \in \mathcal{A}$. An* access structure *is a monotone collection $\mathcal{A} \subseteq 2^P$ of non-empty subsets of P. Sets in $\mathcal{A}$ are called* authorized*, and sets not in $\mathcal{A}$ are called* unauthorized*.*

Definition 2 (Distribution Scheme). *Let $P = \{p_1, \ldots, p_n\}$ be a set of parties, and $p_0 \notin P$ be a special party called* the dealer*. An n-party* distribution scheme *$\Sigma = \langle \Pi, \mu \rangle$ with domain of secrets K is a pair where μ is a probability distribution on some finite set R (the set of random strings) and Π is a mapping from $K \times R$ to a set of n-tuples $K_1 \times K_2 \times \ldots \times K_n$, where K_i is called the* share-domain *of p_i. A dealer distributes a secret $s \in K$ according to Σ by first sampling a string $r \in R$ according to μ, computing a vector of* shares *$\Pi(s, r) = (s_1, \ldots, s_n)$, and then privately communicating each share s_i to the party p_i.*

We next give a definition of secret-sharing scheme using the entropy function. This definition is the same as that of [20, 10] and is equivalent to the definition of [11, 1, 3]. Before stating the definition, we present some notations. Let $\mathcal{A}$ be an access structure on the set of parties P. We defined a distribution scheme Σ as a probabilistic mapping that given a secret s generates a vector of shares. It will be convenient to view the secret as the share of the dealer, and for every $T \subseteq P \cup \{p_0\}$ to consider the vector of shares of T. Any probability distribution on the domain of secrets, together with the distribution scheme Σ, induces, for any $T \subseteq P \cup \{p_0\}$, a probability distribution on the vector of shares of the parties in T. We denote the random variable taking values according to this probability distribution on the vector of shares of T by S_T, and by S the random variable denoting the secret (i.e., $S = S_{\{p_0\}}$). Note that for disjoint subsets T_1, T_2, the random variable denoting the vector of shares of $T_1 \cup T_2$ can be written either as $S_{T_1 \cup T_2}$ or as $S_{T_1} S_{T_2}$. For a singleton $\{b\}$, we will write S_b instead of $S_{\{b\}}$.

Definition 3 (Secret-Sharing Scheme). *We say that a distribution scheme is a secret-sharing scheme realizing an access structure $\mathcal{A}$ with respect to a given probability distribution on the secrets, denoted by a random variable S, if the following conditions hold.*

Correctness. *For every authorized set $T \in \mathcal{A}$, the shares of the parties in T determine the secret, that is,*

$$H(S|S_T) = 0. \tag{1}$$

Privacy. *For every unauthorized set $T \notin \mathcal{A}$, the shares of the parties in T do not disclose any information on the secret, that is,*

$$H(S|S_T) = H(S). \tag{2}$$

Remark 4. Although the above definition considers a specific distribution on the secrets, Blundo et al. [6] proved that its correctness and privacy are actually independent of this distribution: If a scheme realizes an access structure with respect to one distribution on the secrets, then it realizes the access structure with respect to any distribution with the same support.

Karnin et al. [20] have showed that the size of the domain of shares of each non-redundant party (that is, a party that appears in at least one minimal authorized set) is at least the size of the domain of secrets. This motivates the definition of ideal secret sharing.

Definition 5 (Ideal Secret-Sharing Scheme and Ideal Access Structure). *A secret-sharing scheme with domain of secrets K is* ideal *if the domain of shares of each party is K. An access structure $\mathcal{A}$ is* ideal *if there exists an ideal secret-sharing scheme realizing it over some finite domain of secrets.*

2.2 Matroids

A matroid is an axiomatic abstraction of linear independence. There are several equivalent axiomatic systems to describe matroids: by independent sets, by bases, by the rank function, or, as done here, by circuits. For more background on matroid theory the reader is referred to [35, 28].

Definition 6 (Matroid). *A matroid $\mathcal{M} = \langle V, \mathcal{C} \rangle$ is a finite set V and a collection $\mathcal{C}$ of subsets of V that satisfy the following three axioms:*

(C0) $\emptyset \notin \mathcal{C}$.
(C1) *If $X \neq Y$ and $X, Y \in \mathcal{C}$, then $X \nsubseteq Y$.*
(C2) *If C_1, C_2 are distinct members of $\mathcal{C}$ and $x \in C_1 \cap C_2$, then there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$.*

The elements of V are called points*, or simply* elements*, and the subsets in $\mathcal{C}$ are called* circuits*.*

For example, let $G = (V, E)$ be an undirected simple graph and $\mathcal{C}$ be the collection of simple cycles in G. Then, $(E, \mathcal{C})$ is a matroid.

Definition 7 (Rank, Independent and Dependent Sets). *A subset of V is* dependent *in a matroid $\mathcal{M}$ if it contains a circuit. If a subset is not dependent, it is* independent. *The* rank *of a subset $T \subseteq V$, denoted* $\mathrm{rank}(T)$, *is the size of the largest independent subset of T.*

Definition 8 (Connected Matroid). *A matroid is* connected *if for every pair of distinct elements x and y there is a circuit containing x and y.*

2.3 Matroids and Secret Sharing

In this section we describe the results relating ideal secret-sharing schemes and matroids. We first define access structures induced by matroids.

Definition 9. *Let $\mathcal{M} = \langle V, \mathcal{C} \rangle$ be a connected matroid and $p_0 \in V$. The* induced access structure of $\mathcal{M}$ with respect to p_0 *is the access structure $\mathcal{A}$ on $P = V \setminus \{p_0\}$ defined by*

$$\mathcal{A} \stackrel{def}{=} \{T : \text{ there exists } C_0 \in \mathcal{C} \text{ such that } p_0 \in C_0 \text{ and } C_0 \setminus \{p_0\} \subseteq T\}.$$

That is, a set T is a minimal authorized set of $\mathcal{A}$ if by adding p_0 to it, it becomes a circuit of $\mathcal{M}$. We think of p_0 as the dealer. We say that an access structure is induced *by $\mathcal{M}$, if it is obtained by setting some arbitrary element of $\mathcal{M}$ as the dealer. In this case, we say that $\mathcal{M}$ is the* appropriate matroid *of $\mathcal{A}$, and that $\mathcal{A}$ is* induced *by $\mathcal{M}$ with respect to p_0.*

Remark 10. The term *the appropriate matroid* is justified, as if some access structure is induced by a matroid, this matroid is unique.

The following fundamental result, proved by Brickell and Davenport [8], gives a necessary condition for an access structure to have an ideal secret-sharing scheme.

Theorem 11 ([8]). *If an access structure is ideal, then it has an appropriate matroid.*

The following result of [21] shows a connection between the rank function of the appropriate matroid and the joint entropy of the collections of shares.

Lemma 12 ([21]). *Assume that the access structure $\mathcal{A} \subseteq 2^P$ is ideal, and let $\langle P \cup \{p_0\}, \mathcal{C} \rangle$ be its appropriate matroid where $p_0 \notin P$. Let Σ be an ideal secret-sharing scheme realizing $\mathcal{A}$ where S is the random variable denoting the secret. Then $H(S_T) = \mathrm{rank}(T) \cdot H(S)$ for any $T \subseteq P \cup \{p_0\}$, where* $\mathrm{rank}(T)$ *is the rank of T in the matroid.*

Example 13. Consider the threshold access structure $\mathcal{A}_t$, which consists of all subsets of participants of size at least t, and Shamir's scheme [31] which is an ideal secret-sharing scheme realizing it. In this scheme, to share a secret s, the dealer randomly chooses a random polynomial $p(x)$ of degree $t-1$ such that $p(0) = s$, and the the share of the ith participant is $p(i)$. The appropriate matroid of $\mathcal{A}_t$ is the uniform matroid with $n+1$ points, whose circuits are the sets of size $t+1$ and $\text{rank}(T) = \min\{|T|, t\}$. Since every t points determine a unique polynomial of degree $t-1$, in Shamir's scheme $H(S_T) = \min\{|T|, t\}\, H(S)$, as implied by Lemma 12.

We next quote results from [2] proving lower and upper bounds on the size of shares' domains of subsets of parties in matroid-induced access structures. These results generalize the results of [21] on ideal secret-sharing schemes to non-ideal secret-sharing schemes for matroid-induced access structures.

Theorem 14 ([2]). *Let $\mathcal{M} = \langle V, \mathcal{C}\rangle$ be a connected matroid where $|V| = n+1$, and $p_0 \in V$. Furthermore, let $\mathcal{A}$ be the induced access structure of $\mathcal{M}$ with respect to p_0, and let Σ be* any *secret-sharing scheme realizing $\mathcal{A}$. For every $T \subseteq V$,*

$$H(S_T) \geq \text{rank}(T) \cdot H(S).$$

Theorem 15 ([2]). *Let $\mathcal{M} = \langle V, \mathcal{C}\rangle$ be a connected matroid where $|V| = n+1$, $p_0 \in V$ and let $\mathcal{A}$ be the induced access structure of $\mathcal{M}$ with respect to p_0. Furthermore, let Σ be* any *secret-sharing scheme realizing $\mathcal{A}$, and let $\lambda \geq 0$ be such that $H(S_v) \leq (1+\lambda)H(S)$ for every $v \in V \setminus \{p_0\}$. Then, for every $T \subseteq V$*

$$H(S_T) \leq \text{rank}(T)(1+\lambda)H(S) + (|T| - \text{rank}(T))\lambda n H(S). \tag{3}$$

2.4 The Vamos Matroid

In this paper we prove lower bounds on the size of shares in secret-sharing schemes realizing the access structures induced by the Vamos matroid. The Vamos matroid [34] is the smallest known matroid that is non-representable over any field, and is also non-algebraic (for more details on these notions see [35, 28]; we will not need these notions in this paper).

Definition 16 (The Vamos Matroid). *The Vamos matroid $\mathcal{V}$ is defined on the set $V = \{v_1, v_2, \ldots, v_8\}$. Its independent sets are all the sets of cardinality ≤ 4 except for five: $\{v_1, v_2, v_3, v_4\}$, $\{v_1, v_2, v_5, v_6\}$, $\{v_3, v_4, v_5, v_6\}$, $\{v_3, v_4, v_7, v_8\}$, and $\{v_5, v_6, v_7, v_8\}$.*

Note that these 5 sets are all the unions of two pairs from $\{v_1, v_2\}$, $\{v_3, v_4\}$, $\{v_5, v_6\}$, and $\{v_7, v_8\}$, excluding $\{v_1, v_2, v_7, v_8\}$. The five sets listed in Definition 16 are circuits in $\mathcal{V}$ while the set $\{v_1, v_2, v_7, v_8\}$ is independent; these facts will be used later.

There are two non-isomorphic access structures induced by the Vamos matroid. First, the access structures obtained by setting v_1, v_2, v_7, or v_8 as the dealer are isomorphic. The other access structure is obtained by setting v_3, v_4, v_5, or v_6 as the dealer.

Definition 17 (The Access Structures $\mathcal{V}_6$ and $\mathcal{V}_8$). *The access structure $\mathcal{V}_8$ is the access structure induced by the Vamos matroid with respect to v_8. That is, in this access structure the parties are $\{v_1, \dots, v_7\}$ and a set of parties is a minimal authorized set if this set together with v_8 is a circuit in $\mathcal{V}$. The access structure $\mathcal{V}_6$ is the access structure induced by the Vamos matroid with respect to v_6. That is, in this access structure the parties are $\{v_1, \dots, v_5, v_7, v_8\}$ and a set of parties is a minimal authorized set if this set together with v_6 is a circuit in $\mathcal{V}$.*

Example 18. We next give examples of authorized and non-authorized sets in $\mathcal{V}_6$.

1. The set $\{v_5, v_7, v_8\}$ is authorized, since $\{v_5, v_6, v_7, v_8\}$ is a circuit.
2. The circuit $\{v_1, v_2, v_3, v_4\}$ is unauthorized, since the set $\{v_1, v_2, v_3, v_4, v_6\}$ does not contain a circuit that contains v_6. To check this, we first note that this 5-set itself cannot be a circuit, since it contains the circuit $\{v_1, v_2, v_3, v_4\}$. Second, the only circuit it contains is $\{v_1, v_2, v_3, v_4\}$, which does not contain v_6.
3. The set $\{v_1, v_2, v_7, v_8\}$ is a minimal authorized set, since $\{v_1, v_2, v_6, v_7, v_8\}$ is a circuit (as it is dependent, and no circuit of size 4 is contained in it).

3 Lower Bounds for the Vamos Access Structure

In this section we prove our main result, stating that the access structures induced by the Vamos matroid cannot be close to ideal. That is, their information rate is bounded away from 1.

We will use a non-Shannon information inequality proved by Zhang and Yeung [36]. This inequality was used related to the Vamos matroid in [16] for proving lower bounds for network coding and in [27] for proving that a function is not asymptotically entropic.

Theorem 19 ([36, Theorem 3]). *For every four discrete random variables A, B, C, and D the following inequality holds:*

$$\begin{aligned} &3[H(CD) + H(BD) + H(BC)] + H(AC) + H(AB) \\ &\geq H(D) + 2[H(C) + H(B)] + H(AD) + 4H(BCD) + H(ABC). \end{aligned} \tag{4}$$

Seymour [30] proved that $\mathcal{V}_6$ and $\mathcal{V}_8$ are not ideal. Inequality (4) was used in [27] to give an alternative proof of this fact. We next present the proof of [27]. Assume there is an ideal secret-sharing scheme realizing the Vamos access structure $\mathcal{V}_6$. Define the following random variables

$$\begin{aligned} A &\stackrel{\text{def}}{=} S_{\{v_1,v_2\}}, \\ B &\stackrel{\text{def}}{=} S_{\{v_3,v_4\}}, \\ C &\stackrel{\text{def}}{=} S_{\{v_5,v_6\}}, \\ D &\stackrel{\text{def}}{=} S_{\{v_7,v_8\}}. \end{aligned} \tag{5}$$

By Lemma 12 $H(S_T) = \mathrm{rank}(T)H(S)$ for every set $T \subseteq \{v_1, \ldots, v_8\}$. Since all sets of size 2 are independent in the Vamos matroid, $H(A) = H(B) = H(C) = H(D) = 2H(S)$. Furthermore, by the definition of the circuits of size 4 in the Vamos matroid $H(AB) = H(AC) = H(BC) = H(BD) = H(CD) = 3H(S)$ while $H(AD) = 4H(S)$. Finally, $H(BCD) = H(ABC) = 4H(S)$. Under the above definition of A, B, C, and D we notice that the l.h.s. of (4) is $33H(S)$ while the r.h.s. of (4) is $34H(S)$, a contradiction. Note that this proof strongly exploits the fact that the random variable AD, which corresponds to the shares of the independent set $\{v_1, v_2, v_7, v_8\}$, appears in the r.h.s. of (4), while the random variables appearing in the l.h.s. of (4) correspond to the shares of circuits in the matroid.

Applying Theorem 14 and Theorem 15, we can generalize the above proof and prove that $\mathcal{V}_6$ cannot be close to ideal. That is, we can prove that in every secret-sharing scheme realizing $\mathcal{V}_6$, the size of the entropy of the share of at least one party is at least $(1+1/110)H(S)$. Using direct arguments, we prove that the size of the entropy of the share of at least one party is at least $(1 + 1/9)H(S)$. Before we formally state our result, we prove two lemmas. First, to aid us in proving the better lower bound, we rearrange Inequality (4):

Lemma 20. *For every four discrete random variables A, B, C, and D the following inequality holds:*

$$\begin{aligned} &3H(C|D) + 2H(C|B) + H(B|C) + H(A|C) \\ &\geq H(A|D) + 3H(C|BD) + H(BC|D) + H(C|AB). \end{aligned} \tag{6}$$

Proof. The claim is proved by a simple manipulation of (4). By (28), $3H(BCD) = 3H(C|BD) + 3H(BD)$ and $H(ABC) = H(C|AB) + H(AB)$. Substituting these expressions in (4) and rearranging the terms, we get

$$\begin{aligned} &3H(CD) + 3H(BC) + H(AC) \\ &\geq H(D) + 2[H(C) + H(B)] \\ &\quad + H(AD) + 3H(C|BD) + H(BCD) + H(C|AB). \end{aligned} \tag{7}$$

By (28), $2H(BC) = 2H(B) + 2H(C|B)$, $H(BC) = H(C) + H(B|C)$, and $H(AC) = H(C)+H(A|C)$. Substituting these expressions in (7) and rearranging the terms, we get

$$\begin{aligned} &3H(CD) + 2H(C|B) + H(B|C) + H(A|C) \\ &\geq H(D) + H(AD) + 3H(C|BD) + H(BCD) + H(C|AB). \end{aligned} \tag{8}$$

By (28), $3H(CD) = 3H(D) + 3H(C|D)$, $H(AD) = H(D) + H(A|D)$, and $H(BCD) = H(D) + H(BC|D)$. Substituting these expressions in (8) and rearranging the terms, we get (6). □

To prove our lower bounds, we need the following simple lemma whose proof can be found in [2]. For completeness we present its proof here. Informally, this lemma states that if a set T is unauthorized and $T \cup \{b\}$ is authorized for some participant b, then guessing b's share given the shares of T is at least as hard as guessing the secret. Otherwise, the unauthorized set T can guess the share of b, and via the share compute the secret. Since, by the privacy requirement, the unauthorized set T cannot have any information on the secret, the entropy of the share must be at least $H(S)$.

Lemma 21. *Let $T \subseteq V \setminus \{p_0\}$ and $b \notin T$ such that $T \cup \{b\} \in \mathcal{A}$ and $T \notin \mathcal{A}$. Then, $H(S_b|S_T) \geq H(S)$.*

Proof. By applying (33) twice,

$$H(S, S_b|S_T) = H(S_b|S_T) + H(S|S_b, S_T) = H(S|S_T) + H(S_b|S, S_T).$$

The proof is straightforward from the second equality by taking into account that $H(S|S_T) = H(S)$, $H(S|S_b, S_T) = 0$, and that the conditional entropy function is nonnegative. □

3.1 Proving the Lower Bound for $\mathcal{V}_6$

We next state and prove our main result.

Theorem 22. *In any secret-sharing scheme realizing $\mathcal{V}_6$ with respect to a distribution on the secrets denoted by a random variable S, the entropy of the shares of at least one party is at least $(1 + 1/9)H(S)$.*

Proof. We fix any scheme realizing $\mathcal{V}_6$ and define λ as

$$\lambda \stackrel{\text{def}}{=} \frac{\max_{1 \leq i \leq 8}(H(S_{v_i}))}{H(S)} - 1.$$

In particular, for $1 \leq i \leq 8$:

$$H(S_{v_i}) \leq (1 + \lambda)H(S). \tag{9}$$

Recall that $H(S_{v_6}) = H(S)$ as v_6 is the dealer. We use the same random variables A, B, C, and D as defined in (5). We will show that Lemma 20 implies that $\lambda \geq 1/9$.

We start with giving upper-bounds on the terms on the left hand side of (6). Recall that v_6 is the dealer, $C = S_{\{v_5,v_6\}}$, and $D = S_{\{v_7,v_8\}}$. Thus, since $\{v_5, v_7, v_8\}$ is authorized,

$$\begin{aligned} H(C|D) &= H(S_{v_5}|S_{v_7}, S_{v_8}) + H(S_{v_6}|S_{v_5}, S_{v_7}, S_{v_8}) \quad \text{(from (33))} \\ &\leq H(S_{v_5}) \leq (1 + \lambda)H(S). \end{aligned} \tag{10}$$

Similarly,

$$H(C|B) \leq (1 + \lambda)H(S). \tag{11}$$

Next, recall that $B = S_{\{v_3,v_4\}}$. By applying (29) and (33),

$$\begin{aligned} H(B|C) &= H(S_{v_4}|C) + H(S_{v_3}|S_{v_4}, S_{v_5}, S_{v_6}) \\ &\leq H(S_{v_4}) + H(S_{v_3}, S_{v_6}|S_{v_4}, S_{v_5}) - H(S_{v_6}|S_{v_4}, S_{v_5}) \\ &= H(S_{v_4}) + H(S_{v_3}|S_{v_4}, S_{v_5}) + H(S_{v_6}|S_{v_3}, S_{v_4}, S_{v_5}) - H(S_{v_6}|S_{v_4}, S_{v_5}). \end{aligned}$$

Therefore, since $\{v_3, v_4, v_5\}$ is authorized and $\{v_4, v_5\}$ is unauthorized,

$$H(B|C) \leq H(S_{v_4}) + H(S_{v_3}) - H(S) \leq (1 + 2\lambda)H(S).$$

Similarly,

$$H(A|C) \leq (1 + 2\lambda)H(S). \tag{12}$$

So, the l.h.s. of (6) is at most $(7 + 9\lambda)H(S)$.

We continue by giving lower-bounds on the terms in the right hand side of (6). First, by using (32) and (33),

$$\begin{aligned} H(A|D) &= H(S_{v_1}|D) + H(S_{v_2}|D, S_{v_1}) \\ &\geq H(S_{v_1}|D, S_{v_2}) + H(S_{v_2}|D, S_{v_1}) \\ &\geq 2H(S), \end{aligned} \tag{13}$$

where the last inequality is obtained from Lemma 21 as $\{v_1, v_2, v_7, v_8\}$ is a minimal authorized set. Second, from (33) and (2) as BD is unauthorized

$$H(C|BD) \geq H(S_{v_6}|BD) \geq H(S). \tag{14}$$

Third, by (33), (32), and Lemma 21,

$$\begin{aligned} H(BC|D) &= H(B|D) + H(C|BD) \\ &\geq H(S_{v_3}|D) + H(S) \\ &\geq H(S_{v_3}|D, S_{v_1}) + H(S). \end{aligned}$$

From Lemma 21 and the fact that $\{v_1, v_3, v_7, v_8\}$ is a minimal authorized set,

$$H(BC|D) \geq 2H(S).$$

Fourth, from (33) and (2) as AB is unauthorized,

$$H(C|AB) \geq H(S_{v_6}|AB) \geq H(S). \tag{15}$$

So, the r.h.s. of (6) is at least $8H(S)$.

To conclude, we have proved that the l.h.s. of (6) is at most $(7+9\lambda)H(S)$ and the r.h.s. of (6) is at least $8H(S)$. As the l.h.s. of (6) should be at least the r.h.s. of (6), we deduce that $(7 + 9\lambda)H(S) \geq 8H(S)$, which implies that $\lambda \geq 1/9$. □

By Remark 4, we can assume without loss of generality that the distribution on the secrets is uniform, that is, if the domain of secrets is K, then $H(S) = \log |K|$. Furthermore, by (27), if the domain of shares of v_i is K_i, then $H(S_{v_i}) \leq \log |K_i|$. Thus, we can reformulate Theorem 22 as follows.

Corollary 23. *In any secret-sharing scheme realizing $\mathcal{V}_6$ with respect to a distribution on the secrets with support K, the size of the domain of shares of at least one party is at least $|K|^{1+1/9}$.*

3.2 Proving the Lower Bound for $\mathcal{V}_8$

In a similar manner to the proof of the lower bound for $\mathcal{V}_6$, we prove a slightly weaker lower-bound for $\mathcal{V}_8$. As before, we begin by rearranging Inequality (4). The next lemma is proved similarly to Lemma 20.

Lemma 24. *For every four discrete random variables A, B, C, and D the following inequality holds:*

$$\begin{aligned} &3H(D|C) + 2H(D|B) + H(BD) + H(B|A) \\ &\geq H(D) + H(D|A) + H(B|C) + 4H(D|BC) + H(B|AC). \end{aligned} \tag{16}$$

Theorem 25. *In any secret-sharing scheme realizing $\mathcal{V}_8$ with respect to a distribution on the secrets denoted by a random variable S, the entropy of the shares of at least one party is at least $(1 + 1/10)H(S)$.*

Proof. We fix any scheme realizing $\mathcal{V}_8$ and we define λ as in the proof of Theorem 22. Then $H(S_{v_i}) \leq (1 + \lambda)H(S)$ for every $i = 1, \dots, 8$. Recall that $H(S_{v_8}) = H(S)$ as v_8 is the dealer. We use the same random variables A, B, C, and D as defined in (5). In a similar way as in Theorem 22, we find bounds on the terms of (16) to obtain a bound on λ.

Claim. $H(B|A) \leq (1 + 3\lambda)H(S)$.

To prove this claim, we first observe that

$$\begin{aligned} H(B|A) &= H(S_{v_3}, S_{v_4}|S_{v_1}, S_{v_2}) \\ &\leq H(S_{v_3}) + H(S_{v_4}|S_{v_1}, S_{v_2}, S_{v_3}) \\ &\leq (1 + \lambda)H(S) + H(S_{v_4}|S_{v_1}, S_{v_2}, S_{v_3}). \end{aligned} \tag{17}$$

We now bound $H(S_{v_4}|S_{\{v_1,v_2,v_3\}})$. By applying (33) twice,

$$\begin{aligned} H(S_{v_4}, S_{v_5}|S_{\{v_1,v_2,v_3\}}) &= H(S_{v_4}|S_{\{v_1,v_2,v_3\}}, S_{v_5}) + H(S_{v_5}|S_{\{v_1,v_2,v_3\}}) \\ &= H(S_{v_5}|S_{\{v_1,v_2,v_3\}}, S_{v_4}) + H(S_{v_4}|S_{\{v_1,v_2,v_3\}}). \end{aligned} \tag{18}$$

Thus, by (18)

$$\begin{aligned} H(S_{v_4}|S_{\{v_1,v_2,v_3\}}) = H(S_{v_4}|S_{\{v_1,v_2,v_3,v_5\}}) + H(S_{v_5}|S_{\{v_1.v_2,v_3\}}) \\ -H(S_{v_5}|S_{\{v_1.v_2,v_3,v_4\}}). \end{aligned} \tag{19}$$

We next bound each of the elements of the above sum, and get the desired result. First,

$$H(S_{v_5}|S_{\{v_1,v_2,v_3,v_4\}}) \leq H(S_{v_5}) \leq (1 + \lambda)H(S).$$

Second, from Lemma 21 we have

$$H(S_{v_5}|S_{\{v_1,v_2,v_3,v_4\}}) \geq H(S).$$

Next observe that $\{v_1, v_2, v_3, v_5\}$ is authorized in $\mathcal{V}_8$, and hence $H(S_{v_8}|S_{\{v_1,v_2,v_3,v_5\}}) = 0$, thus,

$$\begin{aligned}
H(S_{v_4}|S_{\{v_1,v_2,v_3,v_5\}}) &= H(S_{\{v_1,v_2,v_3,v_5\}}, S_{v_4}) - H(S_{\{v_1,v_2,v_3,v_5\}}) \\
&= H(S_{\{v_1,v_2,v_3,v_4,v_5\}}) \\
&\quad -[H(S_{v_8}|S_{\{v_1,v_2,v_3,v_5\}}) + H(S_{\{v_1,v_2,v_3,v_5\}})] \\
&= H(S_{\{v_1,v_2,v_3,v_4,v_5\}}) - H(S_{\{v_1,v_2,v_3,v_5,v_8\}}) \\
&\leq H(S_{\{v_1,v_2,v_3,v_4,v_5,v_8\}}) - H(S_{\{v_1,v_2,v_3,v_5,v_8\}}) \\
&= H(S_{v_4}|S_{\{v_1,v_2,v_3,v_5,v_8\}}) \\
&\leq H(S_{v_4}|S_{\{v_1,v_2,v_5,v_8\}}) \\
&= H(S_{v_4}S_{v_8}|S_{\{v_1,v_2,v_5\}}) - H(S_{v_8}|S_{\{v_1,v_2,v_5\}}) \\
&= [H(S_{v_4}|S_{\{v_1,v_2,v_5\}}) + H(S_{v_8}|S_{\{v_1,v_2,v_4,v_5\}})] \\
&\quad -H(S_{v_8}|S_{\{v_1,v_2,v_5\}}) \\
&\leq H(S_{v_4}) + 0 - H(S) \\
&\leq \lambda H(S). \qquad (20)
\end{aligned}$$

In the last steps we used that $\{v_1, v_2, v_4, v_5\}$ is a minimal authorized subset. Now, by summing up the bounds,

$$H(S_{v_4}|S_{\{v_1,v_2,v_3\}}) \leq \lambda H(S) + (1+\lambda)H(S) - H(S) \ = \ 2\lambda H(S). \qquad (21)$$

Thus, by (17) and (21), $H(B|A) \leq (1 + 3\lambda)H(S)$, which concludes the proof of our claim.

Since $\{v_5, v_6, v_7\}$ is an authorized set,

$$\begin{aligned}
H(D) - H(D|C) &= (H(S_{v_7}) + H(S_{v_8}|S_{v_7})) \\
&\quad -(H(S_{v_7}|S_{\{v_5,v_6\}}) + H(S_{v_8}|S_{\{v_5,v_6,v_7\}})) \\
&= H(S_{v_7}) + H(S) - H(S_{v_7}|S_{\{v_5,v_6\}}) - 0 \\
&\geq H(S). \qquad (22)
\end{aligned}$$

Thus, by (16) and (22),

$$\begin{aligned}
&2H(D|C) + 2H(D|B) + H(BD) + H(B|A) \\
&\geq H(D|A) + H(B|C) + 4H(D|BC) + H(B|AC) + H(S). \qquad (23)
\end{aligned}$$

We next give upper bounds for the terms in the l.h.s. of (23). We proved before that $H(B|A) \leq (1 + 3\lambda)H(S)$. For the rest of the terms in the l.h.s. we use straightforward bounds. First,

$$H(D|C) = H(S_{v_7}S_{v_8}|C) \leq H(S_{v_8}|S_{v_7}C) + H(S_{v_7}) \leq (1+\lambda)H(S)$$

because $\{v_5, v_6, v_7\}$ is authorized, and similarly $H(D|B) \leq (1 + \lambda)H(S)$. Second, $H(BD) = H(S_{\{v_3,v_4,v_7,v_8\}}) = H(S_{v_8}|S_{\{v_3,v_4,v_7\}}) + H(S_{\{v_3,v_4,v_7\}}) \leq 3(1 + \lambda)H(S)$, since $\{v_3, v_4, v_7\}$ is authorized. Thus, the l.h.s. of (23) is less than $(8 + 10\lambda)H(S)$.

We continue by giving lower bounds for the terms in the r.h.s. of (23). First, by Lemma 21,

$$H(D|A) = H(S_{v_8}|S_{\{v_1,v_2,v_7\}}) + H(S_{v_7}|S_{\{v_1,v_2\}}) \geq 2H(S),$$

since $\{v_1, v_2, v_7\}$ is unauthorized and $\{v_1, v_2, v_5, v_7\}$ is authorized. Second,

$$H(B|C) \geq H(B|AC) \geq H(S) \tag{24}$$

since $\{v_1, v_2, v_5, v_6\}$ is unauthorized and $\{v_1, v_2, v_3, v_4, v_5, v_6\}$ is authorized. Next, $H(D|BC) \geq H(S)$ since the set $\{v_3, v_4, v_5, v_6\}$ is unauthorized, while $\{v_7, v_8\}$ contains the dealer v_8. Finally, $H(B|AC) \geq H(S)$ by (24). Thus, we conclude that the r.h.s. of (23) is at least $9H(S)$.

Finally, the bounds we obtained for both sides of Inequality (23) imply that $\lambda \geq 1/10$. □

Corollary 26. *In any secret-sharing scheme realizing $\mathcal{V}_8$ with respect to a distribution on the secret with support K, the size of the domain of shares of at least one party is at least $|K|^{1+1/10}$.*

3.3 Lower Bounds for Linear Secret-Sharing Schemes

In the following, we present a lower bound for the size of the shares' domain that applies only to *linear* secret-sharing schemes with access structure $\mathcal{V}_6$ or $\mathcal{V}_8$. Nearly all known secret-sharing schemes are linear. A secret-sharing scheme is linear if the distribution scheme is such that the domain of secrets K, the domain of random strings R, and the domains of shares of the i-th party K_i, for every i, are vector spaces over some finite field, Π is a linear mapping, and the distribution on random strings μ is uniform. This bound is obtained in a very similar way as the previous ones by using an inequality due to Ingleton [17], which applies only to linear random variables, that is, random variables defined by linear mappings.

Theorem 27 ([17, 28]). *For every four* linear *discrete random variables A, B, C, and D the following inequality holds:*

$$\begin{aligned} &H(CD) + H(BD) + H(BC) + H(AC) + H(AB) \\ &\geq H(C) + H(B) + H(AD) + H(BCD) + H(ABC). \end{aligned} \tag{25}$$

The proof of the next lemma is very similar to the one of Lemma 20.

Lemma 28. *For every four linear discrete random variables A, B, C, and D the following inequality holds:*

$$\begin{aligned} &H(C|D) + H(C|B) + H(A|C) \\ &\geq H(A|D) + H(C|BD) + H(C|AB). \end{aligned} \tag{26}$$

The following result is proved in a similar way to the proof of Theorem 22.

Theorem 29. *In any* linear *secret-sharing scheme realizing* $\mathcal{V}_6$ *with respect to a distribution on the secrets denoted by a random variable* S*, the entropy of the shares of at least one party is at least* $(1 + 1/4)H(S)$*.*

Proof. We fix any *linear* scheme realizing $\mathcal{V}_6$ and define

$$\lambda \stackrel{\text{def}}{=} \max_{1 \leq i \leq 8} (H(S_{v_i}))/H(S) - 1.$$

We use the same random variables A, B, C, and D as defined in (5). Note that all bounds proved in Section 3.1 apply, in particular, to linear secret-sharing realizing $\mathcal{V}_6$. Thus, by (10), (11), and (12), the l.h.s. of (26) is at most $(3 + 4\lambda)H(S)$. By (13), (14), and (15), the r.h.s. of (26) is at least $4H(S)$. This implies that $(3 + 4\lambda)H(S) \geq 4H(S)$, which implies that $\lambda \geq 1/4$.

Corollary 30. *In any linear secret-sharing scheme realizing* $\mathcal{V}_6$ *with respect to a distribution on the secrets with support* K*, the size of the domain of shares of at least one party is at least* $|K|^{1+1/4}$*.*

Finally, the same bound applies to the linear secret-sharing schemes with access structure $\mathcal{V}_8$ by duality. The *dual* of an access structure $\mathcal{A}$ is the access structure

$$\mathcal{A}^* \stackrel{\text{def}}{=} \{T \subseteq P \,:\, P \setminus T \notin \mathcal{A}\}.$$

It is well known that, for every linear secret-sharing scheme Σ with access structure $\mathcal{A}$, there exists a linear secret sharing scheme Σ^* for $\mathcal{A}^*$ such that the domain of the shares of every participant is the same for Σ and for Σ^* (see [14], for instance). Therefore, since $\mathcal{V}_8^*$ is isomorphic to $\mathcal{V}_6$, the bounds in Theorem 29 and Corollary 30 apply also to the access structure $\mathcal{V}_8$.

References

1. A. Beimel and B. Chor. Universally ideal secret sharing schemes. *IEEE Trans. on Information Theory*, 40(3):786–794, 1994.
2. A. Beimel and N. Livne. On matroids and non-ideal secret sharing. In S. Halevi and T. Rabin, editors, *Proc. of the Third Theory of Cryptography Conference – TCC 2006*, volume 3876 of *LNCS*, pages 482–501, 2006.
3. M. Bellare and P. Rogaway. Robust computational secret sharing and a unified account of classical secret-sharing goals. In Proc. of the 14th conference on Computer and communications security, pages 172–184, 2007.
4. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology – CRYPTO '88*, volume 403 of *LNCS*, pages 27–35. 1990.
5. G. R. Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, pages 313–317. 1979.
6. C. Blundo, A. De Santis, and U. Vaccaro. On secret sharing schemes. *Inform. Process. Lett.*, 65(1):25–32, 1998.
7. E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.

8. E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.
9. E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. of Cryptology*, 5(3):153–166, 1992.
10. R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. of Cryptology*, 6(3):157–168, 1993.
11. B. Chor and E. Kushilevitz. Secret sharing over infinite domains. *J. of Cryptology*, 6(2):87–96, 1993.
12. T. M. Cover and J. A. Thomas. *Elements of Information Theory.* John Wiley & Sons, 1991.
13. L. Csirmaz. The size of a share must be large. *J. of Cryptology*, 10(4):223–231, 1997.
14. M. van Dijk, W.A. Jackson, and K. M. Martin. A note on duality in linear secret sharing schemes. *Bull. of the Institute of Combinatorics and its Applications*, 19:98–101, 1997.
15. R. Dougherty, C. Freiling, and K. Zeger. Six new non-Shannon information inequalities. In *IEEE International Symposium on Information Theory (ISIT)*, pages 233–236, 2006.
16. R. Dougherty, C. Freiling, and K. Zeger. Networks, matroids, and non-Shannon information inequalities. *IEEE Trans. on Information Theory*, 53(6):1949–1969, 2007.
17. A. W. Ingleton. Conditions for representability and transversability of matroids. In *Proc. Fr. Br. Conf 1970*, pages 62–67. Springer-Verlag, 1971.
18. M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of the IEEE Global Telecommunication Conf., Globecom 87*, pages 99–102, 1987.
19. M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102–111, 1993.
20. E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.
21. K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii. Nonperfect secret sharing schemes and matroids. In *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *LNCS*, pages 126–141. 1994.
22. N. Livne. On matroids and non-ideal secret sharing. Master's thesis, Ben-Gurion University, Beer-Sheva, 2005.
23. J. Martí-Farré and C. Padró. Secret sharing schemes with three or four minimal qualified subsets. *Designs, Codes and Cryptography*, 34(1):17–34, 2005.
24. J. Martí-Farré and C. Padró. On secret sharing schemes, matroids and polymatroids. In S. Vadhan, editor, *Proc. of the Fourth Theory of Cryptography Conference – TCC 2007*, volume 4392 of *LNCS*, pages 253–272. 2007.
25. J. Martí-Farré and C. Padró. On secret sharing schemes, matroids and polymatroids. Journal version of [24]. Technical Report 2006/077, Cryptology ePrint Archive, 2006. `http://eprint.iacr.org/`.
26. F. Matúš. Matroid representations by partitions. *Discrete Mathematics*, 203:169–194, 1999.
27. F. Matúš. Two constructions on limits of entropy functions. *IEEE Trans. on Information Theory*, 53(1):320–330, 2007.
28. J. G. Oxley. *Matroid Theory.* Oxford University Press, 1992.
29. P. D. Seymour. A forbidden minor characterization of matroid ports. *Quart. J. Math. Oxford Ser.*, 27:407–413, 1976.

30. P. D. Seymour. On secret-sharing matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.
31. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
32. G. J. Simmons, W. Jackson, and K. M. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.
33. J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179–197, 1998.
34. P. Vamos. On the representation of independence structures. Unpublished manuscript, 1968.
35. D. J. A. Welsh. *Matroid Theory.* Academic press, London, 1976.
36. Z. Zhang and R. W. Yeung. On characterization of entropy function via information inequalities. *IEEE Trans. on Information Theory*, 44(4):1440–1452, 1998.

A Basic Definitions from Information Theory

In this appendix, we review the basic concepts of information theory used in this paper. For a complete treatment of this subject see, e.g., [12]. All the logarithms here are of base 2.

Given a finite random variable X, we define the *entropy* of X, denoted $H(X)$, as

$$H(X) \stackrel{\text{def}}{=} -\sum_{x,\Pr[X=x]>0} \Pr[X=x]\log\Pr[X=x].$$

It can be proved that

$$0 \le H(X) \le \log|\operatorname{supp}(X)|, \tag{27}$$

where $|\operatorname{supp}(X)|$ is the size of the support of X (the number of values with probability greater than zero). The upper bound is obtained if and only if the distribution of X is uniform.

Given two finite random variables X and Y (possibly dependent), we define the *conditioned entropy of X given Y* as

$$H(X|Y) \stackrel{\text{def}}{=} H(XY) - H(Y). \tag{28}$$

For convenience, when dealing with the entropy function, XY will denote $X \cup Y$. From the definition of the conditional entropy, the following properties can be proved:

$$0 \le H(X|Y) \le H(X), \tag{29}$$

$$H(Y) \le H(XY), \tag{30}$$

and

$$H(XY) \le H(X) + H(Y). \tag{31}$$

Given three finite random variable X, Y and Z (possibly dependent), the following properties hold:

$$H(X|Y) \ge H(X|YZ), \tag{32}$$

$$H(XY|Z) = H(X|YZ) + H(Y|Z) \ge H(Y|Z), \tag{33}$$

and

$$H(XY|Z) \le H(X|Z) + H(Y|Z). \tag{34}$$