On Matroids and Non-ideal Secret Sharing

Amos Beimel* and Noam Livne

Dept. of Computer Science, Ben-Gurion University, Beer-Sheva 84105, Israel.

Abstract. Secret-sharing schemes are a tool used in many cryptographic protocols. In these schemes, a dealer holding a secret string distributes shares to the parties such that only authorized subsets of participants can reconstruct the secret from their shares. The collection of authorized sets is called an access structure. An access structure is *ideal* if there is a secret-sharing scheme realizing it such that the shares are taken from the same domain as the secrets. Brickell and Davenport (J. of Cryptology, 1991) have shown that ideal access structures are closely related to matroids. They give a necessary condition for an access structure to be ideal – the access structure must be induced by a matroid. Seymour (J. of Combinatorial Theory B, 1992) showed that the necessary condition is not sufficient: There exists an access structure induced by a matroid that does not have an ideal scheme.
In this work we continue the research on access structures induced by matroids. Our main result in this paper is strengthening the result of Seymour. We show that in any secret sharing scheme realizing the access structure induced by the Vamos matroid with domain of the secrets of size k, the size of the domain of the shares is at least $k + \Omega(\sqrt{k})$. Our second result considers non-ideal secret sharing schemes realizing access structures induced by matroids. We prove that the fact that an access structure is induced by a matroid implies lower and upper bounds on the size of the domain of shares of subsets of participants even in non-ideal schemes (this generalized results of Brickell and Davenport for ideal schemes).

1 Introduction

Secret sharing schemes are a tool used in many cryptographic protocols. A secret sharing scheme involves a dealer who has a secret, a finite set of n participants, and a collection $\mathcal{A}$ of subsets of the set of participants called the access structure. A secret-sharing scheme for $\mathcal{A}$ is a method by which the dealer distributes shares 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. A secret sharing scheme can only exist for monotone access structures, i.e. if a subset A can reconstruct the secret, then every superset of A can also reconstruct the secret. Given any monotone

* Partially supported by the David and Lucile Packard Foundation grant of Matthew Franklin, and by the Frankel Center for Computer Science.

access structure, Ito, Saito, and Nishizeki [22] show how to build a secret sharing scheme that realizes the access structure. Even with more efficient schemes presented since, e.g. in [5, 41, 10, 25, 44, 21], most access structures require shares of exponential size: if the domain of the secrets is binary, the shares are strings of length $2^{\Theta(n)}$, where n is the number of participants

Certain access structures give rise to very economical secret sharing schemes. A secret sharing scheme is called *ideal* if the shares are taken from the same domain as the secrets. For example, Shamir's threshold secret sharing scheme [40] is ideal. An access structure is called ideal if there is an ideal secret sharing scheme which realizes the access structure over some finite domain of secrets. Ideal access structures are interesting for a few reasons: (1) they are the most efficient secret sharing schemes as proved by [26], (2) they are most suitable for composition of secret sharing schemes, and (3) they have interesting combinatorial structure, namely, they have a matroidial structure, as proved by [11] and discussed in the next paragraph.

Brickell and Davenport [11] have shown that ideal access structures are closely related to matroids over a set containing the participants and the dealer. They give a necessary condition for an access structure to be ideal – the access structure must be induced by a matroid – and a somewhat stronger sufficient condition – the matroid should be representable over some finite field. The question of an exact characterization of ideal access structures is still open. Seymour [39] has shown that the necessary condition is not sufficient: there exists an access structure induced by a matroid that does not have an ideal scheme. The following natural open question arises: How far from ideal can access structures induced by matroids be? Is there an upper-bound on the shares' size implied by being an access structure induced by a matroid? There is no better known upper bound on the share size than the $2^{O(n)}$ bound for general access structures. Most known secret sharing schemes are linear (see discussion in [2]). On one hand, the number of linear schemes with n participants, binary domain of secrets, and shares of size $\mathrm{poly}(n)$ is $2^{\mathrm{poly}(n)}$. On the other hand, the number of matroids with n points is $\exp(2^{\Theta(n)})$ (see [47]) and every matroid induces at least one access structure. Thus, for most access structures induced by matroids, the size of the shares in linear secret-sharing schemes is super-polynomial. This gives some evidence that access structures induced by matroids do not have efficient secret sharing schemes for a reasonable size of domain of secrets.

Our Results. In this work we continue the research on access structures induced by matroids. Seymour [39] showed that any access structure induced by the Vamos matroid [46] is not ideal. Our main result is strengthening this result. We consider an access structure induced by the Vamos matroid and show that in any secret sharing scheme realizing this access structure with domain of the secret of size k, the size of the domain of the shares is at least $k + \Omega(\sqrt{k})$ (compared to the lower bound of $k+1$ implied by [39]). Towards proving this lower bound, we needed to strengthen some results of [11] to non-ideal secret sharing schemes realizing access structures induced by matroids. We then needed to generalize Seymour's ideas to obtain our lower bound. We note that the upper-bound on the size of the domain of shares in a secret sharing scheme realizing the access structure induced by the Vamos matroid is poly(k), thus our work still leaves open the question of the minimal-size share domain for this access structure.

Brickell and Davenport [11] proved that the size of the domain of shares of a subset of participants in an ideal scheme is exactly determined by the size of the domain of secrets and the rank of the subset in the matroid inducing the access structure. We consider non-ideal secret sharing schemes realizing access structures induced by matroids. We prove that the fact that an access structure is induced by a matroid implies lower and upper bounds on the size of the domain of shares of subsets of participants even in non-ideal schemes. These lower and upper bounds, beside being interesting for their own, are used to prove our main result. We need both the lower bounds and the upper bounds to prove our main result – the lower bound on the size of the domain of shares in the Vamos matroid.

We prove two incomparable versions of such bounds. The first version, in Section 3, contains somewhat weaker bounds; however, this is the version we can use in the proof of our main result. The second version, in Section 5, contains bounds on the entropy of shares of subsets of participants. Entropy arguments have been used to give bounds on the size of shares in secret sharing schemes starting with [26, 12]. Specifically, entropy arguments have been used for ideal secret sharing schemes in [27]. We were not able to use the bounds we proved via entropy in the proof of our main result for technical reasons. We include them in this paper since we believe that they are interesting for their own sake. Furthermore, they might be useful in proving stronger bounds than the lower bound proved here, either for the matroid induced by the Vamos matroid, or for access structures induced by other matroids. See discussion in Example 4 at the end of this paper.

Historical Background. Secret sharing schemes were introduced by Blakley [6] and Shamir [40] for the threshold case, that is, for the case where the subsets that can reconstruct the secret are all the sets whose cardinality is at least a certain threshold. Secret sharing schemes for general access structures were introduced by Ito, Saito, and Nishizeki in [22]. More efficient schemes were presented in, e.g., [5, 41, 10, 25, 44, 21]. Originally motivated by the problem of secure information storage, secret-sharing schemes have found numerous other applications in cryptography and distributed computing, e.g., Byzantine agreement [38], secure multiparty computations [4, 13, 15], threshold cryptography [19], and access control [33].

Several lower bounds on the share size of secret-sharing schemes were obtained [5, 12, 7, 20, 18, 17]. The strongest current bound is $\Omega(n^2/\log n)$ [17] for the total size of the shares of all the participants, where n is the number of participants in the system. However, there is a huge gap between these lower bounds and the best known upper bounds of $2^{O(n)}$ for general access structures. The question of super-polynomial lower bounds on the size of shares for some (explicit or random) access structures is still open.

Ideal secret sharing schemes and ideal access structures have been first considered in [10] and have been studied extensively thereafter, e.g. in [1, 3, 8, 11, 23, 24, 27, 29–32, 34, 35, 37, 42, 43, 45, 16]. There are two common definitions for ideal access structures in the secret sharing literature. The first, that will also be used here, can be found implicitly in [11] and explicitly in [31, 1, 34, 35, 3]. The second can be found in [29, 30, 32]. Livne [28] pointed that these definitions are not necessarily equivalent. Furthermore, he proposed a candidate access structure that is ideal according to one definition but possibly is not ideal according to the stronger definition.

Organization. In Section 2 we present basic definitions of secret sharing schemes and matroids, and discuss the relation between them. In Section 3 we prove some technical lemmas concerning weak secret sharing schemes; these lemmas are used to prove our main result. In Section 4 we prove a lower bound on the size of shares in any secret sharing realizing the access structure induced by the Vamos matroid. Finally, in Section 5 we prove upper and lower bounds on the entropy of shares of subsets of participants in secret sharing schemes realizing matroid induced access structures. In Appendix A we supply some background results on the entropy function.

2 Preliminaries

In this section we define weak secret sharing schemes, review some background on matroids, and discuss the connection between secret sharing schemes and matroids.

Definition 1 (Access Structure). *Let P be a finite set of participants. A collection $\mathcal{A} \subseteq 2^P$ is* monotone *if $B \in \mathcal{A}$ and $B \subseteq C \subseteq P$ 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. *A set B is called a* minterm *of $\mathcal{A}$ if $B \in \mathcal{A}$ and for every $C \subsetneq B$, the set C is unauthorized. A participant is called* redundant *if there is no minterm that contains it. An access structure is called* connected *if it has no redundant participants.*

In this section we only give a relaxed definition of secret sharing scheme, which we call a *weak secret sharing scheme*. The formal definition of (strong) secret sharing scheme appears in Section 5. While in the definition of secret sharing schemes it is required that the uncertainty of the secret given the shares of an unauthorized subset of participants is the same as the a-priory uncertainty of the secret (in the information theoretic sense), here we require merely that no value of the secret could be ruled out, i.e. that each value of the secret has probability greater than zero. In particular, every secret sharing scheme is a weak secret sharing scheme. Thus, in the proof of our main result we prove lower bounds on the size of shares in weak secret sharing schemes.

Definition 2 (Weak Secret-Sharing Scheme and Weakly Ideal Access Structure). *Let P be a set of participants, and let K be a finite set of secrets.*

A weak secret sharing scheme *with domain of secrets* K *is a matrix* M *whose columns are indexed by* $P \cup \{p_0\}$*, where* $p_0 \notin P$*, and with all entries in column* p_0 *from* K*. When the dealer wants to distribute a secret* $s \in K$*, it chooses a row* $r \in M$ *such that* $M_{r,p_0} = s$*, and privately communicates to each participant* $p \in P$ *the value* $M_{r,p}$*. We refer to* $M_{r,p}$ *as the* share *of participant* p*. Given a vector of shares* $\mathbf{K_A}$*, denote by* $K(p_0|\mathbf{K_A})$ *the possible values of the secret given that the participants in* A *receive the vector of shares* $\mathbf{K_A}$*.*

We say that M realizes *a weak secret sharing scheme for the access structure* $\mathcal{A} \subseteq 2^P$ *if the following two requirements hold:*

- CORRECTNESS. *The secret can be reconstructed by any authorized set of participants:* $|K(p_0|\mathbf{K_A})| = 1$ *for any* $A \in \mathcal{A}$ *and every possible vector of shares* $\mathbf{K_A}$ *for the set* A*.*
- WEAK PRIVACY. *Given a vector of shares of an unauthorized set of participants, none of the values of the secret can be ruled out:* $K(p_0|\mathbf{K_A}) = K$ *for any* $A \notin \mathcal{A}$ *and every possible vector of shares* $\mathbf{K_A}$ *for the set* A*.*

If an access structure has a weak secret sharing scheme with shares' domain of every participant equal to the domain of the secret for some finite domain of secrets, we say that the access structure is weakly ideal*.*

Example 1. As an example, consider Shamir's threshold scheme [40]. Denote $P = \{1, \ldots, n\}$, let $t \leq n$, and define the threshold access structure $\mathcal{A}_t = \{A \subseteq P : |A| \geq t\}$. We choose some prime number $q \geq n$, and define a secret sharing scheme with domain of secrets of size q as follows. In order to distribute a secret $s \in \{0, \ldots, q-1\}$, the dealer randomly chooses, with uniform distribution, a polynomial p of degree $t-1$ over $\mathrm{GF}(q)$ such that $p(0) = s$. The dealer then distributes to each participant $p_i \in P$ the share $p(i)$. When an authorized subset of participants (of size at least t) wants to reconstruct the secret, it has at least t distinct points of the polynomial p, therefore it can determine p, and it can calculate $p(0)$. An unauthorized subset cannot eliminate any value of the secret. In this scheme, the matrix M contains q^t rows; a row $\langle p(0), p(1), \ldots, p(n) \rangle$ for every polynomial p of degree $t-1$ over $\mathrm{GF}(q)$.

We next give some notations concerning weak secret sharing schemes. Given $A, B \subseteq P \cup \{p_0\}$ and $\mathbf{K_B} \in K(B)$, denote by $K(A|\mathbf{K_B})$ the set of combinations of shares the participants in A can receive given that the participants in B received the vector of shares $\mathbf{K_B}$. That is, if M' is the restriction of M to the rows such that the values in the columns in B are $\mathbf{K_B}$, then $K(A|\mathbf{K_B})$ is the set of the distinct rows in the restriction of M' to the columns in A. Given $\mathbf{K_A} \in K(A|\mathbf{K_B})$, we say that $\mathbf{K_A}$ *coincides* with $\mathbf{K_B}$ (that is, there is a row in M that gives to the participants in A the shares in $\mathbf{K_A}$ and to the participants in B the shares in $\mathbf{K_B}$). Of course, this relation is symmetric. We denote $K(\{v_{i_1}, v_{i_2}, \ldots, v_{i_\ell}\})$ by $K(v_{i_1}, v_{i_2}, \ldots, v_{i_\ell})$. Given sets of participants $A, B_1, \ldots, B_\ell \subseteq V$, and vectors of shares $\mathbf{K_{B_i}} \in K(B_i)$ for $1 \leq i \leq \ell$, we also denote $K(A|\mathbf{K_{B_1}}, \ldots, \mathbf{K_{B_\ell}})$ as the set of vectors of shares the (ordered) set of participants A can receive given that the participants of B_i received the shares $\mathbf{K_{B_i}}$ for $1 \le i \le \ell$. Given two sets of participants $A, B \subseteq V$, and a set $X_B \subseteq K(B)$ we denote $K(A|X_B) \stackrel{\text{def}}{=} \bigcup_{\mathbf{K_B} \in X_B} K(A|\mathbf{K_B})$.

2.1 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 [47, 36].

Definition 3 (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 $X \not\subseteq Y$.* (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 graph and $\mathcal{C}$ be the collection of simple cycles in G. Then, $(E, \mathcal{C})$ is a matroid.

Definition 4. *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 $A \subseteq V$, denoted* $\mathrm{rank}(A)$*, is the size of a maximal independent subset of A. A matroid is* connected *if for every pair of elements x, y there is a circuit containing x and y.*

The following lemma shows that a stronger statement than (C2) can be made about the circuits of a matroid. Its proof can be found, e.g., in [47, 36].

Lemma 1. *If C_1, C_2 are distinct members of $\mathcal{C}$ and $x \in C_1 \cap C_2$, then for any element $y \in C_1 \vartriangle C_2$ there exists $C_3 \in \mathcal{C}$ such that $y \in C_3$ and $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$.*

The following lemma, whose proof can be found in [47, 36], states that if a matroid is connected then the set of circuits through a fixed point uniquely determines the matroid.

Lemma 2. *Let e be an element of a connected matroid $\mathcal{M}$ and let $\mathcal{C}_e$ be the set of circuits of $\mathcal{M}$ that contain e. For $C_1, C_2 \in \mathcal{C}_e$ define:*

$$I_e(C_1, C_2) \stackrel{def}{=} \bigcap \{C_3 : C_3 \in \mathcal{C}_e, C_3 \subseteq C_1 \cup C_2\}$$

and

$$D_e(C_1, C_2) \stackrel{def}{=} (C_1 \cup C_2) \setminus I_e(C_1, C_2).$$

Then, all *of the circuits of $\mathcal{M}$ that do not contain e are the* minimal *sets of the form $D_e(C_1, C_2)$ where C_1 and C_2 are distinct circuits in $\mathcal{C}_e$.*

2.2 Matroids and Secret Sharing

We next define the access structures induced by matroids. This definition is used to give a necessary condition for ideal access structures.

Definition 5. *Let $\mathcal{M} = \langle V, \mathcal{C} \rangle$ be a 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 $P = V \setminus \{p_0\}$, where*

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

That is, a set is a minterm 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 *from $\mathcal{M}$, 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 $\mathcal{A}$.*

If a connected access structure has an appropriate matroid, then this matroid is also connected. Thus, by Lemma 2, if a connected access structure has an appropriate matroid, then this matroid is unique. Of course, not every access structure has an appropriate matroid.

We now quote some results concerning weak secret sharing schemes. Since every secret sharing scheme is, in particular, a weak secret sharing scheme, these results hold for the regular case as well. The following fundamental result, which is proved in [11], connects matroids and secret sharing schemes.

Theorem 1 ([11]). *If an access structure is weakly ideal, then it has an appropriate matroid.*

The following result, which is implicit in [11], shows the connection between the rank function of the appropriate matroid and the size of the domain of shares of sets of participants.

Lemma 3 ([11]). *Assume that the access structure $\mathcal{A} \subseteq 2^P$ is weakly ideal, and let $\langle P \cup \{p_0\}, \mathcal{C} \rangle$ be its appropriate matroid where $p_0 \notin P$. Let M be an ideal weak secret sharing scheme realizing $\mathcal{A}$ with domain of secrets (and shares) K. Then $|K(X)| = |K|^{\mathrm{rank}(X)}$ for any $X \subseteq P \cup \{p_0\}$, where* $\mathrm{rank}(X)$ *is the rank of X in the matroid.*

Remark 1. A corollary of Lemma 3 is that M can realize a secret sharing scheme for *any* access structure induced from $\mathcal{M}$ (i.e., with every element set as the dealer).

Example 2. Consider the threshold access structure $\mathcal{A}_t$ and Shamir's scheme [40] realizing it (see Example 1). The appropriate matroid of $\mathcal{A}_t$ is the matroid with $n+1$ points, whose circuits are the sets of size $t+1$ and $\mathrm{rank}(X) = \min\{|X|, t\}$. Since every t points determine a unique polynomial of degree $t-1$, in Shamir's scheme $|K(X)| = |K|^{\min\{|X|,t\}}$, as implied by Lemma 3.

3 Secret Sharing Schemes Realizing Matroid-Induced Access Structures

We now prove some lemmas concerning weak secret sharing schemes and matroid-induced access structures with arbitrary size of shares domain. The next lemma gives a lower bound on the size of the shares of certain subsets of participants. This lemma holds for every access structure.

Lemma 4. *Let $\mathcal{A} \subseteq 2^P$ be an access structure, $A, B \subseteq P$, and $b \in B \setminus A$ such that $A \cup B \in \mathcal{A}$ and $A \cup B \setminus \{b\} \notin \mathcal{A}$. Denote the dealer p_0 and define $K \stackrel{def}{=} K(p_0)$ (that is, K is the domain of secrets). Then, $|K(b|\mathbf{K_A})| \geq |K|$ for any $\mathbf{K_A} \in K(A)$.*

Proof. Since $A \cup B \setminus \{b\} \notin \mathcal{A}$, by the privacy requirement, for any $\mathbf{K_{A \cup B \setminus \{b\}}} \in K(A \cup B \setminus \{b\})$,

$$K(p_0|\mathbf{K_{A \cup B \setminus \{b\}}}) = K. \tag{1}$$

Since $A \cup B$ is authorized, by the correctness requirement, for any $\mathbf{K_{A \cup B}} \in K(A \cup B)$,

$$|K(p_0|\mathbf{K_{A \cup B}})| = 1. \tag{2}$$

Furthermore, $K(p_0|\mathbf{K_{A \cup B \setminus \{b\}}}) = \bigcup_{\mathbf{K_b} \in K(b|\mathbf{K_{A \cup B \setminus \{b\}}})} K(p_0|\mathbf{K_{A \cup B \setminus \{b\}}}, \mathbf{K_b})$ for any $\mathbf{K_{A \cup B \setminus \{b\}}} \in K(A \cup B \setminus \{b\})$. Since, by (2), every set in this union is of size one, and since, by (1), the size of the union is $|K|$, there are at least $|K|$ sets in the union. Hence $|K(b|\mathbf{K_{A \cup B \setminus \{b\}}})| \geq |K|$. Define $\mathbf{K_A}$ as the restrictions of the vector $\mathbf{K_{A \cup B \setminus \{b\}}}$ to the set A. Since $K(b|\mathbf{K_{A \cup B \setminus \{b\}}}) \subseteq K(b|\mathbf{K_A})$, the lemma follows. □

Lemma 5. *Let $\mathcal{M} = \langle P \cup \{p_0\}, \mathcal{C} \rangle$ be the appropriate matroid of an access structure $\mathcal{A} \subseteq 2^P$, and let $C \in \mathcal{C}$ such that $p_0 \in C$. Let $A \subseteq P \cup \{p_0\}$ and $D \subseteq P$ such that $A \cap D = \emptyset$. If $A \cup D \subsetneq C$, then $|K(A|\mathbf{K_D})| \geq |K|^{|A|}$ for every $\mathbf{K_D} \in K(D)$.*

Proof. We will prove the lemma by induction on $|A|$. If $|A| = 0$, the claim is trivial. For the induction step, let $a \in A$. Since $A \cup D \subsetneq C$, we have $A \cup D \setminus \{a\} \subsetneq C$. By the induction hypothesis, $|K(A \setminus \{a\} |\mathbf{K_D})| \geq |K|^{|A|-1}$. Therefore, it is sufficient to prove that $|K(A|\mathbf{K_D})| \geq |K||K(A \setminus \{a\} |\mathbf{K_D})|$ for some $a \in A$. If $p_0 \in A$, then we choose $a = p_0$. Note that $A \cup D \setminus \{p_0\}$ is unauthorized. If this is not the case, then $A \cup D$ contains a circuit C_0 which contains p_0. But since $A \cup D$ is properly contained in C, it follows that C_0 is properly contained in C, a contradiction to Axiom (C1) of the matroids. Now since $A \cup D \setminus \{p_0\}$ is unauthorized, by the privacy requirement, $|K(p_0|\mathbf{K_{A \setminus \{p_0\}}}, \mathbf{K_D})| = |K|$ for any $\mathbf{K_{A \setminus \{p_0\}}} \in K(A \setminus \{p_0\})$. Therefore, $|K(A|\mathbf{K_D})| = |K||K(A \setminus \{a\} |\mathbf{K_D})|$, which concludes this case.

If $p_0 \notin A$, then we choose an arbitrary $a \in A$. Now $A \cup D \setminus \{a\}$ is unauthorized. Otherwise $(A \cup D \setminus \{a\}) \cup \{p_0\}$ contains a circuit C_0 which contains p_0. But since $A \cup D$ is properly contained in C, it follows that C_0 is properly contained in C, a contradiction. Moreover, $A \cup D \subseteq C \setminus \{p_0\}$, and $C \setminus \{p_0\}$ is authorized. Therefore, by Lemma 4, $|K(a|\mathbf{K}_{\mathbf{A}\setminus\{\mathbf{a}\}}, \mathbf{K}_{\mathbf{D}})| \geq |K|$ for any $\mathbf{K}_{\mathbf{A}\setminus\{\mathbf{a}\}} \in K(A \setminus \{a\})$. It follows that $|K(A)| \geq |K||K(A \setminus \{a\} |\mathbf{K}_{\mathbf{D}})|$, which concludes the proof. $\square$

In the ideal case, by Lemma 3 we have an upper bound on the share domain of every subset of participants that form a circuit in the appropriate matroid. In the non-ideal case we cannot apply Lemma 3. Lemma 6 will be used to overcome this difficulty. To prove Lemma 6, we need the following claim.

Claim. Let N and K be 2 finite sets, where $|N| = m, |K| = k$, and $m \geq k$. Let f_1, f_2 be functions from a subset of N onto K. Then

$$|\{\langle x_1, x_2\rangle : x_1, x_2 \in N, f_1(x_1) = f_2(x_2)\}| \leq k - 1 + (m - k + 1)^2.$$

Proof. Without loss of generality, assume $K = \{1, 2, \ldots, k\}$. For $1 \leq i \leq k$ define $a_i \stackrel{\text{def}}{=} |f_1^{-1}(i)|$ and $b_i \stackrel{\text{def}}{=} |f_2^{-1}(i)|$. Then $\sum_{1 \leq i \leq k} a_i \leq m$ and $\sum_{1 \leq i \leq k} b_i \leq m$, since both these sums are the size of the domains of the functions. Moreover, since both these functions are onto K, we have $a_i \geq 1$ and $b_i \geq 1$ for all $1 \leq i \leq k$. Thus, $1 \leq a_i \leq m - k + 1$ and $1 \leq b_i \leq m - k + 1$ for every $1 \leq i \leq k$. From the definitions $|\{\langle x_1, x_2\rangle : x_1, x_2 \in N, f_1(x_1) = f_2(x_2)\}| = \sum_{1 \leq i \leq k} a_i b_i$. Assume without loss of generality that a_1 is maximal in $a_1, a_2, \ldots, a_k$. Then

$$\sum_{i=1}^{k} a_i b_i \leq \sum_{i=1}^{k} (a_i + a_1(b_i - 1)) \leq a_1(m - k) + m \leq k - 1 + (m - k + 1)^2. \quad \square$$

We note that this claim is tight as shown in the following simple example: $f_1(i) = f_2(i) = i$ for $1 \leq i \leq k$ and $f_1(i) = f_2(i) = 1$ for $k + 1 \leq i \leq m$.

Lemma 6. *Let $\mathcal{A}$ be an access structure, and denote the dealer by p_0. Let $A \subseteq P$ and $b_1, b_2 \in P$ such that $A \notin \mathcal{A}$, $A \cup \{b_1\} \in \mathcal{A}$, and $A \cup \{b_2\} \in \mathcal{A}$. Consider a weak secret sharing scheme realizing $\mathcal{A}$ in which the size of the domain of the secret is k, and the size of the domain of the shares of each participant is bounded by m. Then $|K(b_1, b_2|\mathbf{K}_{\mathbf{A}})| \leq k - 1 + (m - k + 1)^2$ for any $\mathbf{K}_{\mathbf{A}} \in K(A)$.*

Proof. Fix some $\mathbf{K}_{\mathbf{A}} \in K(A)$. Since $A \cup \{b_1\} \in \mathcal{A}$, given $\mathbf{K}_{\mathbf{A}}$, any $\mathbf{K}_{\mathbf{b_1}} \in K(b_1|\mathbf{K}_{\mathbf{A}})$ determines the secret. Moreover, since $A \notin \mathcal{A}$, given $\mathbf{K}_{\mathbf{A}}$ any value of the secret is possible. Therefore, $\mathbf{K}_{\mathbf{A}}$ induces a function from $K(b_1|\mathbf{K}_{\mathbf{A}})$ onto $K(p_0)$. Formally, the set of 2-vectors $K(b_1, p_0|\mathbf{K}_{\mathbf{A}})$ viewed as a set of ordered pairs form a function with $K(b_1|\mathbf{K}_{\mathbf{A}})$ as its domain and $K(p_0)$ as its image. Denote this function by f_1. Similarly $\mathbf{K}_{\mathbf{A}}$ also induces a function from $K(b_2|\mathbf{K}_{\mathbf{A}})$ onto $K(p_0)$. Denote this function by f_2.

Given $\mathbf{K}_{\mathbf{A}}$, consider any $\langle x_1, x_2\rangle \in K(b_1, b_2|\mathbf{K}_{\mathbf{A}})$. There is a row r in M that gives to the participants in A the values in $\mathbf{K}_{\mathbf{A}}$, and to b_1, b_2 the values x_1, x_2 respectively. However, $M_{r,p_0} = f_1(x_1) = f_2(x_2)$. Informally, given $\mathbf{K}_{\mathbf{A}}$, the shares x_1 and x_2 must "agree" on the secret. Thus, $f_1(x_1) = f_2(x_2)$ for every $\langle x_1, x_2\rangle \in K(b_1, b_2|\mathbf{K}_{\mathbf{A}})$. Since both f_1 and f_2 are onto $K(p_0)$, and since the domain of both functions is bounded by m, Claim 3 implies that $|K(b_1, b_2|\mathbf{K}_{\mathbf{A}})| \leq k - 1 + (m - k + 1)^2$. $\square$

4 Secret Sharing and the Vamos Matroid

In this section we prove lower bounds on the size of shares in secret sharing schemes realizing an access structure induced by the Vamos matroid. The Vamos matroid [46] is the smallest known matroid that is non-representable over any field, and is also non-algebraic (for more details on these notions see [47, 36]).

Definition 6 (The Vamos Matroid). *The Vamos matroid $\mathcal{V}$ is defined on the set $V = \{v_1, v_2, \ldots, v_8\}$, and its independent sets are all the sets of cardinality ≤ 4 except for five, namely $\{v_1, v_2, v_3, v_4\}$, $\{v_1, v_2, v_5, v_6\}$, $\{v_3, v_4, v_5, v_6\}$, $\{v_3, v_4, v_7, v_8\}$, 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 6 are circuits, a fact that will be used later. Seymour [39] proved that any access structure induced by the Vamos matroid is non-ideal. In this section we strengthen this result.

Definition 7 (The Access Structure V_8). *The access structure V_8 is the access structure induced by the Vamos matroid with respect to v_8.*[1] *That is, in this access structure, a set of participants is a minterm, if this set together with v_8 is a circuit in $\mathcal{V}$.*

Example 3. We next give examples of authorized and non-authorized sets in V_8. The set $\{v_3, v_4, v_7\}$ is authorized, since $\{v_3, v_4, v_7, v_8\}$ is a circuit. The circuit $\{v_1, v_2, v_3, v_4\}$ is unauthorized, since the set $\{v_1, v_2, v_3, v_4, v_8\}$ does not contain a circuit that contains v_8. 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_8. The set $\{v_1, v_2, v_3, v_4, v_5\}$ is authorized, since $\{v_1, v_2, v_3, v_5, v_8\}$ is a circuit (as well as $\{v_1, v_2, v_4, v_5, v_8\}$, $\{v_1, v_3, v_4, v_5, v_8\}$, and $\{v_2, v_3, v_4, v_5, v_8\}$).

For a given secret sharing scheme realizing V_8, assume $|K(v_8)| = k$, and $|K(v_i)| \leq m$ for $1 \leq i \leq 7$, i.e., the size of the domain of the secrets is k and the size of the domain of the shares of each participant is upper bounded by m. By [26], for every secret sharing scheme, the size of the domain of shares of each non-redundant participant is at least the size of the domain of secrets, that is, $m \geq k$. Seymour [39] proved that the Vamos access structure is not ideal, that is, $m \geq k + 1$. We next strengthen this result. To achieve the lower bound on m here, we fix an arbitrary $\langle x_1, x_2 \rangle \in K(v_1, v_2)$ and calculate an upper bound on the size of $K(v_7, v_8 | x_1, x_2)$ as a function of m and k. By Lemma 5 the size of this set is at least k^2, and thus, we achieve a lower bound on m.

[1] There are two non-isomorphic access structures induced by the Vamos matroid. The access structure V_8 is isomorphic to the access structure obtained by setting v_1, v_2, or v_7 as the dealer. The other access structure is obtained by setting v_3, v_4, v_5, or v_6 as the dealer.

Fix some arbitrary $\langle x_1, x_2\rangle \in K(v_1, v_2)$, and define $A \stackrel{\text{def}}{=} K(v_5, v_6|x_1, x_2)$ (see Fig. 1). Our goal is to count the possible shares $\{v_7, v_8\}$ can receive given $\langle x_1, x_2\rangle$. We upper bound this value by considering all the possible shares $\{v_5, v_6\}$ can receive given $\langle x_1, x_2\rangle$ (namely, the set A), and considering the union of all the sets $K(v_7, v_8|y_5, y_6)$ for all the vectors $\langle y_5, y_6\rangle$ in A. We first bound the size of A.

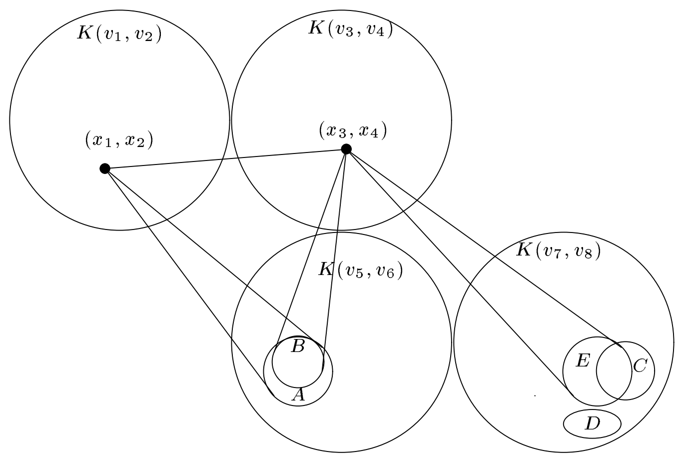

Fig. 1. Sets in the proof of Theorem 2. Circles denote sets, and points denote elements in the sets. Two elements are connected if they coincide. A line connects an element and a subset, if the subset is the set of all elements that coincide with the element. For example, $\langle x_1, x_2\rangle$ and A are connected with lines because A is the set of elements in $K(v_5, v_6)$ that can coincide with $\langle x_1, x_2\rangle$.

Lemma 7. $|A| \le m^{\frac{k-1+(m-k+1)^2}{k}}$.

Proof. Fix an arbitrary $x_3 \in K(v_3|x_1, x_2)$. The set $\{v_1, v_2, v_3\}$ is unauthorized (since $\{v_1, v_2, v_3, v_8\}$ is independent). Since $\{v_1, v_2, v_3, v_5, v_8\}$ is a circuit, $\{v_1, v_2, v_3, v_5\}$ is authorized. Similarly, the set $\{v_1, v_2, v_3, v_6\}$ is authorized too. Since $|K(v_5)| \le m$, and $|K(v_6)| \le m$, by Lemma 6,

$$|K(v_5, v_6|x_1, x_2, x_3)| \le k - 1 + (m - k + 1)^2. \tag{3}$$

We now bound the size of $K(v_3, v_5, v_6|x_1, x_2)$. Notice that

$$K(v_3, v_5, v_6|x_1, x_2) = \bigcup_{y_3 \in K(v_3|x_1, x_2)} \{\langle y_3, y_5, y_6\rangle : \langle y_5, y_6\rangle \in K(v_5, v_6|x_1, x_2, y_3)\}.$$

That is, we count all the y_3's that coincide with $\langle x_1, x_2\rangle$, and for each such y_3 we count all the $\langle y_5, y_6\rangle$'s that coincide with $\langle x_1, x_2, y_3\rangle$. Since (3) is true for any

$y_3 \in K(v_3|x_1,x_2)$, the size of each set in the union is at most $k-1+(m-k+1)^2$, and since $|K(v_3|x_1,x_2)| \le |K(v_3)| \le m$, there are at most m sets in the union. Therefore,

$$|K(v_3,v_5,v_6|x_1,x_2)| \le m\left(k-1+(m-k+1)^2\right). \tag{4}$$

On the other hand,

$$K(v_3,v_5,v_6|x_1,x_2) = \bigcup_{\langle y_5,y_6\rangle \in A} \{\langle y_3,y_5,y_6\rangle : \langle y_3\rangle \in K(v_3|x_1,x_2,y_5,y_6)\}.$$

Since $\{v_1,v_2,v_5,v_6\}$ is unauthorized, but $\{v_1,v_2,v_3,v_5,v_6\}$ is authorized, by Lemma 4 each set in this union is of size at least k. Since all these sets are disjoint, and by (4), there are at most $\frac{m}{k}(k-1+(m-k+1)^2)$ sets in this union. We conclude that $|A| \le m(k-1+(m-k+1)^2)/k$. □

In addition to x_1,x_2, fix an arbitrary vector $\langle x_3,x_4\rangle \in K(v_3,v_4|x_1,x_2)$. We define, in addition to A, a set of vectors $B \stackrel{\text{def}}{=} K(v_5,v_6|x_1,x_2,x_3,x_4)$. That is, the set A is the shares $\{v_5,v_6\}$ can receive given $\langle x_1,x_2\rangle$, and B is the shares $\{v_5,v_6\}$ can receive given $\langle x_1,x_2,x_3,x_4\rangle$. Clearly $B \subseteq A$.

To count the vectors in $K(v_7,v_8|A)$, we define two sets $C \stackrel{\text{def}}{=} K(v_7,v_8|B) = \bigcup_{\langle y_5,y_6\rangle\in B} K(v_7,v_8|y_5,y_6)$, and $D \stackrel{\text{def}}{=} K(v_7,v_8|A\setminus B)$.

Lemma 8. $|C|+|D| \le m-k^2+\left(\frac{k-1+(m-k+1)^2}{k}\right)m^2$.

Proof. First we show that $|C| \le |B|(m-k)+m$. Define $E \stackrel{\text{def}}{=} K(v_7,v_8|x_3,x_4)$. Informally, we will show that E is small and for any $\langle y_5,y_6\rangle \in B$ the set E contains a large portion of $K(v_7,v_8|y_5,y_6)$.

Since $\{v_3,v_4,v_7\}$ is authorized and by the correctness requirement, given $\langle x_3,x_4\rangle$ any $y_7 \in K(v_7|x_3,x_4)$ determines the secret, therefore

$$|E| = |K(v_7,v_8|x_3,x_4)| = |K(v_7|x_3,x_4)| \le |K(v_7)| \le m. \tag{5}$$

Since $\{v_3,v_4,v_5,v_6\}$ is unauthorized, for any $\langle y_5,y_6\rangle \in K(v_5,v_6|x_3,x_4)$, and in particular for any $\langle y_5,y_6\rangle \in B$, we have $|K(v_8|x_3,x_4,y_5,y_6)| = k$. Therefore,

$$|K(v_7,v_8|x_3,x_4,y_5,y_6)| \ge k$$

for any $\langle y_5,y_6\rangle \in B$. Clearly, $K(v_7,v_8|x_3,x_4,y_5,y_6) \subseteq E$ for any $\langle y_5,y_6\rangle \in B$. Since $K(v_7,v_8|x_3,x_4,y_5,y_6) \subseteq K(v_7,v_8|y_5,y_6)$ we conclude that for any $\langle y_5,y_6\rangle \in B$,

$$|K(v_7,v_8|y_5,y_6)\cap E| \ge k. \tag{6}$$

That is, given any $\langle y_5,y_6\rangle \in B$, at least k elements from $K(v_7,v_8|y_5,y_6)$ are in E. We now upper bound the number of elements of $K(v_7,v_8|y_5,y_6)$ not in E. To do this, we bound the total number of elements in $K(v_7,v_8|y_5,y_6)$ for any $\langle y_5,y_6\rangle$. Since $\{v_5,v_6,v_7\}$ is authorized, by the correctness requirement, given $\langle y_5, y_6\rangle$ any $y_7 \in K(v_7|y_5, y_6)$ determines the secret, therefore for any $\langle y_5, y_6\rangle \in K(v_5, v_6|x_1, x_2)$,

$$|K(v_7, v_8|y_5, y_6)| = |K(v_7|y_5, y_6)| \leq |K(v_7)| \leq m. \tag{7}$$

With (6), we conclude that for any $\langle y_5, y_6\rangle \in B$,

$$|K(v_7, v_8|y_5, y_6) \setminus E| \leq m - k. \tag{8}$$

That is, given any $\langle y_5, y_6\rangle \in B$, at most $m - k$ elements from $K(v_7, v_8|y_5, y_6)$ are not in E. Thus, by (5),

$$|C| \leq |E| + |B|(m-k) \ \leq \ m + |B|(m-k). \tag{9}$$

Furthermore, by (7), given any element in $A \setminus B$, the number of possible shares for $\{v_7, v_8\}$ is at most m. Therefore,

$$|D| \leq |A \setminus B|m. \tag{10}$$

Finally, since $\{v_1, v_2, v_3, v_4\}$ is unauthorized, but $\{v_1, v_2, v_3, v_4, v_5\}$ is authorized, by Lemma 4 we have $|K(v_5|x_1, x_2, x_3, x_4)| \geq k$, and therefore

$$|B| = |K(v_5, v_6|x_1, x_2, x_3, x_4)| \geq |K(v_5|x_1, x_2, x_3, x_4)| \geq k. \tag{11}$$

We now complete the proof of the lemma:

$$\begin{aligned} |C| + |D| \leq m + |B|(m-k) + |A \setminus B|m \ &= \ m - k|B| + |A|m \\ &\leq m - k^2 + \left(\frac{k - 1 + (m-k+1)^2}{k}\right) m^2. \end{aligned}$$

The first inequality follows (9) and (10). The equality is implied by the fact that $B \subseteq A$. The last inequality follows (11) and Lemma 7. □

Lemma 9. *For every* $\langle x_1, x_2\rangle \in K(v_1, v_2)$

$$K(v_7, v_8|x_1, x_2) \leq m - k^2 + m^2 \frac{k + (m-k+1)^2}{k}.$$

Proof. We first show that $K(v_7, v_8|x_1, x_2) \subseteq K(v_7, v_8|A)$. Take any $\langle y_7, y_8\rangle \in K(v_7, v_8|x_1, x_2)$. The vector $\langle x_1, x_2, y_7, y_8\rangle$ can be extended to a vector

$$\langle x_1, x_2, y_5, y_6, y_7, y_8\rangle \in K(v_1, v_2, v_5, v_6, v_7, v_8).$$

Thus, $\langle y_5, y_6, y_7, y_8\rangle \in K(v_5, v_6, v_7, v_8)$ and $\langle y_5, y_6\rangle \in K(v_5, v_6|x_1, x_2) = A$, and so $\langle y_7, y_8\rangle \in K(v_7, v_8|A)$. Consequently,

$$\begin{aligned} |K(v_7, v_8|x_1, x_2)| \leq |K(v_7, v_8|A)| \ &\leq \ |C| + |D| \\ &= m - k^2 + m^2 \frac{k - 1 + (m-k+1)^2}{k} \\ &< m - k^2 + m^2 \frac{k + (m-k+1)^2}{k}. \end{aligned}$$

□

Theorem 2. *For any $0 < \lambda < 1$ there exists $k_0 \in \mathbb{N}$, such that for any secret sharing scheme realizing V_8, with the domain of the secret of size $k > k_0$, the size of at least one share domain is larger then $k + \lambda\sqrt{k}$.*

Proof. Let $0 < \lambda < 1$, and assume $m \leq k+\lambda\sqrt{k}$. Since $\{v_1, v_2, v_3, v_7, v_8\}$ is a circuit in the Vamos matroid and $\{v_1, v_2, v_7, v_8\} \subseteq \{v_1, v_2, v_3, v_7, v_8\}$, by Lemma 5, $|K(v_7, v_8|x_1, x_2)| \geq k^2$ for every $\langle x_1, x_2\rangle \in K(v_1, v_2)$ in any secret sharing scheme realizing V_8. Combining this with Lemma 9, we have that if m is an upper bound on the size of the domain of the shares, then the following inequality must hold:

$$\left(m - k^2 + m^2\frac{k + (m-k+1)^2}{k}\right) \geq k^2. \tag{12}$$

Since the left side of Inequality (12) increases as m increases, and since $m \leq k + \lambda\sqrt{k}$, we can substitute m with $k + \lambda\sqrt{k}$. After rearranging we have:

$$k^2 \leq k + \lambda\sqrt{k} - k^2 + (k^2 + \lambda^2 k + 2\lambda k\sqrt{k})\frac{k + (\lambda\sqrt{k}+1)^2}{k} = \lambda^2 k^2 + p_\lambda(k),$$

where $p_\lambda(k)$ is a polynomial of degree 1.5 in k. Thus, $1 - \lambda^2 \leq \frac{p_\lambda(k)}{k^2}$. Since $1 - \lambda^2 > 0$ and since $\lim_{k\to\infty} \frac{p_\lambda(k)}{k^2} = 0$, we conclude that there exists some $k_0 \in \mathbb{N}$, such that for any $k \geq k_0$, Inequality (12) does not hold. We conclude that for any $k \geq k_0$, at least one participant must have domain of shares larger than $k + \lambda\sqrt{k}$. □

5 Upper and Lower Bounds for Matroid Induced Access Structures

In this section we define secret sharing schemes using the entropy function, as done in [26, 12], and then use some tools from information theory to prove lower and upper bounds on sizes of shares' domains of subsets of participants in matroid induced access structures. The purpose of these lemmas is to generalize Lemma 3 of [11] to non-ideal secret sharing schemes for matroid induced access structures. These lemmas were not used in the proof of Theorem 2, but they might be used to prove a stronger bound than the lower bound proved here. For a review on the notions from information theory, see Appendix A. We start by defining (strong) secret sharing schemes using the entropy function.

Definition 8 (Distribution Scheme). *Let P be a set of participants, and $p_0 \notin P$ be a special participant called* the dealer. *Furthermore, let K be a finite set of secrets. A* distribution scheme *Σ with* domain of secrets *K is a pair $\langle \{M^s\}_{s\in K}, \{\Pi_s\}_{s\in K}\rangle$, where $\{M^s\}_{s\in K}$ is a family of matrices whose columns are indexed by P, and Π_s is a probability distribution on the rows of M^s for each $s \in K$. When the dealer wants to distribute a secret $s \in K$, it chooses according to the probability distribution Π_s on M^s, a row $r \in M^s$, and privately communicates to each participant $p \in P$ the value $M^s_{r,p}$. We refer to $M^s_{r,p}$ as the* share *of participant p.*

Let $\mathcal{A}$ be an access structure whose set of participants is P, and denote the dealer by p_0. Assume that Σ is a distribution scheme for $\mathcal{A}$. Any probability distribution on the domain of secrets, together with the scheme Σ, induces a probability distribution on $K(A)$, for any subset $A \subseteq P$. We denote the random variable taking values in $K(A)$ according to this probability distribution by S_A, and denote the random variable taking values in K according to the probability distribution on the secrets by S. Note that the random variable taking values in $K(A \cup B)$ can be written either as $S_{A \cup B}$ or as $S_A S_B$.

Definition 9 (Secret Sharing Scheme). *A distribution scheme is a secret sharing scheme realizing an access structure $\mathcal{A}$ if the following two requirements hold:*

CORRECTNESS. *The secret can be reconstructed by any authorized set.*

$$A \in \mathcal{A} \Longrightarrow H(S|S_A) = 0. \tag{13}$$

PRIVACY. *Every unauthorized set can learn nothing about the secret (in the information theoretic sense) from its shares. Formally,*

$$A \notin \mathcal{A} \Longrightarrow H(S|S_A) = H(S). \tag{14}$$

5.1 Lower Bounds on the Entropy of Shares of Subsets

Let $p_0 \in V$ and let $\langle V, \mathcal{C} \rangle$ be the appropriate matroid of an access structure $\mathcal{A} \subseteq 2^{V \setminus \{p_0\}}$. In Theorem 3 we prove a lower bound on the entropy of the shares of any subset of V. To prove Theorem 3 we prove two lemmas. The first lemma, which generalizes Lemma 4, makes no use of the fact that $\mathcal{A}$ has an appropriate matroid; it is proven for any access structure.

Lemma 10. *Let $A, B \subseteq V \setminus \{p_0\}$ and $b \in B \setminus A$ such that $A \cup B \in \mathcal{A}$ and $A \cup B \setminus \{b\} \notin \mathcal{A}$. Then, $H(S_b|S_A) \geq H(S)$.*

Proof.

$$\begin{aligned}
H(S_b|S_A) &\geq H(S_b|S_A S_{B\setminus\{b\}}) \qquad \text{(from (21))} \\
&= H(S|S_{A\cup B}) + H(S_b|S_{A\cup B\setminus\{b\}}) \qquad \text{(since } H(S|S_{A\cup B}) = 0 \text{ by (13))} \\
&= H(S_b S|S_{A\cup B\setminus\{b\}}) \qquad \text{(from (22))} \\
&= H(S_b|S_{A\cup B\setminus\{b\}} S) + H(S|S_{A\cup B\setminus\{b\}}) \qquad \text{(from (22))} \\
&\geq H(S) \qquad \text{(from (19) and (14), and because } A \cup B \setminus \{b\} \notin \mathcal{A}) \qquad \square
\end{aligned}$$

A consequence of Lemma 10 is that if $I \subseteq A$ for a minterm A and $i \in I$, then $H(S_i|S_{I\setminus\{i\}}) \geq H(S)$. Combining this with (20), we get by induction that $H(S_I) \geq |I|H(S)$. We now generalize this claim for every independent set. We next prove a lemma on matroids that will be used to prove this generalization. The next lemma, intuitively, states that in every independent set of participants there is a participant that is needed in order to reveal the secret. That is, there is a minterm (minimal authorized set) such that omitting this participant from the union of the independent set and the minterm results in an unauthorized set. Define $\mathcal{C}_0 \stackrel{\text{def}}{=} \{C \in \mathcal{C} : p_0 \in C\}$.

Lemma 11. *For every independent set $I \subseteq V \setminus \{p_0\}$, there exists $i \in I$ and $C \in \mathcal{C}_0$ such that $i \in C$ and there is no $C_1 \in \mathcal{C}_0$ such that $C_1 \subseteq C \cup I \setminus \{i\}$.*

Proof. For every $i \in I$ there exists a circuit $C \in \mathcal{C}_0$ such that $i \in C$ (since $\mathcal{M}$ is connected). Choose an $i \in I$ and $C \in \mathcal{C}_0$ such that $i \in C$ and for every $C' \in \mathcal{C}_0$

$$I \cap C' \neq \emptyset \Longrightarrow C' \setminus I \text{ is not properly contained in } C \setminus I. \tag{15}$$

(Note that not necessarily every i can be chosen.) We claim that such i and C satisfy the conditions of the lemma, namely, there is no $C_1 \in \mathcal{C}_0$ such that $C_1 \subseteq C \cup I \setminus \{i\}$. Assume towards contradiction that this is not the case, and choose $C_1 \in \mathcal{C}_0$ such that

$$C_1 \subseteq C \cup I \setminus \{i\}\,. \tag{16}$$

We have $C_1 \cap I \neq \emptyset$, otherwise $C_1 \subsetneq C$ in a contradiction to Axiom (C1) of the matroids. Therefore, by (15) and (16), $C \setminus I = C_1 \setminus I$. Let $c \in C \setminus I = C_1 \setminus I$. Such c exists, otherwise we have $C_1 \subseteq I$ and so I is not independent. Since $c \in C \cap C_1$, by Axiom (C2) there exists a circuit $C_2 \subseteq C \cup C_1 \setminus \{c\}$. We have $C_2 \cap I \neq \emptyset$ (otherwise $C_2 \subsetneq C$), and so $p_0 \notin C_2$ (otherwise we have a contradiction to (15)), and so $p_0 \in C \setminus \mathcal{C}_2$. Moreover, $C_2 \setminus I \neq \emptyset$, otherwise $C_2 \subseteq I$ contradicting the independence of I. So there exists $c' \in C_2 \setminus I$, where $c' \neq c$. Since $C_2 \setminus I \subseteq C \setminus I$ we have that $c' \in C \setminus I$, so $c' \in C_2 \cap C$, and therefore there is a circuit $C_3 \in \mathcal{C}_0$ such that $C_3 \subseteq C_2 \cup C \setminus \{c'\}$ (from Lemma 1). Since $c' \in C \setminus C_3$, we have $C_3 \setminus I \subsetneq C \setminus I$. Moreover $C_3 \cap I \neq \emptyset$ (otherwise $C_3 \subsetneq C$), and therefore C_3 is a contradiction to the minimality of $C \setminus I$ (defined in (15)), so C and i satisfy the conditions of the lemma. ◻

Theorem 3. *For every $A \subseteq V, H(S_A) \geq \mathrm{rank}(A)H(S)$.*

Proof. From the definition of the rank function and (20), it is sufficient to show that the statement holds for any independent set $I \subseteq V$. Since every subset of an independent set in a matroid is independent, by induction, it is sufficient to show that for every independent set I there exists $i \in I$ such that $H(S_I) \geq H(S) + H(S_{I\setminus\{i\}})$. If $p_0 \in I$ then since I is independent it contains no circuit, and particularly no circuit which contains p_0. Therefore, $I \setminus \{p_0\}$ contains no minterm, and we have $I \setminus \{p_0\} \notin \mathcal{A}$. Now by (14) $H(S|S_{I\setminus\{p_0\}}) = H(S)$, and we have $H(S_I) = H(S|S_{I\setminus\{p_0\}}) + H(S_{I\setminus\{p_0\}}) = H(S) + H(S_{I\setminus\{p_0\}})$. Otherwise, by Lemma 11 for every independent set $I \subseteq V \setminus \{p_0\}$, there exists $i \in I$ and $C \in \mathcal{C}_0$ such that $i \in C$ and there is no $C_1 \in \mathcal{C}_0$ such that $C_1 \subseteq C \cup I \setminus \{i\}$. Therefore, we have $I \cup C \setminus \{i, p_0\} \notin \mathcal{A}$, but $I \cup C \setminus \{p_0\} \in \mathcal{A}$, and so, by Lemma 10, $H(S_i|S_{I\setminus\{i\}}) \geq H(S)$ and we have $H(S_I) = H(S_i|S_{I\setminus\{i\}}) + H(S_{I\setminus\{i\}}) \geq H(S) + H(S_{I\setminus\{i\}})$. ◻

5.2 Upper Bounds on the Entropy of Shares of Subsets

In Lemma 15 we prove an upper bound on the entropy of "the last element of a circuit," that is, we prove an upper bound on the entropy of an element in a circuit, given the rest of the elements, and assuming an upper bound on the entropy of the participants. This enables us to prove, in Theorem 4, upper bounds on the entropy of shares of subsets. Let $\mathcal{M}$ and Σ be as above, and assume that, for every $v \in V \setminus \{p_0\}$, $H(S_v) \le (1+\lambda)H(S)$ for some $\lambda \ge 0$. Define $\mathcal{C}_0 \stackrel{\text{def}}{=} \{C \in \mathcal{C} : p_0 \in C\}$ as above. For lack of space, some proofs in this section are omitted.

Lemma 12. *For every $C \in \mathcal{C}_0$ and $c \in C$, $H(S_c | S_{C\setminus\{c\}}) \le \lambda H(S)$.*

Lemma 13. *For every $C \in \mathcal{C} \setminus \mathcal{C}_0$ and $c \in C$, there exists $C_1, C_2 \in \mathcal{C}_0$ such that $C = D_{p_0}(C_1, C_2)$, and $c \in C_1 \setminus C_2$ (where $D_{p_0}(C_1, C_2)$ is defined in Lemma 2).*

Proof. From Lemma 2 there are $C_1, C_2 \in \mathcal{C}_0$ such that $C = D_{p_0}(C_1, C_2)$. If $c \in C_1 \vartriangle C_2$ we are done. Otherwise, $c \in C_1 \cap C_2$. By the definition of $D_{p_0}(C_1, C_2)$, there must be some $C_3 \in \mathcal{C}_0$ such that $C_3 \subseteq C_1 \cup C_2 \setminus \{c\}$ (otherwise $c \in I_{p_0}(C_1, C_2)$), and so we have $c \in C_1 \setminus C_3$. We now prove that $C = D_{p_0}(C_1, C_3)$ and this completes the proof. Notice that $C_1 \cup C_3 \subseteq C_1 \cup C_2$, from which we get $I_{p_0}(C_1, C_2) \subseteq I_{p_0}(C_1, C_3)$. Therefore, $D_{p_0}(C_1, C_3) \subseteq D_{p_0}(C_1, C_2)$. By Lemma 2, the circuits which do not contain p_0 are the *minimal* sets of the form $D_{p_0}(C_1, C_2)$ for all $C_1, C_2 \in \mathcal{C}_0$. Thus, since $D_{p_0}(C_1, C_2)$ is a circuit, $D_{p_0}(C_1, C_3) = D_{p_0}(C_1, C_2)$, and therefore $C = D_{p_0}(C_1, C_3)$ as desired. $\square$

Lemma 14. *Let $C = D_{p_0}(C_1, C_2)$, and $I = I_{p_0}(C_1, C_2) \setminus \{p_0\}$. Then,*

$$H(S_I | S_C) \ge |I| H(S).$$

Lemma 15. *For every $C \in \mathcal{C} \setminus \mathcal{C}_0$ such that $C = D_{p_0}(C_1, C_2)$, and $c \in C$ such that $c \in C_1 \setminus C_2$, $H(S_c | S_{C\setminus\{c\}}) \le |I_{p_0}(C_1, C_2)| \lambda H(S)$. In particular, for every $C \in \mathcal{C} \setminus \mathcal{C}_0$ and $c \in C$, $H(S_c | S_{C\setminus\{c\}}) \le n\lambda H(S)$.*

Theorem 4. *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 a secret sharing scheme realizing $\mathcal{A}$, and let $\lambda \ge 0$ be such that $H(S_v) \le (1+\lambda)H(S)$ for every $v \in V \setminus \{p_0\}$. Then, for every $A \subseteq V$*

$$H(S_A) \le \mathrm{rank}(A)(1+\lambda)H(S) + (|A| - \mathrm{rank}(A))\lambda n H(S).$$

The previous theorem is useful only when $\lambda \le 1/(n-1)$ (otherwise the bound $H(S_A) \le |A|(1+\lambda)H(S)$ is better). We next show how to apply these results to the Vamos matroid, considered in Section 4. We then compare this bound to the bound we achieve in Section 4.

Example 4. Consider a secret sharing scheme realizing the Vamos access structure V_8. Recall that the set $\{v_1, v_2, v_5, v_6\}$ is a circuit of the Vamos matroid. By Theorem 4, $H(S_{\{v_1,v_2,v_5,v_6\}}) \le (3+10\lambda)H(S)$ (by using Lemma 15 we can get a better dependence of λ). Since $\{v_1, v_2\}$ is independent, by Theorem 3, $H(S_{\{v_1,v_2\}}) \ge 2H(S)$. Thus, by (20), $H(S_{\{v_5,v_6\}} | S_{\{v_1,v_2\}}) = H(S_{\{v_1,v_2,v_5,v_6\}}) - H(S_{\{v_1,v_2\}}) \le (1+10\lambda)H(S)$. Thus, there is a vector of shares $\langle x_1, x_2 \rangle$ such that

$$H\left(S_{\{v_5,v_6\}} | S_{\{v_1,v_2\}} = \langle x_1, x_2 \rangle\right) \le (1+10\lambda)H(S).$$

Now, we consider a specific setting of the parameters. Let us assume that there are k possible secrets distributed uniformly, and the size of the domain of shares of each participant is at most $2k$. Thus, $H(S) = \log k$ and, by (18), $H(S_{v_i}) \leq \log(2k) = H(S) + 1 = (1 + 1/\log k)H(S)$. Thus, there is a vector of shares $\langle x_1, x_2 \rangle$ such that $H(S_{\{v_5,v_6\}} | S_{\{v_1,v_2\}} = \langle x_1, x_2 \rangle) \leq (1 + 10/\log k)H(S)$. This should be compared to the bound of approximately $2H(S)$ we can achieve by Lemma 7 and (18). Notice that in the proof of our main result we prove in Lemma 7 an *upper bound* on the number of possible shares of $\{v_5, v_6\}$ given a vector of shares $\langle x_1, x_2 \rangle$ of $\{v_1, v_2\}$. Here we give a better upper-bound on the entropy of the shares of $\{v_5, v_6\}$ given a vector of shares $\langle x_1, x_2 \rangle$ of $\{v_1, v_2\}$. We do not know how to use this better bound on the entropy in the proof of the lower bound for the Vamos access structure.

Acknowledgment. We thank Enav Weinreb for very helpful discussions.

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 Y. Ishai. On the power of nonlinear secret-sharing. *SIAM Journal on Discrete Mathematics*, 19(1):258-280, 2005.
3. A. Beimel, T. Tassa, and E. Weinreb. Characterizing ideal weighted threshold secret sharing. In *TCC 2005*, vol. 3378 of *LNCS*, pages 600–619. 2005.
4. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computations. In *Proc. of the 20th STOC*, pages 1–10, 1988.
5. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *CRYPTO '88*, vol. 403 of *LNCS*, pages 27–35. 1990.
6. G. R. Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, pages 313–317. 1979.
7. C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the information rate of secret sharing schemes. *Theoretical Computer Science*, 154(2):283–306, 1996.
8. C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decomposition and secret sharing schemes. *J. of Cryptology*, 8(1):39–64, 1995.
9. C. Blundo, A. De Santis, and A. Giorgio Gaggia. Probability of shares in secret sharing schemes. *Inform. Process. Lett.*, 72:169–175, 1999.
10. E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.
11. E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. of Cryptology*, 4(73):123–134, 1991.
12. 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.
13. D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *Proc. of the 20th STOC*, pages 11–19, 1988.
14. T. M. Cover and J. A. Thomas. *Elements of Information Theory.* John Wiley & Sons, 1991.
15. R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *EUROCRYPT 2000*, vol. 1807 of *LNCS*, pages 316–334. 2000.

16. R. Cramer, V. Daza, I. Gracia, J. Jimenez Urroz, G. Leander, J. Marti-Farre, and C. Padro. On codes, matroids and secure multi-party computation from linear secret sharing schemes. In *CRYPTO 2005*, vol. 3621 of *LNCS*, pages 327–343. 2005.
17. L. Csirmaz. The dealer's random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar.*, 32(3–4):429–437, 1996.
18. L. Csirmaz. The size of a share must be large. *J. of Cryptology*, 10(4):223–231, 1997.
19. Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In *CRYPTO '91*, vol. 576 of *LNCS*, pages 457–469. 1992.
20. M. van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6:143–169, 1995.
21. M. van Dijk. A linear construction of secret sharing schemes. *Designs, Codes and Cryptography*, 12(2):161–201, 1997.
22. M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Proc. of Globecom 87*, pages 99–102, 1987. Journal version: Multiple assignment scheme for sharing secret. *J. of Cryptology*, 6(1):15-20, 1993.
23. W. Jackson and K. M. Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography*, 9:267–286, 1996.
24. W. Jackson, K. M. Martin, and C. M. O'Keefe. Ideal secret sharing schemes with multiple secrets. *J. of Cryptology*, 9(4):233–250, 1996.
25. M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th Structure in Complexity Theory*, pages 102–111, 1993.
26. E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, 1983.
27. K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii. Nonperfect secret sharing schemes and matroids. In *EUROCRYPT '93*, vol. 765 of *LNCS*, pages 126–141. 1994.
28. N. Livne. On matroids and non-ideal secret sharing. Master's thesis, Ben-Gurion University, Beer-Sheva, 2005.
29. J. Martí-Farré and C. Padró. Secret sharing schemes on access structures with intersection number equal to one. In *SCN '02*, vol. 2576 of *LNCS*, pages 354–363. 2002.
30. 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.
31. K. M. Martin. *Discrete Structures in the Theory of Secret Sharing.* PhD thesis, University of London, 1991.
32. P. Morillo, C. Padró, G. Sáez, and J. L. Villar. Weighted threshold secret sharing schemes. *Inform. Process. Lett.*, 70(5):211–216, 1999.
33. M. Naor and A. Wool. Access control and signatures via quorum secret sharing. *IEEE Transactions on Parallel and Distributed Systems*, 9(1):909–922, 1998.
34. S.-L. Ng. A representation of a family of secret sharing matroids. *Designs, Codes and Cryptography*, 30(1):5–19, 2003.
35. S.-L. Ng and M. Walker. On the composition of matroids and ideal secret sharing schemes. *Designs, Codes and Cryptography*, 24(1):49 – 67, 2001.
36. J. G. Oxley. *Matroid Theory.* Oxford University Press, 1992.
37. C. Padró and G. Sáez. Secret sharing schemes with bipartite access structure. *IEEE Trans. on Information Theory*, 46:2596–2605, 2000.
38. M. O. Rabin. Randomized Byzantine generals. In *Proc. of the 24th FOCS*, pages 403–409, 1983.

39. P. D. Seymour. On secret-sharing matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.
40. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.
41. G. J. Simmons, W. Jackson, and K. M. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.
42. J. Simonis and A. Ashikhmin. Almost affine codes. *Designs, Codes and Cryptography*, 14(2):179–197, 1998.
43. D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography*, 2:357–390, 1992.
44. D. R. Stinson. Decomposition construction for secret sharing schemes. *IEEE Trans. on Information Theory*, 40(1):118–125, 1994.
45. T. Tassa. Hierarchical threshold secret sharing. In *TCC 2004*, vol. 2951 of *LNCS*, pages 473–490. 2004.
46. P. Vamos. On the representation of independence structures. Unpublished manuscript, 1968.
47. D. J. A. Welsh. *Matroid Theory.* Academic press, London, 1976.

A Basic Definitions from Information Theory

We review here the basic concepts of Information Theory used in this paper. For a complete treatment of this subject, see [14]. All the logarithms here are of base 2.

Given a probability distribution $\{p(x)\}_{x\in X}$ on a finite set X, we define the *entropy* of X, denoted $H(X)$, as

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

Given two sets X and Y and a joint probability distribution $\{p(x,y)\}_{x\in X, y\in Y}$ on $X\times Y$, we define the *conditioned entropy of* X *given* Y as

$$H(X|Y) \stackrel{\text{def}}{=} -\sum_{y\in Y, p(y)>0}\ \sum_{x\in X, p(x|y)>0} p(y)p(x|y)\log p(x|y).$$

We also define the *conditioned mutual information* $I(X;Y|Z)$ between X and Y given Z as

$$I(X;Y|Z) \stackrel{\text{def}}{=} H(X|Z) - H(X|YZ). \tag{17}$$

For convenience, in the following text, when dealing with the entropy function XY will denote $X\cup Y$. We will use the following properties of the entropy function. Let X, Y, and Z be random variables, and $|X|$ be the size of the support of X (the number of values with probability greater than zero).

$$0 \le H(X) \le \log|X| \tag{18}$$

$$0 \le H(X|Y) \le H(X) \tag{19}$$

$$H(Y) \le H(XY) = H(X|Y) + H(Y) \le H(X) + H(Y) \tag{20}$$

$$H(X|Y) \ge H(X|YZ) \tag{21}$$

$$H(XY|Z) = H(X|YZ) + H(Y|Z) \tag{22}$$

$$I(X;Y|Z) = H(X|Z) - H(X|YZ) = H(Y|Z) - H(Y|XZ) = I(Y;X|Z) \tag{23}$$