On Matroids and Non-ideal Secret Sharing

Amos Beimel and Noam Livne

***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) has proved that the necessary condition is not sufficient: There exists an access structure induced by a matroid that does not have an ideal scheme.**

The research on access structures induced by matroids is continued in this work. The main result in this paper is strengthening the result of Seymour. It is shown 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 $k + \Omega(\sqrt{k})$. The second result considers non-ideal secret-sharing schemes realizing access structures induced by matroids. It is proved 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 (as long as the shares are still relatively short). This generalized results of Brickell and Davenport for ideal schemes. Finally, an example of a non-ideal access structure that is nearly ideal is presented.

***Index Terms*—Secret-sharing schemes, Vamos matroid, Weakly-private secret-sharing schemes.**

I. 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 access structure, Ito, Saito, and Nishizeki [2] have constructed a secret-sharing scheme realizing the access structure. Even with more efficient schemes presented since, e.g. in [3], [4], [5], [6], [7], [8], most access structures require shares of exponential size: even 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 [9] 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 have the most efficient secret-sharing schemes as proved by [10], (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 [12] 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. Matúš [13] has shown that access structures induced by several other matroids do not have ideal schemes. 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?

For access structures induced by matroids, there is no better known upper bound on the share size than the $2^{O(n)}$ bound for general access structures (which follows from [2]). Most known secret-sharing schemes are linear (see discussion in Section I-B). On one hand, the number of linear schemes with n participants, binary domain of secrets, and shares of size $\mathrm{poly}(n)$ is $2^{\mathrm{poly}(n)}$ (this follows by a simple counting of linear schemes, observing that we only consider finite fields with $2^{\mathrm{poly}(n)}$ elements). On the other hand, the number of matroids with n points is $\exp(2^{\Theta(n)})$ (see [14]) and every matroid induces exactly one access structure (given a fixed dealer). Thus, for most access structures induced by matroids, the size of the shares in linear secret-sharing schemes with binary domain 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.

A preliminary version of this paper appears in [1].

Amos Beimel is with the dept. of Computer Science, Ben-Gurion University, Beer-Sheva, Israel. Partially supported by the David and Lucile Packard Foundation grant of Matthew Franklin, and by the Frankel Center for Computer Science at the Ben-Gurion University.

Noam Livne is with the Weizmann institute of science, Rehovot, Israel. Work done while at the dept. of Computer Science, Ben-Gurion University, Beer-Sheva, Israel.

A. Our Results

In this work we continue the research on access structures induced by matroids. Seymour [12] has showed that any access structure induced by the Vamos matroid [15] 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 [12]). We first give a somewhat simpler proof of Seymour's result, and then strengthen it. Towards proving this stronger 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. The best secret-sharing scheme realizing the access structure induced by the Vamos matroid was recently presented by Martí-Farré and Padró [16] (improving on [17]); in this scheme the size of the domain of shares is $k^{4/3}$. Thus, our work still leaves open the question of the minimal-size share domain for this access structure.

In this work, we consider a weaker notion of secret-sharing schemes, called weakly-private secret-sharing schemes. In these schemes an unauthorized set can never rule out any secret (in contrast to perfect schemes where an unauthorized set cannot deduce any "probabilistic" information on the secret). Since every perfect secret-sharing scheme is a weakly-private secret-sharing scheme, it suffices to prove lower bounds for weakly-private secret-sharing schemes. In particular, in this work we prove the lower bound of $k + \Omega(\sqrt{k})$ for weakly-private secret-sharing schemes. Following this work, Beimel and Franklin [18] have studied weakly-private secret-sharing schemes and have proved upper bounds for such schemes. In particular, for the access structure induced by the Vamos matroid, they construct a weakly-private scheme in which the size of the domain of shares is $16k$. Thus, to prove lower bound of k^α for some $\alpha > 1$, it would be necessary to use arguments that do not hold for weakly-private secret-sharing schemes.

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 (provided that the domain of shares is still relatively small). 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 III, contains somewhat weaker bounds; however, this is the version we can use in the proof of our main result. The second version, in Section V, 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 [10], [19]. Specifically, entropy arguments have been used for ideal secret-sharing schemes in [20]. 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.

As the entropy bounds do not hold for weakly-private secret-sharing schemes, these bounds seem useful in view of the upper bound of [18]. Indeed, in a follow-up work [21], these bounds are used to prove stronger bounds than the lower bound proved here: In any secret-sharing scheme realizing an access structure induced by the Vamos matroid, the size of the domain of shares of at least one participant is at least $k^{1.1}$ (where k is the size of the domain of secrets)

Finally, we present an example of a non-ideal access structure induced by a matroid, which is nearly ideal: for infinitely many values of k it has a secret-sharing scheme realizing it with domain of secrets of size k and domain of shares of size $k + 1$. The fact that the access structure described in our example is nearly ideal was proved independently by Matúš [22]. This implies that there is an access structure with optimal information rate 1 that is not ideal.

We remark that our results in this paper are related to an open problem of Martí-Farré and Padró [23], [24]:

Question 1: Does there exist an access structure whose optimal share size is $\Theta(k^\alpha)$ for some constant $1 < \alpha < 1.5$? By a recent result of [17], such access structure must have an appropriate matroid as in every secret-sharing scheme realizing an access structure that does not have an appropriate matroid the size of the domain of shares of at least one participant is at least $k^{1.5}$. The results of [21], together with the result of [16], show that the access structures induced by the Vamos matroid are such access structures.

B. Related Works

Secret-sharing schemes were first introduced by Blakley [25] and Shamir [9] 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 [2]. More efficient schemes were presented in, e.g., [3], [4], [5], [6], [7], [8]. 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 [26], secure multiparty computations [27], [28], [29], threshold cryptography [30], and access control [31].

Several lower bounds on the share size of secret-sharing schemes were obtained [3], [19], [32], [33], [34], [35]. The strongest current bound is proved by Csirmaz [35]; he proves that for every n there is an access structure $\mathcal{A}_n$ with n participants such that for every integer ℓ and every secret-sharing scheme realizing $\mathcal{A}_n$ with ℓ-bit secrets the size of the shares of at least one participant is $\Omega(\ell n / \log n)$. 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 implicit) access structures is still open.

Ideal secret-sharing schemes and ideal access structures, considered in this work, have been studied extensively. Brickell [5] was the first to introduce the notion of ideal access structures. He has shown that if an access structure is induced by a matroid representable over some finite field, then the access structure is ideal. In particular, he designed ideal secret-sharing schemes for multilevel access structures, and for compartmented access structures (Tassa [36] and Dyn and Tassa [37] have constructed explicit ideal secret-sharing schemes for these access structures). Brickell and Davenport [11] have shown that ideal access structures are closely related to matroids over a set containing the participants and the dealer, and, as elaborated above, give a necessary condition and a sufficient condition for an access structure to be ideal (see also [38]).

However, there is still a gap between these conditions: Seymour [12] has shown that the necessary condition of [11] is not sufficient, by showing that the access structure induced by the Vamos matroid does not have an ideal scheme. Simonis and Ashikhmin [39] have given a more geometric proof of this result. Matúš [13] has shown that ideal schemes are closely related to the solutions of a system of generalized quasigroup equations associated to the matroid inducing the access structure. Using this relation, Matúš has shown that access structures induced by several other matroids (including the nonDesargues matroids and matroids that contain as restriction both the Fano and nonFano matroids) do not have ideal schemes.

Kurosawa et al. [20] have studied the connection between non-perfect secret-sharing schemes and matroids. Beimel and Chor [40] have characterized universally ideal access structures, that is, access structures that are ideal over every finite domain of secrets. As an intermediate step, they have proved that an access structure is ideal over a binary domain (respectively, ternary domain) of secrets if and only if it is induced by a matroid representable over $\mathbb{F}_2$ (respectively, $\mathbb{F}_3$). Jackson, Martin, and O'Keefe [41] have considered ideal secret-sharing schemes with multiple secrets. Simonis and Ashikhmin [39] have defined almost affine codes, which can be viewed as a matrix such that there exists an integer q for which any restriction of the columns of the matrix yields a submatrix with q^i distinct rows, for some integer i. They have shown that almost affine codes are essentially ideal secret-sharing schemes. Ng and Walker [42] have defined the strong connectivity equivalence relation, and have shown that under this equivalence relation an ideal secret-sharing scheme decomposes into threshold schemes. They have given a necessary condition for an access structure to be ideal for the case when the number of equivalence classes is two. Ng [43] has proved that this condition is sufficient. In a recent paper, Farràs, Martí-Farré, and Padró [44] have presented a characterization of matroid-related multipartite access structures in terms of discrete polymatroids, and provide a necessary condition and a sufficient condition for a multipartite access structure to be ideal.

As there is no exact characterization of ideal access structures, ideal access structures were characterized for particular families of access structures: access structures on sets of four participants [45] and five participants [46], access structures in which the minimal authorized sets are of size 2 (called graph access structures) [47], bipartite access structures [48], access structures with three or four minimal subsets [23], access structures with intersection number equal to one [24], and weighted threshold access structures [49] (special cases of ideal weighted access structures were characterized in [50]). Recently, Martí-Farré and Padró [17] (generalizing results of [45], [46], [47], [48], [23], [24]) have shown that in any non-matroidial access-structure, there is at least one participant whose share domain size is at least $k^{1.5}$, where k is the size of the domain of secrets.

Most previously known secret-sharing schemes were *linear*. In a linear scheme, the secret is viewed as an element of a finite field, and the shares are obtained by applying a linear mapping to the secret and several independent random field elements. For example, the schemes of [9], [25], [2], [3], [4], [51], [6] are all linear, and the ideal schemes implied by the sufficient condition of [5], [11] are linear. A generalization of linear schemes are multi-linear schemes of van Dijk [8], where the secret is a vector of elements from a finite field, and the shares are obtained by applying a linear mapping to the coordinates of a vector representing the secret and several independent random field elements. Simonis and Ashikhmin [39] have given an example of an access structure that has an ideal multilinear secret-sharing scheme, but does not have an ideal linear secret-sharing scheme. Beimel and Ishai [52] have discussed compositions of linear schemes over different fields, which they call quasi-linear schemes. Beimel and Weinreb [53] have proved that there are quasi-linear schemes that are superpolynomially more efficient than linear schemes. The only known secret-sharing schemes that are neither multi-linear nor quasi-linear have been presented in [52]; however these schemes are not ideal.

C. Organization

In Section II we present basic definitions of secret-sharing schemes and matroids, and discuss the relations between them. In Section III we prove some technical lemmas concerning weakly-private secret-sharing schemes; these lemmas are used to prove our main result. In Section IV we first reprove the known result that any access structure induced by the Vamos matroid is non-ideal, and then strengthen this result. In Section V 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 Section VI we give an example of a non-ideal access structure that is nearly ideal. Finally, in Section VII we present some concluding remarks and describe related open problems.

II. Preliminaries

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

A. Secret Sharing

Definition 2.1 (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 $B \subseteq C$ 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.

Definition 2.2 (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 each 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.

It is important to stress that the description of the scheme, namely, $\langle \{M_s\}_{s\in K}, \{\Pi_s\}_{s\in K}\rangle$, is public knowledge. The uncertainty that an unauthorized subset of participants has about the secret is an outcome of the uncertainty of the dealer's choice of the row $r \in M_s$.

Sometimes it is convenient to represent $\{M_s\}_{s\in K}$ as one matrix M, defined as follows

$$M = \left\{ \langle s, r_1, \ldots, r_{|P|}\rangle : \begin{array}{c} s \in K \text{ and } \langle r_1, \ldots, r_{|P|}\rangle \\ \text{is a vector in } M_s \end{array} \right\}. \quad (1)$$

We think of the left-most column of M as the dealer's column, and denote it p_0. For any $A \subseteq P$, denote by $K(A)$ the set of distinct rows in the restriction of M to the columns in A. That is, $K(A)$ is the set of vectors of shares the participants in A can receive. Given $\mathbf{K_A} \in K(A)$, denote by $K(p_0|\mathbf{K_A})$ the set of possible values of the secret given that the participants in A receive the vector of shares $\mathbf{K_A}$.

Definition 2.3 (Secret-Sharing Scheme): We say that a distribution scheme Σ is a secret-sharing scheme realizing an access structure $\mathcal{A} \subseteq 2^P$ if the following two requirements hold:

Correctness: The secret s can be reconstructed by any authorized set of participants. That is, for any $A \in \mathcal{A}$ and $\mathbf{K_A} \in K(A)$,

$$|K(p_0|\mathbf{K_A})| = 1. \quad (2)$$

Intuitively, if A is an authorized set of participants, then, for any vector of shares $\mathbf{K_A} \in K(A)$ that the participants in A receive, there exists exactly one secret $s \in K$ that the dealer could choose in order to distribute the shares in $\mathbf{K_A}$ (however, there can be more than one row that the dealer could choose).

Privacy: Every unauthorized set can learn nothing about the secret (in the information theoretic sense) from their shares. Formally, for every set $A \notin \mathcal{A}$, for every two secrets $s_1, s_2 \in K$, and for every $\mathbf{K_A} \in K(A)$:

$$\Pr_{r_1}[M_{s_1}[r_1, A] = \mathbf{K_A}] = \Pr_{r_2}[M_{s_2}[r_2, A] = \mathbf{K_A}], \quad (3)$$

where the rows r_1 and r_2 are chosen from the probability distributions Π_{s_1} and Π_{s_2} respectively, and $M_{s_i}[r_j, A]$ is the restriction of the row r_j in M_{s_i} to the columns in A.
Sometimes we will denote the domain of secrets by $K(p_0)$, the share domain of the dealer. However, the dealer is not a participant.

Example 2.4: As an example for our definitions, we consider Shamir's threshold scheme [9]. Denote $P = \{1, \ldots, n\}$, let $t \le n$, and define the access structure $\mathcal{A}_t = \{A \subseteq P : |A| \ge t\}$. We choose some prime number $q > n$, 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 Q of degree $t-1$ over $\mathbb{F}_q$ such that $Q(0) = s$. The dealer then distributes to each participant $p_i \in P$ the share $Q(i)$. 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 Q of degree $t-1$, therefore, it can determine Q, and it can calculate $Q(0)$. If an unauthorized subset of participants – a subset of cardinality less than t – wants to reconstruct the secret, then for any $s \in \{0, \ldots, q-1\}$ there is an equal number of polynomials through the points given to the participants and the point $(0, s)$. Thus, this unauthorized subset has no information about the secret.

In such a scheme, for each secret $s \in \mathbb{F}_q$, the matrix M_s contains q^{t-1} rows; a row $\langle Q(1), \ldots, Q(n)\rangle$ for every polynomial Q of degree $t-1$ over $\mathbb{F}_q$ such that $Q(0) = s$. The matrix M contains q^t rows, a row for every polynomial Q of degree $t-1$ over $\mathbb{F}_q$. The distribution Π_s is the uniform distribution on the rows of M_s.

Karnin et al. [10] have showed that the size of the domain of shares of each participant is at least the size of the domain of secrets. This motivates the definition of ideal secret-sharing.

Definition 2.5 (Ideal Access Structures): A secret-sharing scheme with domain of secrets K is *ideal* if the domain of shares of each user is K. An access structure $\mathcal{A}$ is *k-ideal* if there exists an ideal secret-sharing scheme realizing it with domain of secrets K of size k. An access structure $\mathcal{A}$ is *ideal* if it is k-ideal for some $k \ge 2$.

We next give a relaxed definition of secret-sharing scheme, which we call a *weakly-private secret-sharing scheme*. In a weakly-private secret-sharing scheme, a weaker condition for privacy is required. While in the previous definition 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.

Definition 2.6 (Weakly-Private Secret-Sharing Scheme): Let P be a set of participants, and let K be a finite set of secrets. A *weakly-private 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.

We say that M is a *weakly-private* 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, that is, for any $A \in \mathcal{A}$ and $\mathbf{K_A} \in K(A)$,

$$|K(p_0|\mathbf{K_A})| = 1. \tag{4}$$

Weak Privacy: Given a vector of shares of an unauthorized set of participants, none of the values of the secret can be ruled out. That is, for any $A \notin \mathcal{A}$ and $\mathbf{K_A} \in K(A)$

$$K(p_0|\mathbf{K_A}) = K(p_0). \tag{5}$$

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

Remark 2.7: If $\Sigma = \langle \{\mathcal{M}_s\}_{s\in K}, \{\Pi_s\}_{s\in K}\rangle$ is a secret-sharing scheme with M defined as in (1), then M is a weakly-private secret-sharing scheme. That is, every secret-sharing scheme implies a weakly-private secret-sharing scheme. Thus, for proving lower bounds on the size of shares it suffices to consider weakly-private secret-sharing schemes.

We next give some notations concerning weakly-private secret-sharing schemes. Given two sets of participants $A, B \subseteq P \cup \{p_0\}$ and a vector of shares $\mathbf{K_B} \in K(B)$, denote by $K(A|\mathbf{K_B})$ the set of vectors 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. We say that $\mathbf{K_A}$ *coincides* with $\mathbf{K_B}$ if $\mathbf{K_A} \in K(A|\mathbf{K_B})$ (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 $A, B_1, \ldots, B_\ell \subseteq P \cup \{p_0\}$, 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 $1 \leq i \leq \ell$. Given two sets of participants $A, B \subseteq P \cup \{p_0\}$, and a set $X_B \subseteq K(B)$ we denote

$$K(A|X_B) \stackrel{\text{def}}{=} \bigcup_{\mathbf{K_B} \in X_B} K(A|\mathbf{K_B}).$$

Throughout the paper it will be clear from the context which columns (participants) does the conditioning value $\mathbf{K_B}$ in the notation $K(A|\mathbf{K_B})$ refer to.

B. 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 [14], [54].

Definition 2.8 (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 graph and $\mathcal{C}$ be the collection of simple cycles in G. Then, $(E, \mathcal{C})$ is a matroid.

Definition 2.9 (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 $A \subseteq V$, denoted $\mathrm{rank}(A)$, is the size of a maximal independent subset of A.

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 [14].

Lemma 2.10: If C_1, C_2 are distinct members of $\mathcal{C}$ and $x \in C_1 \cap C_2$, then for any element $y \in C_1 \setminus C_2$ there exists $C_3 \in \mathcal{C}$ such that $y \in C_3$ and $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$.

Definition 2.11 (Connected Matroid): A matroid is connected if for every pair of distinct elements x and y there is a circuit containing x and y.

The following lemma, whose proof can be found in [14], [54], states that if a matroid is connected then the set of circuits through a fixed point uniquely determines the matroid.

Lemma 2.12: 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:

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

and

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

In other words, $c \in D_e(C_1, C_2)$ if $c \in C_1 \cup C_2$ and there exists a circuit $C_3 \in \mathcal{C}_e$ such that $C_3 \subseteq (C_1 \cup C_2) \setminus \{c\}$. 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 $\mathcal{C}_e$.

The following example demonstrates this lemma.

Example 2.13: Let $\mathcal{M} = \langle V, \mathcal{C}\rangle$ be a matroid, with $V = \{a, b, c, d, e\}$ and

$$\mathcal{C} = \{\{a, d, e\}, \{b, c, d\}, \{a, b, c, e\}\}.$$

Thus, $\mathcal{C}_e = \{\{a, d, e\}, \{a, b, c, e\}\}$. Consider the circuit $\{b, c, d\}$, which does not contain e. Then this circuit is obtained by calculating

$$J_e(\{a, d, e\}, \{a, b, c, e\}) = \{a, e\},$$

and then

$$D_e(\{a, d, e\}, \{a, b, c, e\}) = \{a, b, c, d, e\} \setminus \{a, e\} = \{b, c, d\}.$$

C. Matroids and Secret Sharing

Definition 2.14: 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

$$\mathcal{A} \stackrel{\text{def}}{=} \left\{ A : \begin{array}{l} \text{There exists } C_0 \in \mathcal{C} \text{ such that } p_0 \in C_0 \\ \text{and } C_0 \setminus \{p_0\} \subseteq A \end{array} \right\}.$$

That is, a set A is a minterm of $\mathcal{A}$ if by adding p_0 to A, 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 $\mathcal{A}$.

A corollary of Lemma 2.12 is that if a connected access structure has an appropriate matroid, then this matroid is unique. Of course, not every access structure has an appropriate matroid. If a connected access structure has an appropriate matroid, then this matroid is also connected.

We now quote some results concerning weakly-private secret-sharing schemes. Since every secret-sharing scheme is, in particular, a weakly-private 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 2.15 ([11]): If an access structure is weakly ideal, then it has an appropriate matroid.

Remark 2.16: As mentioned above, by Lemma 2.12 for a connected access structure the appropriate matroid is unique.

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 2.17 ([11]): Assume that a connected access structure $\mathcal{A} \subseteq 2^P$ is weakly ideal, and let $\langle P \cup \{p_0\}, \mathcal{C} \rangle$ be its appropriate connected matroid where $p_0 \notin P$. Let M be an ideal weakly-private 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 2.18: By Lemma 2.17, if M is a weakly ideal secret-sharing scheme for $\mathcal{A}$, then M is an ideal secret-sharing scheme for $\mathcal{A}$, where the dealer chooses the random row with uniform distribution. That is, any weakly ideal secret-sharing scheme induces an ideal secret-sharing scheme. For every $s \in K$ define M_s as the set of rows of M where the value of p_0 is s, restricted to P, and Π_s as the uniform distribution on the rows of M_s.

Remark 2.19: Let $\mathcal{A}$ be a weakly ideal access structure and $\mathcal{M} = \langle V, \mathcal{C} \rangle$ be its appropriate matroid. By Definition 2.14, we can fix any $p \in V$ and get an induced access structure

$$\mathcal{A}_p \stackrel{\text{def}}{=} \left\{ A : \begin{array}{l} \text{There exists } C \in \mathcal{C} \text{ such that } p \in C \\ \text{and } C \setminus \{p\} \subseteq A \end{array} \right\}.$$

Another corollary of Lemma 2.17 is that if M is a weakly-private secret-sharing scheme realizing $\mathcal{A}$, then M is a weakly-private secret-sharing scheme realizing $\mathcal{A}_p$ for *any* $p \in V$ as explained below: On one hand, if A is a minimal authorized set of $\mathcal{A}_p$, then $A \cup \{p\}$ is a circuit of $\mathcal{M}$, therefore, $\mathrm{rank}(A \cup \{p\}) = \mathrm{rank}(A) = |A|$. Hence, by Lemma 2.17, $|K(p|\mathbf{K_A})| = 1$ for every $\mathbf{K_A}$. On the other hand, if A is an unauthorized set of $\mathcal{A}_p$, then it can be shown that $\mathrm{rank}(A \cup \{p\}) = \mathrm{rank}(A) + 1$. Hence, by Lemma 2.17, $|K(p|\mathbf{K_A})| = K = K(p)$ for every $\mathbf{K_A}$.

Example 2.20: Consider the threshold access structure $\mathcal{A}_t$ and Shamir's scheme [9] realizing it (see Example 2.4). 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 2.17.

III. Secret-Sharing Schemes Realizing Matroid-Induced Access Structures

We now prove some lemmas concerning weakly-private secret-sharing schemes and matroid-induced access structures with arbitrary size of shares domain. In the rest of this section, denote the dealer p_0, and define $K \stackrel{\text{def}}{=} K(p_0)$ (that is, K is the domain of secrets).

The next lemma, which will be used throughout this paper, gives a lower bound on the size of the shares of certain subsets of participants. This lemma holds for every access structure.

Lemma 3.1: 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 $A \cup B \setminus \{b\} \notin \mathcal{A}$. Then, $|K(b|\mathbf{K_A})| \geq |K|$ for any $\mathbf{K_A} \in K(A)$.

Proof: Since $A \cup B \setminus \{b\}$ is unauthorized, by (5), for any $\mathbf{K_{A \cup B \setminus \{b\}}} \in K(A \cup B \setminus \{b\})$,

$$K(p_0|\mathbf{K_{A\cup B\setminus\{b\}}}) = K. \tag{6}$$

Since $A \cup B$ is authorized, by (4), for any $\mathbf{K_{A\cup B}} \in K(A \cup B)$,

$$|K(p_0|\mathbf{K_{A\cup B}})| = 1. \tag{7}$$

Furthermore, for any $\mathbf{K_{A\cup B\setminus\{b\}}} \in K(A \cup B \setminus \{b\})$,

$$K(p_0|\mathbf{K_{A\cup B\setminus\{b\}}}) = \bigcup_{\mathbf{K_{\{b\}}} \in K(b|\mathbf{K_{A\cup B\setminus\{b\}}})} K(p_0|\mathbf{K_{A\cup B\setminus\{b\}}}, \mathbf{K_{\{b\}}}).$$

Since, by (7), every set in this union is of size one, and since, by (6), 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 restriction of the vector $\mathbf{K_{A\cup B\setminus\{b\}}}$ to the shares of the participants in A. Since $K(b|\mathbf{K_{A\cup B\setminus\{b\}}}) \subseteq K(b|\mathbf{K_A})$, the lemma follows. ■

Lemma 3.2: Let $\mathcal{M} = \langle P \cup \{p_0\}, \mathcal{C} \rangle$ be the appropriate matroid of a connected access structure $\mathcal{A} \subseteq 2^P$, and let $C \in \mathcal{C}$ be a circuit 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 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 $|K(A|\mathbf{K_D})| \geq |K| \cdot |K(A \setminus \{a\}|\mathbf{K_D})|$ for some $a \in A$. We consider two cases, first we assume that $p_0 \in A$, and then we assume that $p_0 \notin A$.

If $p_0 \in A$, then $A \cup D \setminus \{p_0\}$ is a proper subset of the minterm $C \setminus \{p_0\}$, thus, $A \cup D \setminus \{p_0\}$ is unauthorized. Now, by (5), $|K(p_0|\mathbf{K_{A\setminus\{p_0\}}},\mathbf{K_D})| = |K|$ for any $\mathbf{K_{A\setminus\{p_0\}}} \in K(A\setminus\{p_0\})$. Therefore, since every vector in $K(A|\mathbf{K_D})$ can be written as $\langle x,\mathbf{K_{A\setminus\{p_0\}}}\rangle$ for a unique $\mathbf{K_{A\setminus\{p_0\}}} \in K(A\setminus\{p_0\}|\mathbf{K_D})$ and $x \in K(p_0|\mathbf{K_{A\setminus\{p_0\}}},\mathbf{K_D})$,

$$\begin{aligned}
&|K(A|\mathbf{K_D})| \\
&= \sum_{\mathbf{K_{A\setminus\{p_0\}}}\in K(A\setminus\{p_0\}|\mathbf{K_D})} \big|K(p_0|\mathbf{K_{A\setminus\{p_0\}}},\mathbf{K_D})\big| \\
&= |K|\cdot|K(A\setminus\{p_0\}|\mathbf{K_D})|.
\end{aligned}$$

This concludes the case $p_0 \in A$ by taking $a = p_0$.

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 3.1, $|K(a|\mathbf{K_{A\setminus\{a\}}},\mathbf{K_D})| \geq |K|$ for any $\mathbf{K_{A\setminus\{a\}}} \in K(A\setminus\{a\})$. It follows that $|K(A|\mathbf{K_D})| \geq |K|\cdot|K(A\setminus\{a\}|\mathbf{K_D})|$, which concludes the proof. ■

In the ideal case, by Lemma 2.17, we get an upper bound on the share domain of every subset of participants that forms a circuit in the appropriate matroid (including circuits that do not contain the dealer). In the non-ideal case we cannot apply Lemma 2.17. Lemma 3.5 will be used to overcome this difficulty. To prove Lemma 3.5, we need the following claim. This claim offers an upper bound on the number of ordered pairs of points that have the same image.

Claim 3.3: Let m be an integer, M_1, M_2 be two sets of size at most m, and K be a set of size $k \leq m$. Let f_i be a function from M_i onto K for $i \in \{1,2\}$. Then, $|\{\langle x_1,x_2\rangle : x_1\in M_1, x_2\in M_2, f_1(x_1)=f_2(x_2)\}| \leq k-1+(m-k+1)^2$.

Proof: Without loss of generality, assume $K=\{1,2,\ldots,k\}$. For $1\leq i\leq k$ define

$$a_i \stackrel{\text{def}}{=} |f_1^{-1}(i)| \text{ and } b_i \stackrel{\text{def}}{=} |f_2^{-1}(i)|.$$

Then,

$$\sum_{i=1}^{k} a_i \leq m \quad\text{and}\quad \sum_{i=1}^{k} b_i \leq m,$$

since both these sums are the size of the domains of the functions. Moreover, since the functions f_1 and f_2 are onto K, we have $a_i \geq 1$ and $b_i \geq 1$ for all $1\leq i\leq k$. Thus, in particular, $a_1 \leq m-k+1$. From the definitions

$$\begin{aligned}
&|\{\langle x_1,x_2\rangle : x_1\in M_1, x_2\in M_2, f_1(x_1)=f_2(x_2)\}| \\
&= \sum_{i=1}^{k} |\{\langle x_1,x_2\rangle : f_1(x_1)=f_2(x_2)=i\}| \\
&= \sum_{i=1}^{k} a_i b_i.
\end{aligned}$$

Assume without loss of generality that a_1 is maximal in $a_1,a_2,\ldots,a_k$. Then,

$$\begin{aligned}
\sum_{i=1}^{k} a_i b_i &= \sum_{i=1}^{k}\big(a_i + a_i(b_i-1)\big) \\
&\leq \sum_{i=1}^{k}\big(a_i + a_1(b_i-1)\big) \\
&= a_1\Big(\sum_{i=1}^{k}(b_i-1)\Big) + \sum_{i=1}^{k} a_i \\
&= a_1\Big(\sum_{i=1}^{k} b_i - k\Big) + \sum_{i=1}^{k} a_i \\
&\leq a_1(m-k)+m \\
&\leq (m-k+1)(m-k)+m \\
&= k-1+(m-k+1)^2.
\end{aligned}$$

■

Example 3.4: We note that Claim 3.3 is tight as shown in this simple example. Let $M_1 = M_2 = \{1,\ldots,m\}$ and define f_1 and f_2 as follows: $f_1(i)=f_2(i)=i$ for $1\leq i\leq k-1$ and $f_1(i)=f_2(i)=k$ for $k\leq i\leq m$. Thus,

$$\begin{aligned}
&|\{\langle x_1,x_2\rangle : x_1\in M_1, x_2\in M_2, f_1(x_1)=f_2(x_2)\}| \\
&= |\{\langle i,i\rangle : 1\leq i\leq k-1\}| \\
&\quad + |\{\langle x_1,x_2\rangle : k\leq x_1\leq m, k\leq x_1\leq m\}| \\
&= k-1+(m-k+1)^2.
\end{aligned}$$

Lemma 3.5: Let $\mathcal{A}$ be an access structure. Let $Z\subseteq P$ and $b_1,b_2\in P$ such that $b_1\neq b_2$ and $Z\notin\mathcal{A}$, $Z\cup\{b_1\}\in\mathcal{A}$, and $Z\cup\{b_2\}\in\mathcal{A}$. Consider a weakly-private 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 $|K(b_1,b_2|\mathbf{K_Z})| \leq k-1+(m-k+1)^2$ for any $\mathbf{K_Z}\in K(Z)$.

Proof: Fix some $\mathbf{K_Z}\in K(Z)$. Since $Z\cup\{b_1\}\in\mathcal{A}$, given $\mathbf{K_Z}$ any $\mathbf{K_{b_1}}\in K(b_1|\mathbf{K_Z})$ determines the secret. Moreover, since $Z\notin\mathcal{A}$, given $\mathbf{K_Z}$ any value of the secret is possible. Therefore, $\mathbf{K_Z}$ induces a function from $K(b_1|\mathbf{K_Z})$ onto $K(p_0)$ (where p_0 is the dealer). Denote this function by f_1. Similarly $\mathbf{K_Z}$ also induces a function from $K(b_2|\mathbf{K_Z})$ onto $K(p_0)$. Denote this function by f_2.

Given $\mathbf{K_Z}$, consider any $\langle x_1,x_2\rangle\in K(b_1,b_2|\mathbf{K_Z})$. Since $\langle x_1,x_2\rangle\in K(b_1,b_2|\mathbf{K_Z})$, there is a row r in M that gives to the participants in Z the values in $\mathbf{K_Z}$, and to b_1,b_2 the values x_1,x_2 respectively. But then $M[r,p_0]=f_1(x_1)=f_2(x_2)$. Informally, given $\mathbf{K_Z}$, the shares x_1 and x_2 must "agree" on the secret. Thus, $f_1(x_1)=f_2(x_2)$ for every $\langle x_1,x_2\rangle\in K(b_1,b_2|\mathbf{K_Z})$. Since both f_1 and f_2 are onto $K(p_0)$, and since the domain of both functions is bounded by m, Claim 3.3 implies that $|K(b_1,b_2|\mathbf{K_Z})|\leq k-1+(m-k+1)^2$. ■

E.g., in any ideal scheme (where $k=m$), under the conditions of the lemma, $|K(b_1,b_2|\mathbf{K_Z})|=k$. If $m\leq k+\sqrt{k}-1$, then $|K(b_1,b_2|\mathbf{K_Z})|<2k$.

IV. 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 [15] is the smallest known matroid that is non-representable over any field, and is also non-algebraic (for more details on these notions see [14], [54]).

Definition 4.1 (The Vamos Matroid): The Vamos matroid $\mathcal{V}$ is defined on the set $V = \{v_1, v_2, \dots, v_8\}$, 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 4.1 are circuits, a fact that will be used later. Seymour [12] has proved that any access structure induced by the Vamos matroid is non-ideal. First, we will prove Seymour's result in a simplified way, then, in Section IV-B, we will generalize it.

Definition 4.2 (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 4.3: We next give examples of authorized and unauthorized sets in V_8.

(1) The set $\{v_3, v_4, v_7\}$ is authorized, since $\{v_3, v_4, v_7, v_8\}$ is a circuit.
(2) The circuit $\{v_1, v_2, v_3, v_4\}$ is unauthorized, since the set $\{v_1, v_2, v_3, v_4, v_8\}$ does not contain a circuit that contains v_8. To check this, 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.
(3) The set $\{v_1, v_2, v_3, v_4, v_5\}$ is authorized, since the set $\{v_1, v_2, v_3, v_5, v_8\}$ is a circuit (as well as the sets $\{v_1, v_2, v_4, v_5, v_8\}$, $\{v_1, v_3, v_4, v_5, v_8\}$, and $\{v_2, v_3, v_4, v_5, v_8\}$).

A. The Vamos Access Structure is Non-Ideal

The following theorem is the main result in [12]. The proof we present here is somewhat simpler than the proof in [12]. In Section IV-B we strengthen this result; the purpose of presenting this proof is to explain the ideas of the stronger result.[2]

Theorem 4.4: The access structure V_8 is non-ideal.

Proof: Assume towards contradiction that the access structure V_8 has an ideal secret-sharing scheme. In particular, it has a weakly ideal secret-sharing scheme. Let M be a matrix, with entries from K, realizing it. The rank of $\{v_1, v_2, v_7, v_8\}$ in the Vamos matroid is 4, thus, by Lemma 2.17, the size of the domain of shares of $\{v_1, v_2, v_7, v_8\}$, namely $|K(v_1, v_2, v_7, v_8)|$, is $|K|^4$. Since $K(v_1, v_2) = K(v_7, v_8) = K^2$, for every $\langle x_1, x_2\rangle \in K(v_1, v_2)$ we have

$$|K(v_7, v_8|x_1, x_2)| = |K|^2. \tag{8}$$

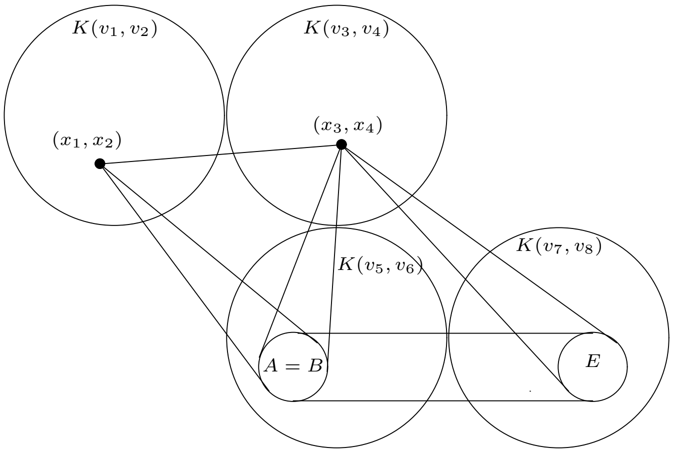

Fig. 1. Sets in the proof of Theorem 4.4. Circles denote sets, and points denote elements in the sets. Two elements are connected if they coincide. A line connects an element and a subset, if the subset is the set of all elements that coincide with the element. For example, $\langle x_1, x_2\rangle$ and A are connected with lines because A is the set of elements in $K(v_5, v_6)$ that coincide with $\langle x_1, x_2\rangle$. Likewise, A and E are connected, because for every element in A, the set E is the set of elements in $K(v_7, v_8)$ that coincide with the element, and vice versa.

However, we will prove that from restrictions implied by Lemma 2.17, Equation (8) does not hold, thus, there cannot be an ideal scheme realizing V_8. Fix arbitrary $\langle x_1, x_2\rangle \in K(v_1, v_2)$, and define

$$A \stackrel{\text{def}}{=} K(v_5, v_6|x_1, x_2)$$

(for an illustration see Figure 1). Furthermore, fix arbitrary $\langle x_3, x_4\rangle \in K(v_3, v_4|x_1, x_2)$ and define

$$B \stackrel{\text{def}}{=} K(v_5, v_6|x_3, x_4).$$

Notice that A and B depend on the choice of x_1, x_2. The outline of the proof is as follows. First, we will show in Claim 4.5 that $|A| = |B| = |K|$, and that this fact implies that $A = B$. Define

$$E \stackrel{\text{def}}{=} K(v_7, v_8|x_3, x_4).$$

By symmetric arguments, it will be showed in (13) that E is the set $K(v_7, v_8|y_5, y_6)$ for any $\langle y_5, y_6\rangle \in A$, therefore $K(v_7, v_8|A) = \cup_{y_5, y_6 \in A} K(v_7, v_8|y_5, y_6) = E$. That is, the possible shares of v_7, v_8 given that the shares of v_5, v_6 are in A, are exactly the possible shares of v_7, v_8 given that the shares of v_3, v_4 are the fixed shares x_3, x_4. Furthermore, it will be proved in (14) that $|E| = |K|$. The set $K(v_7, v_8|x_1, x_2)$ is contained in the set $K(v_7, v_8|A)$, since A is the set of shares of v_5, v_6 possible with x_1, x_2. Thus, $|K(v_7, v_8|x_1, x_2)| \leq |K(v_7, v_8|A)| = |E| = |K|$ in a contradiction to (8).

Claim 4.5: A=B.

Proof: Since $\mathrm{rank}(\{v_1, v_2\}) = 2$, by Lemma 2.17, $K(v_1, v_2) = K^2$. Since $\mathrm{rank}(\{v_1, v_2, v_3\}) = 3$,

[1] There are two non-isomorphic access structures induced by the Vamos matroid. The access structure V_8 is isomorphic to the access structures 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.

[2] While in [12] Seymour has proved that any access structure induced by the Vamos matroid is non-ideal, here we prove this for a specific access structure induced by it. But, as implied by Remark 2.19, this yields that any access structure induced by the Vamos matroid is non-ideal.

by Lemma 2.17, $K(v_1, v_2, v_3) = K^3$ and therefore $K(v_3|y_1, y_2) = K$ for every $\langle y_1, y_2\rangle \in K(v_1, v_2) = K^2$. Since $\text{rank}(v_1, v_2, v_3, v_4) = 3$ too, it follows that $|K(v_4|y_1, y_2, y_3)| = 1$ for every $\langle y_1, y_2, y_3\rangle \in K(v_1, v_2, v_3) = K^3$. This implies, in particular, that for every $\langle y_1, y_2\rangle \in K(v_1, v_2) = K^2$

$$|K(v_3, v_4|y_1, y_2)| = |K|. \tag{9}$$

By symmetry, since $\text{rank}(\{v_1, v_2\}) = 2$ and $\text{rank}(\{v_1, v_2, v_5\}) = \text{rank}(\{v_1, v_2, v_5, v_6\}) = 3$, for every $\langle y_1, y_2\rangle \in K(v_1, v_2) = K^2$,

$$|K(v_5, v_6|y_1, y_2)| = |K|, \tag{10}$$

and, since $\text{rank}(\{v_3, v_4\}) = 2$ and $\text{rank}(\{v_3, v_4, v_5\}) = \text{rank}(\{v_3, v_4, v_5, v_6\}) = 3$, for every $\langle y_3, y_4\rangle \in K(v_3, v_4) = K^2$

$$|K(v_5, v_6|y_3, y_4)| = |K|. \tag{11}$$

Since $\text{rank}(v_1, v_2, v_3, v_4, v_5, v_6) = 4$, by Lemma 2.17,

$$|K(v_1, v_2, v_3, v_4, v_5, v_6)| = |K|^4. \tag{12}$$

By (9) and (10), $|K(v_3, v_4, v_5, v_6|y_1, y_2)| \le |K|^2$ for every $\langle y_1, y_2\rangle \in K^2$. Since $K(v_1, v_2) = K^2$, Equation (12) implies that equality holds here, that is, $|K(v_3, v_4, v_5, v_6|y_1, y_2)| = |K|^2$ for every $\langle y_1, y_2\rangle \in K^2$. Thus, for every $\langle y_1, y_2\rangle \in K(v_1, v_2)$, every $\langle y_3, y_4\rangle \in K(v_3, v_4|y_1, y_2)$, and every $\langle y_5, y_6\rangle \in K(v_5, v_6|y_1, y_2)$, we have $\langle y_3, y_4, y_5, y_6\rangle \in K(v_3, v_4, v_5, v_6|y_1, y_2)$. That is, if the vectors $\langle y_3, y_4\rangle$ and $\langle y_5, y_6\rangle$ are possible shares for $\{v_3, v_4\}$ and $\{v_5, v_6\}$ respectively given that the shares of $\{v_1, v_2\}$ are $\langle y_1, y_2\rangle$, then $\langle y_3, y_4, y_5, y_6\rangle$ is a possible vector of shares for $\{v_3, v_4, v_5, v_6\}$ given $\langle y_1, y_2\rangle$. In particular, since $\langle x_3, x_4\rangle \in K(v_3, v_4|x_1, x_2)$,

$$\begin{aligned} A &= K(v_5, v_6|x_1, x_2) \\ &= K(v_5, v_6|x_1, x_2, x_3, x_4) \\ &\subseteq K(v_5, v_6|x_3, x_4) = B. \end{aligned}$$

Since, by (10) and (11), both these sets are of size $|K|$, we conclude that $A = B$. ■ (of Claim 4.5)

Both the restrictions of the Vamos matroid to $\{v_1, v_2, v_3, v_4, v_5, v_6\}$ and to $\{v_3, v_4, v_5, v_6, v_7, v_8\}$ are isomorphic. By symmetric arguments, for any $\langle y_5, y_6\rangle \in K(v_5, v_6|x_3, x_4)$ and $\langle y_7, y_8\rangle \in K(v_7, v_8|x_3, x_4)$, we have $\langle y_5, y_6, y_7, y_8\rangle \in K(v_5, v_6, v_7, v_8|x_3, x_4)$. In particular, it implies that given any $\langle y_5, y_6\rangle \in A$, we have $K(v_7, v_8|y_5, y_6) = K(v_7, v_8|x_3, x_4)$, from which we conclude that

$$K(v_7, v_8|A) = \bigcup_{y_5, y_6 \in A} K(v_7, v_8|y_5, y_6) = E. \tag{13}$$

By the same arguments as in the proof of (9), since $\text{rank}(\{v_3, v_4\}) = 2$ and $\text{rank}(\{v_3, v_4, v_7\}) = \text{rank}(\{v_3, v_4, v_7, v_8\}) = 3$,

$$|E| = |K|. \tag{14}$$

As argued above, this completes the proof. ■

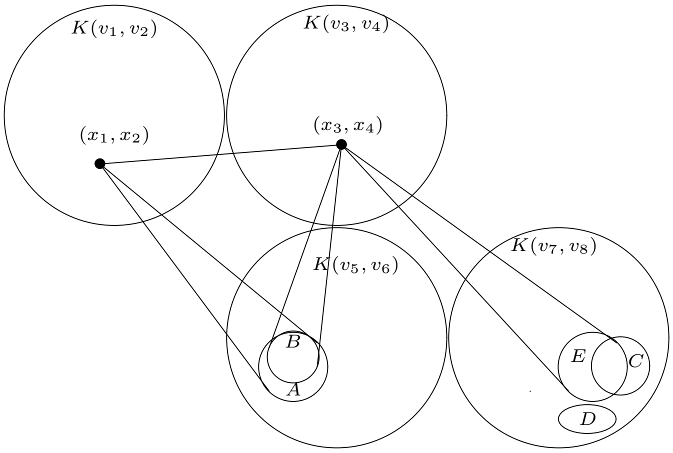

Fig. 2. Sets in the proof of Theorem 4.9.

B. Stronger Bounds on the Vamos Access Structure

For a given secret-sharing scheme realizing V_8, assume $|K(v_8)| = k$, and $|K(v_i)| \le m$ for $1 \le i \le 7$, 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 [10], 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, $m \ge k$. In the previous section we proved that $m \ge k + 1$. That is, the access structure is not ideal. We now prove a stronger lower bound on m.

The framework of the proof is similar to the proof of Theorem 4.4, but because we allow the size of the domain of the shares to be larger than k, we have to consider some more details. There are two main difficulties we have to consider. First, Lemma 2.17 does not apply to non-ideal schemes. Instead, we use Lemmas 3.1, 3.2, and 3.5 to bound the cardinality of the domain of the shares. Second, sets that in the previous proof were equal, due to cardinality constraints, are not necessarily equal here. Instead, we will show a large intersection between them. 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 3.2 the size of this set is at least k^2, and thus we achieve a lower bound on m.

Fix some arbitrary $\langle x_1, x_2\rangle \in K(v_1, v_2)$, and define $A \stackrel{\text{def}}{=} K(v_5, v_6|x_1, x_2)$, as in the proof of Theorem 4.4 (see Figure 2). 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.

Lemma 4.6: $|A| \le m^{\frac{k-1+(m-k+1)^2}{k}}$.

Proof: Let x_3 be an arbitrary element 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, the set $\{v_1, v_2, v_3, v_5\}$ 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 3.5 (with $Z = \{v_1, v_2, v_3\}$, $b_1 = v_5$, and $b_2 = v_6$),

$$|K(v_5, v_6|x_1, x_2, x_3)| \leq k - 1 + (m - k + 1)^2. \tag{15}$$

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

$$K(v_3, v_5, v_6|x_1, x_2) = \bigcup_{x_3 \in K(v_3|x_1,x_2)} \left\{ \begin{array}{l} \langle x_3, y_5, y_6 \rangle : \\ \langle y_5, y_6 \rangle \in K(v_5, v_6|x_1, x_2, x_3) \end{array} \right\}.$$

That is, we count all the x_3's that coincide with $\langle x_1, x_2 \rangle$, and for each such x_3 we count all the $\langle y_5, y_6 \rangle$'s that coincide with $\langle x_1, x_2, x_3 \rangle$. By (15), the size of each set in the union is at most $k - 1 + (m - k + 1)^2$, and since $|K(v_3|x_1, x_2)| \leq |K(v_3)| \leq m$, there are at most m sets in the union. Therefore,

$$|K(v_3, v_5, v_6|x_1, x_2)| \leq m \left(k - 1 + (m - k + 1)^2\right). \tag{16}$$

On the other hand,

$$K(v_3, v_5, v_6|x_1, x_2) \tag{17}$$
$$= \bigcup_{\langle y_5,y_6 \rangle \in A} \left\{ \begin{array}{l} \langle x_3, y_5, y_6 \rangle : \\ \langle x_3 \rangle \in K(v_3|x_1, x_2, y_5, y_6) \end{array} \right\}. \tag{18}$$

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 3.1 each set in this union is of size at least k. Notice that all these sets are disjoint. Thus, by (16), there are at most $\frac{m}{k}(k - 1 + (m - k + 1)^2)$ sets in this union. We conclude that

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

■

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 consists of the shares $\{v_5, v_6\}$ can receive given $\langle x_1, x_2 \rangle$, and the set B consists of 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 the set $K(v_7, v_8|A)$, 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

$$D \stackrel{\text{def}}{=} K(v_7, v_8|A \setminus B) = \bigcup_{\langle y_5,y_6 \rangle \in A \setminus B} K(v_7, v_8|y_5, y_6).$$

Lemma 4.7: $|C| + |D| \leq m - k^2 + \left(\frac{k-1+(m-k+1)^2}{k}\right) m^2$.

Proof: First we show that $|C| \leq |B|(m - k) + m$. Define $E \stackrel{\text{def}}{=} K(v_7, v_8|x_3, x_4)$. Informally, we will show that E is small and that 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, by (4), given $\langle x_3, x_4 \rangle$ any $y_7 \in K(v_7|x_3, x_4)$ determines the secret, therefore

$$|E| = |K(v_7, v_8|x_3, x_4)| = |K(v_7|x_3, x_4)| \leq |K(v_7)| \leq m. \tag{19}$$

Since $\{v_3, v_4, v_5, v_6\}$ is unauthorized, by (5), 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, for any $\langle y_5, y_6 \rangle \in B$,

$$|K(v_7, v_8|x_3, x_4, y_5, y_6)| \geq k. \tag{20}$$

For any $\langle y_5, y_6 \rangle \in B$, clearly $K(v_7, v_8|x_3, x_4, y_5, y_6) \subseteq E$ and $K(v_7, v_8|x_3, x_4, y_5, y_6) \subseteq K(v_7, v_8|y_5, y_6)$. In view of the last two containments, $K(v_7, v_8|x_3, x_4, y_5, y_6) \subseteq K(v_7, v_8|y_5, y_6) \cap E$. Thus, by (20), for any $\langle y_5, y_6 \rangle \in B$

$$|K(v_7, v_8|y_5, y_6) \cap E| \geq k. \tag{21}$$

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 (4), given $\langle y_5, y_6 \rangle$ any $y_7 \in K(v_7|y_5, y_6)$ determines the secret, therefore for any $\langle y_5, y_6 \rangle \in K(v_5, v_6|x_1, x_2)$,

$$|K(v_7, v_8|y_5, y_6)| = |K(v_7|y_5, y_6)| \leq |K(v_7)| \leq m. \tag{22}$$

With (21), we conclude that for any $\langle y_5, y_6 \rangle \in B$,

$$|K(v_7, v_8|y_5, y_6) \setminus E| \leq m - k. \tag{23}$$

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 (23) and (19),

$$|C| \leq |E| + |B|(m - k) \leq m + |B|(m - k). \tag{24}$$

Furthermore, by (22), given any element in $A \setminus B$, the number of possible shares for $\{v_7, v_8\}$ is at most m. Therefore,

$$|D| \leq |A \setminus B| \cdot m. \tag{25}$$

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 3.1,

$$|K(v_5|x_1, x_2, x_3, x_4)| \geq k,$$

and therefore

$$|B| = |K(v_5, v_6|x_1, x_2, x_3, x_4)| \geq |K(v_5|x_1, x_2, x_3, x_4)| \geq k. \tag{26}$$

We now complete the proof of the lemma.

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

The first inequality follows (24) and (25). The equality is implied by the fact that $B \subseteq A$. The last inequality follows (26) and Lemma 4.6. ■

Lemma 4.8: For every $\langle x_1, x_2 \rangle \in K(v_1, v_2)$

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

Proof: We first show that $K(v_7, v_8|x_1, x_2) \subseteq K(v_7, v_8|A)$. Take $\langle y_7, y_8 \rangle \in K(v_7, v_8|x_1, x_2)$. The vector $\langle x_1, x_2, y_7, y_8 \rangle$ can be extended to a vector $\langle x_1, x_2, y_5, y_6, y_7, y_8 \rangle \in K(v_1, v_2, v_5, v_6, v_7, v_8)$. This vector can be restricted to a vector $\langle y_5, y_6, y_7, y_8 \rangle \in$

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

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

■

We are now ready to prove the main result:

Theorem 4.9: 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 than $k + \lambda\sqrt{k}$.

Proof: Let $0 < \lambda < 1$, and assume $m \leq k + \lambda\sqrt{k}$. Since $\{v_1, v_2, v_7, v_8\} \subseteq \{v_1, v_2, v_3, v_7, v_8\}$, and $\{v_1, v_2, v_3, v_7, v_8\}$ is a circuit in the Vamos matroid, by Lemma 3.2, $|K(v_7, v_8|x_1, x_2)| \geq k^2$ 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 4.8, we have that if m is an upper bound on the size of the domain of the shares, then the following inequality must hold:

$$\left(m - k^2 + m^2\frac{k+(m-k+1)^2}{k}\right) \geq k^2. \tag{27}$$

Since the left side of Inequality (27) 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:

$$\begin{aligned} k^2 &\leq k + \lambda\sqrt{k} - k^2 \\ &\quad + (k^2 + \lambda^2 k + 2\lambda k\sqrt{k})\frac{k + (\lambda\sqrt{k}+1)^2}{k} \\ &= k + \lambda\sqrt{k} - k^2 \\ &\quad + (k^2 + \lambda^2 k + 2\lambda k\sqrt{k})\Big(1 + \lambda^2 + \frac{2\lambda}{\sqrt{k}} + \frac{1}{k}\Big) \\ &= \lambda^2 k^2 + p_\lambda(k), \end{aligned}$$

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 (27) does not hold. Therefore, any $k \geq k_0$, at least one participant must have domain of shares larger than $k + \lambda\sqrt{k}$. ■

V. Upper and Lower Bounds for Matroid-Induced Access Structures

In this section we rephrase the concept of secret-sharing scheme in terms of the entropy function, as done in [10], [19], 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 2.17 of [11] to non-ideal secret-sharing schemes for matroid-induced access structures. These lemmas were not used in the proof of Theorem 4.9, but they might be used to prove a stronger bound than the lower bound proved here.

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, e.g., [55]. All the logarithms here are of base 2.

Given a random variable X distributed over a finite set $\mathrm{supp}(X)$ such that $\Pr[X = x] = p(x)$ for every $x \in \mathrm{supp}(X)$, we define the *entropy* of X, denoted $H(X)$, as

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

It can be proved that

$$0 \leq H(X) \leq \log|\mathrm{supp}(X)|, \tag{28}$$

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

Given two random variable X and Y distributed over finite sets $\mathrm{supp}(X)$ and $\mathrm{supp}(Y)$ respectively, such that $\Pr[X = x \text{ and } Y = y] = p(x, y)$ for every $x \in \mathrm{supp}(X), y \in \mathrm{supp}(Y)$, we define the *conditioned entropy of X given Y* as

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

From the definition of the conditional entropy, the following properties can be proved:

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

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

$$H(XY) = H(X|Y) + H(Y), \tag{31}$$

and

$$H(XY) \leq H(X) + H(Y). \tag{32}$$

Given three random variable X, Y, and Z distributed over finite sets $\mathrm{supp}(X)$, $\mathrm{supp}(Y)$, and $\mathrm{supp}(Z)$ respectively, such that $\Pr[X = x, Y = y, \text{ and } Z = z] = p(x, y, z)$ for every $x \in \mathrm{supp}(X), y \in \mathrm{supp}(Y), z \in \mathrm{supp}(Z)$, the following properties hold:

$$H(X|Y) \geq H(X|YZ), \tag{33}$$

$$H(XY|Z) = H(X|YZ) + H(Y|Z), \tag{34}$$

and

$$H(XY|Z) \leq H(X|Z) + H(Y|Z). \tag{35}$$

Finally, define the *conditioned mutual information* $I(X; Y|Z)$ as

$$I(X; Y|Z) \stackrel{\text{def}}{=} H(X|Z) - H(X|YZ) = H(Y|Z) - H(Y|XZ). \tag{36}$$

B. Information Theory and Secret Sharing

We next give an equivalent definition of secret-sharing scheme. This definition is similar to that of [10], [19]. Let $\mathcal{A}$ be an access structure on the set of participants P, and denote the dealer by p_0. Assume that Σ is a distribution scheme for $\mathcal{A}$. Recall that for any participant $p \in P$, we denote by $K(p)$ the set of all possible shares given to p, and, for a given set of participants $A \subseteq P$, we denote by $K(A)$ the set of possible vectors of shares given to the participants in A. We also denote $K(p_0)$ by K (that is, K is the domain of secrets).

A distribution scheme Σ is a probabilistic mapping that given a secret s generates a distribution on the shares. Any probability distribution $\{p_{_K}(s)\}_{s\in K}$ on the domain of secrets, together with the distribution scheme Σ, induces a probability distribution on $K(A)$, for any $A \subseteq P$. We denote this probability distribution by $\{p_{_{K(A)}}(\mathbf{K_A})\}_{\mathbf{K_A}\in K(A)}$, and denote the random variable taking values in $K(A)$ according the probability distribution $\{p_{_{K(A)}}(\mathbf{K_A})\}_{\mathbf{K_A}\in K(A)}$ by S_A, and by S the random variable taking values in K according to the probability distribution $\{p_{_K}(s)\}_{s\in K}$. Note that the random variable taking values in $K(A \cup B)$ can be written either as $S_{A\cup B}$ or as $S_A S_B$. For a singleton $\{b\}$, we will some times write S_b instead of $S_{\{b\}}$. It should be emphasized that Definition 2.3 of secret-sharing scheme does not assume any distribution on the secrets. Here, we assume such distribution, and the results are stated in terms of the entropy of the secret, which is imposed by this distribution.

We can now restate the conditions of correctness and privacy according to the new definitions. Using Bayes' theorem, it can be shown that this restatement is equivalent to Definition 2.3.

Lemma 5.1: Let $p_{_K}(s) > 0$ for every $s \in K$. A distribution scheme is a secret-sharing scheme realizing an access structure $\mathcal{A}$ (according to Definition 2.3) if and only if the following conditions hold.

Correctness: If $A \in \mathcal{A}$, then for all $\mathbf{K_A} \in K(A)$ with $p_{_{K(A)}}(\mathbf{K_A}) > 0$ there exists a unique secret $s \in K$ such that $p_{_K}(s|\mathbf{K_A}) = 1$.

Privacy: If $A \notin \mathcal{A}$, then for all $s \in K$ and for all $\mathbf{K_A} \in K(A)$ with $p_{_{K(A)}}(\mathbf{K_A}) > 0$, it holds that $p_{_K}(s|\mathbf{K_A}) = p_{_K}(s)$.
From the properties of the entropy function, the conditions in Lemma 5.2 are equivalent to the conditions in Lemma 5.1.

Lemma 5.2: A distribution scheme is a secret-sharing scheme realizing an access structure $\mathcal{A}$ (according to Definition 2.3) if and only if the following conditions hold.

Correctness: For every $A \in \mathcal{A}$,

$$H(S|S_A) = 0. \tag{37}$$

Privacy: For every $A \notin \mathcal{A}$,

$$H(S|S_A) = H(S). \tag{38}$$

Blundo et al. [56] showed that it is enough to show privacy of a given secret-sharing scheme with a uniform distribution on the secrets, and that if such a scheme is private, then it is private for any distribution on the secrets.

C. Lower Bounds on the Entropy of Shares of Subsets

Let $\mathcal{M} = \langle V, \mathcal{C}\rangle$ be a connected matroid, $p_0 \in V$ and $\mathcal{A}$ be the induced access structure of $\mathcal{M}$ with respect to p_0. Finally, let Σ be a secret-sharing scheme realizing $\mathcal{A}$. As discussed above, any probability distribution on K, induces a probability distribution on the shares of the subsets of V. We now prove some lemmas concerning these variables.

In Theorem 5.5, we prove a lower bound on the entropy of any independent subset of V. To prove Theorem 5.5 we prove two lemmas. The first lemma, which generalizes Lemma 3.1, makes no use of the fact that $\mathcal{A}$ has an appropriate matroid; it is proven for any access structure.

Lemma 5.3: 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:

$$\begin{aligned}
&H(S_b|S_A)\\
&\geq H(S_b|S_A S_{B\setminus\{b\}}) \qquad \text{(from (33))}\\
&= H(S_b|S_{A\cup B\setminus\{b\}})\\
&\qquad + H(S|S_{A\cup B}) \quad \text{(since } H(S|S_{A\cup B}) = 0 \text{ from (37))}\\
&= H(S_b S|S_{A\cup B\setminus\{b\}}) \qquad \text{(from (34))}\\
&= H(S_b|S_{A\cup B\setminus\{b\}} S) + H(S|S_{A\cup B\setminus\{b\}}) \quad \text{(from (34))}\\
&= H(S_b|S_{A\cup B\setminus\{b\}} S)\\
&\qquad + H(S) \quad \text{(from (38) and because } A\cup B\setminus\{b\} \notin \mathcal{A})\\
&\geq H(S) \qquad \text{(from (29)).}
\end{aligned}$$

■

A consequence of this lemma 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 (31), we get by induction that $H(S_I) \geq |I| \cdot H(S)$. We now generalize this claim to every independent set (which is not necessarily contained in a minterm). 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 5.4: For every non-empty independent set $I \subseteq V \setminus \{p_0\}$, there exist $C \in \mathcal{C}_0$ and $i \in I \cap C$ such that there is no $C_1 \in \mathcal{C}_0$ satisfying

$$C_1 \subseteq C \cup I \setminus \{i\}. \tag{39}$$

Proof: Since the matroid $\mathcal{M}$ is connected, for every $i, j \in V$, there is a circuit $C \in \mathcal{C}$ such that $i, j \in C$ (by Definition 2.11). In particular, there exists a circuit $C \in \mathcal{C}_0$ such that $I \cap C \neq \emptyset$. Choose a circuit $C \in \mathcal{C}_0$ such that $I \cap C \neq \emptyset$ and for every $C' \in \mathcal{C}_0$

$$\begin{aligned}
&I \cap C' \neq \emptyset\\
&\quad \Longrightarrow \quad C' \setminus I \text{ is not properly contained in } C \setminus I.
\end{aligned} \tag{40}$$

Furthermore, choose an arbitrary $i \in I \cap C$.

We claim that such C and i satisfy the conditions of the lemma, namely, there is no $C_1 \in \mathcal{C}_0$ satisfying (39). Assume towards contradiction that this is not the case, and choose $C_1 \in \mathcal{C}_0$ satisfying (39). From C and C_1 we construct circuits C_2 and C_3 such that C_3 contradicts (40).

First, we describe the construction of the circuit C_2. We have

$$C_1 \cap I \quad \neq \quad \emptyset, \tag{41}$$

otherwise $C_1 \subsetneq C$ in a contradiction to Axiom (C1) of the matroids. By (39),

$$C_1 \setminus I \quad \subseteq \quad C \setminus I. \tag{42}$$

Therefore, by (40), (41), and (42)

$$C \setminus I \quad = \quad C_1 \setminus I. \tag{43}$$

Since C is a circuit and I is independent, C is not a subset of I, thus, $C \setminus I \neq \emptyset$. Let

$$c \quad \in \quad C \setminus I = C_1 \setminus I. \tag{44}$$

Since $c \in C \cap C_1$, by Axiom (C2) there exists a circuit

$$C_2 \quad \subseteq \quad C \cup C_1 \setminus \{c\}\,. \tag{45}$$

Next, we describe the construction of the circuit C_3. By (45) and (39),

$$C_2 \quad \subseteq \quad C \cup C_1 \setminus \{c\} \subseteq C \cup I \setminus \{c\}\,. \tag{46}$$

By (46) and (44),

$$C_2 \setminus I \quad \subseteq \quad (C \setminus I) \setminus \{c\} \subsetneq C \setminus I. \tag{47}$$

Thus, since C and C_2 are distinct circuits, by (47),

$$C_2 \cap I \neq \emptyset. \tag{48}$$

Therefore, $p_0 \notin C_2$ by (48), (47), and (40), which implies that $p_0 \in C \setminus \mathcal{C}_2$. 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, by (45), $c' \neq c$. By (47), we have that $c' \in C \setminus I$, so $c' \in C_2 \cap C$. Therefore, Lemma 2.10 implies that there is a circuit C_3 such that $p_0 \in C_3$ and $C_3 \subseteq C_2 \cup C \setminus \{c'\}$. Note that $C_3 \in \mathcal{C}_0$ since $p_0 \in C_3$.

We are ready to conclude the proof by showing the contradiction. Since $c' \in C \setminus (C_3 \cup I)$, we have $C_3 \setminus I \subsetneq C \setminus I$. Moreover, $C_3 \cap I \neq \emptyset$ (otherwise $C_3 \subsetneq C$). Therefore, C_3 is a contradiction to the minimality of $C \setminus I$ (defined in (40)), so C and i satisfy the conditions of the lemma. ■

Theorem 5.5: 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 a secret-sharing scheme realizing $\mathcal{A}$. For every $A \subseteq V$,

$$H(S_A) \geq \mathrm{rank}(A) \cdot H(S).$$

Proof: From the definition of the rank function and (30), it suffices 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, in particular, contains no circuit which contains p_0. Therefore, $I \setminus \{p_0\}$ contains no minterm, i.e., $I \setminus \{p_0\} \notin \mathcal{A}$. Now, by (38), $H(S|S_{I\setminus\{p_0\}}) = H(S)$, and, by (31),

$$\begin{aligned} H(S_I) &= H(S S_{I\setminus\{p_0\}}) \\ &= H(S|S_{I\setminus\{p_0\}}) + H(S_{I\setminus\{p_0\}}) \\ &= H(S) + H(S_{I\setminus\{p_0\}}). \end{aligned}$$

If $p_0 \notin I$, then, by Lemma 5.4, for every independent set $I \subseteq V \setminus \{p_0\}$, there exist $i \in I$ 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 $I \cup C \setminus \{i, p_0\} \notin \mathcal{A}$. On the other hand, $I \cup C \setminus \{p_0\} \in \mathcal{A}$, and so, by Lemma 5.3 (with $b = i$, $A = I \setminus \{i\}$, and $B = (C \cup \{i\}) \setminus \{p_0\}$),

$$H(S_i | S_{I\setminus\{i\}}) \geq H(S). \tag{49}$$

By (49) and (31),

$$\begin{aligned} H(S_I) &= H(S_i S_{I\setminus\{i\}}) \\ &= H(S_i|S_{I\setminus\{i\}}) + H(S_{I\setminus\{i\}}) \\ &\geq H(S) + H(S_{I\setminus\{i\}}). \end{aligned}$$

■

D. Upper Bounds on the Entropy of Shares of Subsets

In Lemma 5.9, we will 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 the share of an element in a circuit given the shares of the rest of the elements (assuming an upper bound on the entropy of the participants). This enables us to prove, in Theorem 5.10, upper bounds on the entropy of shares of subsets.

Assume $\mathcal{M}$ and Σ as above, and in addition, for every $v \in V \setminus \{p_0\}$,

$$H(S_v) \quad \leq \quad (1+\lambda)H(S) \tag{50}$$

for some $\lambda \geq 0$. Define $\mathcal{C}_0 \stackrel{\text{def}}{=} \{C \in \mathcal{C} : p_0 \in C\}$ as above.

Throughout this section we assume that the entropy of the shares of each participant is bounded as stated in (50). By (32), this implies that $H(S_A) \leq |A|(1+\lambda)H(S)$. In the sequel we prove a better upper bound on $H(S_A)$ provided that λ is small enough (in particular, when $\lambda < 1/(n-1)$). Notice that the purpose of these upper bounds is to prove lower bounds. That is, our hope is to assume that (50) holds for some $\lambda > 0$ and achieve a contradiction (in an analogous way to our proof in Theorem 4.9 where we assume that the size of the domain of shares of each participant is $k + \lambda\sqrt{k}$ and achieve a contradiction).

Lemma 5.6: For every $C \in \mathcal{C}_0$ and $c \in C$, $H(S_c|S_{C\setminus\{c\}}) \leq \lambda H(S)$.

Proof: If $c = p_0$, then $C \setminus \{c\} \in \mathcal{A}$ and, therefore, from (37) we get $H(S_c|S_{C\setminus\{c\}}) = 0$. Otherwise, from (36), (38), and (37),

$$\begin{aligned} I(S; S_c|S_{C\setminus\{c,p_0\}}) &= H(S|S_{C\setminus\{c,p_0\}}) - H(S|S_{C\setminus\{p_0\}}) \\ &= H(S). \end{aligned} \tag{51}$$

On the other hand, by (36),

$$I(S; S_c|S_{C\setminus\{c,p_0\}}) = H(S_c|S_{C\setminus\{c,p_0\}}) - H(S_c|S_{C\setminus\{c\}}). \tag{52}$$

Therefore,

$$\begin{aligned}
&H(S_c|S_{C\setminus\{c\}})\\
&\quad= H(S_c|S_{C\setminus\{c,p_0\}}) - H(S) \qquad \text{(by (51) and (52))}\\
&\quad\le H(S_c) - H(S) \qquad \text{(by (29))}\\
&\quad\le (1+\lambda)H(S) - H(S) \qquad \text{(by (50))}\\
&\quad= \lambda H(S).
\end{aligned}$$

■

Lemma 5.7: For every $C \in \mathcal{C} \setminus \mathcal{C}_0$ and $c \in C$, there exist $C_1, C_2 \in \mathcal{C}_0$ 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 2.12).

Proof: From Lemma 2.12 there are $C_1, C_2 \in \mathcal{C}_0$ such that $C = D_{p_0}(C_1, C_2)$. If $c \in C_1 \setminus C_2$ or $c \in C_2 \setminus C_1$ 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 $c \in J_{p_0}(C_1, C_2)$), and, so, $c \in C_1 \setminus C_3$.

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 $J_{p_0}(C_1, C_2) \subseteq J_{p_0}(C_1, C_3)$. Therefore,

$$D_{p_0}(C_1, C_3) \subseteq D_{p_0}(C_1, C_2).$$

By Lemma 2.12, the circuits which do not contain p_0 are the *minimal* sets of the form $D_{p_0}(C_1, C_2)$ for all $C_1, C_2 \in \mathcal{C}_0$. Since $D_{p_0}(C_1, C_2)$ is a circuit, we get

$$D_{p_0}(C_1, C_3) = D_{p_0}(C_1, C_2),$$

and therefore $C = D_{p_0}(C_1, C_3)$ as desired. ■

Lemma 5.8: Let $C_1, C_2 \in \mathcal{C}_0$, $C = D_{p_0}(C_1, C_2)$, and $J = J_{p_0}(C_1, C_2) \setminus \{p_0\}$. Then $H(S_J|S_C) \ge |J| \cdot H(S)$.

Proof: As in Theorem 5.5, it is sufficient to prove that for every $J' \subseteq J$ there exists $i \in J'$ such that $H(S_{J'}|S_C) \ge H(S) + H(S_{J'\setminus\{i\}}|S_C)$. Let $J' \subseteq J$ and $i \in J'$. First,

$$C \cup J \setminus \{i\} \quad\notin\quad \mathcal{A} \tag{53}$$

otherwise, there is some $C' \in \mathcal{C}_0$ such that $C' \subseteq C \cup \{p_0\} \cup J \setminus \{i\} = C_1 \cup C_2 \setminus \{i\}$ contradicting the fact that $i \in J_{p_0}(C_1, C_2)$. Second,

$$C \cup J \in \mathcal{A} \tag{54}$$

since, for example, $C \cup J \cup \{p_0\}$ contains the circuit $C_1 \in \mathcal{C}_0$. Thus, by Lemma 5.3 (with $A = C \cup J' \setminus \{i\}$, $B = J$, and $b = i$), we have $H(S_{\{i\}}|S_{C\cup J'\setminus\{i\}}) \ge H(S)$. Therefore, by (31),

$$\begin{aligned}
H(S_{J'}|S_C) &= H(S_i S_{J'\setminus\{i\}}|S_C)\\
&= H(S_{\{i\}}|S_{C\cup J'\setminus\{i\}}) + H(S_{J'\setminus\{i\}}|S_C)\\
&\ge H(S) + H(S_{J'\setminus\{i\}}|S_C).
\end{aligned}$$

■

Lemma 5.9: For every $C \in \mathcal{C} \setminus \mathcal{C}_0$ such that $C = D_{p_0}(C_1, C_2)$ for some $C_1, C_2 \in \mathcal{C}_0$, and every $c \in C$ such that $c \in C_1 \setminus C_2$,

$$H(S_c|S_{C\setminus\{c\}}) \le |J_{p_0}(C_1, C_2)|\lambda H(S). \tag{55}$$

In particular, for every $C \in \mathcal{C} \setminus \mathcal{C}_0$ and $c \in C$,

$$H(S_c|S_{C\setminus\{c\}}) \le n\lambda H(S)$$

where n is the number of participants (that is, $n = |V| - 1$).

Proof: Denote $J \stackrel{\text{def}}{=} J_{p_0}(C_1, C_2) \setminus \{p_0\}$. Thus,

$$C \;=\; D_{p_0}(C_1, C_2) \;=\; (C_1 \cup C_2) \setminus (J \cup \{p_0\}). \tag{56}$$

By (34) with $X = S_c$, $Y = S_J$, and $Z = S_{C\setminus\{c\}}$,

$$H(S_{J\cup\{c\}}|S_{C\setminus\{c\}}) = H(S_c|S_{J\cup C\setminus\{c\}}) + H(S_J|S_{C\setminus\{c\}}). \tag{57}$$

Similarly, by (34) with $X = S_J$, $Y = S_c$, and $Z = S_{C\setminus\{c\}}$,

$$H(S_{J\cup\{c\}}|S_{C\setminus\{c\}}) = H(S_J|S_C) + H(S_c|S_{C\setminus\{c\}}). \tag{58}$$

Thus, by (58) and (57),

$$\begin{aligned}
H(S_c|S_{C\setminus\{c\}}) &= H(S_{J\cup\{c\}}|S_{C\setminus\{c\}}) - H(S_J|S_C)\\
&= H(S_c|S_{J\cup C\setminus\{c\}})\\
&\quad + H(S_J|S_{C\setminus\{c\}}) - H(S_J|S_C).
\end{aligned} \tag{59}$$

We next bound each term in the above sum, and get the desired result.

First, since $c \notin C_2$ and by (56), we have

$$C_2 \setminus \{p_0\} \quad\subseteq\quad C_1 \cup C_2 \setminus \{c, p_0\} = J \cup C \setminus \{c\}\,. \tag{60}$$

Since C_2 is a circuit that contains p_0, we have $C_2 \setminus \{p_0\} \in \mathcal{A}$, and, by (60), $J \cup C \setminus \{c\} \in \mathcal{A}$. By (37) we deduce

$$H(S|S_{J\cup C\setminus\{c\}}) = 0. \tag{61}$$

Now

$$\begin{aligned}
&H(S_c|S_{J\cup C\setminus\{c\}})\\
&\quad= H(S_{J\cup C}) - H(S_{J\cup C\setminus\{c\}}) \quad \text{(from (31))}\\
&\quad= H(S_{J\cup C})\\
&\qquad - [H(S|S_{J\cup C\setminus\{c\}}) + H(S_{J\cup C\setminus\{c\}})] \quad \text{(from (61))}\\
&\quad= H(S_{J\cup C}) - H(S_{J\cup C\cup\{p_0\}\setminus\{c\}}) \quad \text{(from (31))}\\
&\quad\le H(S_{J\cup C\cup\{p_0\}}) - H(S_{J\cup C\cup\{p_0\}\setminus\{c\}}) \quad \text{(from (30))}\\
&\quad= H(S_c|S_{J\cup C\cup\{p_0\}\setminus\{c\}}) \quad \text{(from (31))}\\
&\quad\le H(S_c|S_{C_1\setminus\{c\}}) \; \text{(since } C_1 \setminus \{c\} \subseteq J \cup C \cup \{p_0\} \setminus \{c\}\text{)}\\
&\quad\le \lambda H(S) \quad \text{(from Lemma 5.6).}
\end{aligned} \tag{62}$$

Second, by the assumption on the size of the shares of the participants, with (29) and (32),

$$\begin{aligned}
H(S_J|S_{C\setminus\{c\}}) &\le H(S_J)\\
&\le \sum_{i\in J} H(S_i)\\
&\le |J|(1+\lambda)H(S).
\end{aligned} \tag{63}$$

Third, from Lemma 5.8 we derive

$$H(S_J|S_C) \quad\ge\quad |J| \cdot H(S). \tag{64}$$

By (59), and by summing up the bounds in (62), (63), and (64) we get:

$$\begin{aligned}
H(S_c|S_{C\setminus\{c\}}) &\le \lambda H(S) + |J|(1+\lambda)H(S) - |J| \cdot H(S)\\
&= (|J|+1)\lambda H(S),
\end{aligned} \tag{65}$$

from which we get (55).

By Lemma 5.7, for every $C \in \mathcal{C} \setminus \mathcal{C}_0$ and $c \in C$ there exist $C_1, C_2 \in \mathcal{C}_0$ such that $C = D_{p_0}(C_1, C_2)$ and $c \in C_1 \setminus C_2$.

Thus, by (65), $H(S_c|S_{C\setminus\{c\}}) \leq (|J|+1)\lambda H(S) \leq n\lambda H(S)$. ■

Theorem 5.10: 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 $\lambda \geq 0$ be such that

$$H(S_v) \leq (1+\lambda)H(S) \tag{66}$$

for every $v \in V \setminus \{p_0\}$. Then, for every $A \subseteq V$

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

Proof: Let $A \subseteq V$, and $I \subseteq A$ be an independent set of size $\operatorname{rank}(A)$. Then,

$$\begin{aligned} &H(S_A) \\ &\leq\ H(S_I) + H(S_{A\setminus I}|S_I) \qquad \text{(by (31))} \\ &\leq\ \sum_{v\in I} H(S_v) + \sum_{v\in A\setminus I} H(S_v|S_I) \qquad \text{(by (32) and (35))} \\ &\leq\ |I|(1+\lambda)H(S) + \sum_{v\in A\setminus I} H(S_v|S_I) \qquad \text{(by (66))}. \end{aligned}$$

Thus, to prove the theorem it suffices to prove that for every $v \in A \setminus I$

$$H(S_v|S_I) \leq \lambda n H(S).$$

To this end, fix $v \in A \setminus I$ and notice that $I \cup \{v\}$ is dependent, thus, it contains some circuit C that contains v. In particular, $C \setminus \{v\} \subseteq I$ and, by (33), $H(S_v|S_I) \leq H(S_v|S_{C\setminus\{v\}})$. If $p_0 \in C$, then, by Lemma 5.6, $H(S_v|S_{C\setminus\{c\}}) \leq \lambda H(S)$. If $p_0 \notin C$, then, by Lemma 5.9, $H(S_v|S_{C\setminus\{v\}}) \leq n\lambda H(S)$. ■

We next show how to apply these results to the Vamos matroid, considered in Section IV. We then compare this bound to the bound we achieve in Section IV.

Example 5.11: Consider a secret-sharing scheme realizing the Vamos access structure V_8. Recall that V_8 has $n = 7$ participants. Furthermore, the set $\{v_1, v_2, v_5, v_6\}$ is a circuit of the Vamos matroid, thus, $\operatorname{rank}(\{v_1, v_2, v_5, v_6\}) = 3$. By Theorem 5.10, $H(S_{\{v_1,v_2,v_5,v_6\}}) \leq (3+10\lambda)H(S)$ (by using Lemma 5.9 we can get a better dependence of λ). Since $\{v_1, v_2\}$ is independent, by Theorem 5.5, $H(S_{\{v_1,v_2\}}) \geq 2H(S)$. Thus, by (31),

$$\begin{aligned} H(S_{\{v_5,v_6\}}|S_{\{v_1,v_2\}}) &= H(S_{\{v_1,v_2,v_5,v_6\}}) - H(S_{\{v_1,v_2\}}) \\ &\leq (1+10\lambda)H(S). \end{aligned}$$

Thus, there is a vector of shares $\langle x_1, x_2\rangle$ such that

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

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 (28), $H(S_{v_i}) \leq \log(2k) = H(S) + 1 = (1 + 1/\log k)H(S)$. Thus, there is a vector of shares $\langle x_1, x_2\rangle$ such that

$$H\big(S_{\{v_5,v_6\}}|S_{\{v_1,v_2\}} = \langle x_1, x_2\rangle\big) \leq (1 + 10/\log k)H(S).$$

This should be compared to the bound of approximately $2H(S)$ we can achieve by Lemma 4.6 and (28). Notice that in the proof of our main result we prove in Lemma 4.6 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 $\{v_1, v_2\}$.

In [21], the bounds proved in this paper, together with a non-Shannon information inequality of [57], are used to prove that in any secret-sharing scheme realizing an access structure induced by the Vamos matroid, the size of the domain of shares of at least one participant is at least $k^{1.1}$, where k is the size of the domain of secrets. This improves the bound of $k + \Omega(\sqrt{k})$ bound proved in this paper.

VI. An Access Structure that is Nearly Ideal

We next present an example of a non-ideal access structure induced by a matroid, which is nearly ideal: for infinitely many values of k it has a secret-sharing scheme realizing it with domain of secrets of size k and domain of shares of size $k+1$. An access structure has information rate 1 if the infimum of the ratio between the log of the size of the shares' domain and the log of the size of the secret's domain is 1. Our example shows that there is an access structure with information rate 1 that is not ideal. The fact that this access structure is nearly ideal was proved independently by Matúš [22].

Definition 6.1 (The Access Structures $\mathcal{F}, \overline{\mathcal{F}}$, and $\mathcal{F} \wedge \overline{\mathcal{F}}$): Let $\mathcal{F}, \overline{\mathcal{F}}$ be access structures on the set of participants $\{a_1, a_2, \ldots, a_6\}$ and $\{b_1, b_2, \ldots, b_6\}$ respectively, where the minterms of $\mathcal{F}$ are

$$\begin{aligned} &\{a_1, a_4\}, \{a_2, a_5\}, \{a_3, a_6\}, \{a_1, a_2, a_6\}, \{a_1, a_3, a_5\}, \\ &\{a_2, a_3, a_4\}, \{a_4, a_5, a_6\}, \end{aligned}$$

and the minterms of $\overline{\mathcal{F}}$ are

$$\begin{aligned} &\{b_1, b_4\}, \{b_2, b_5\}, \{b_3, b_6\}, \{b_1, b_2, b_6\}, \{b_1, b_3, b_5\}, \\ &\{b_2, b_3, b_4\}, \{b_4, b_5, b_6\}, \{b_3, b_4, b_5\}. \end{aligned}$$

Finally, define the access structure $\mathcal{F} \wedge \overline{\mathcal{F}}$ on the set of participants $\{a_1, a_2, \ldots, a_6\} \cup \{b_1, b_2, \ldots, b_6\}$ as

$$\mathcal{F} \wedge \overline{\mathcal{F}} \stackrel{\text{def}}{=} \left\{A \cup B : A \in \mathcal{F}, B \in \overline{\mathcal{F}}\right\}.$$

The access structure $\mathcal{F}$ has an appropriate matroid, namely the Fano matroid, and the access structure $\overline{\mathcal{F}}$ also has an appropriate matroid, namely the nonFano matroid (see, e.g., [40, Example 4.2]). The next observation follows since $\mathcal{F}$ and $\overline{\mathcal{F}}$ have appropriate matroids.

Observation 6.2: The access structure $\mathcal{F} \wedge \overline{\mathcal{F}}$ has an appropriate matroid.

The observation also follows from Claim 6.4 (showing that there is a secret-sharing scheme realizing $\mathcal{F} \wedge \overline{\mathcal{F}}$ in which the size of the domain of shares of each participant is at most $k+1$) and the result of [17] (showing that in every secret-sharing scheme realizing an access structure that does not have an appropriate matroid the size of the domain of shares of at least one participant is $k^{1.5}$).

Using a result of [13], it is easy to show that the access structure $\mathcal{F} \wedge \overline{\mathcal{F}}$ is not ideal.

Claim 6.3: The access structure $\mathcal{F} \wedge \overline{\mathcal{F}}$ is not ideal.

Proof: Matúš [13] proves that for odd k, the access structure $\mathcal{F}$ does not have an ideal scheme with domain of secrets of size k, and for even k, the access structure $\overline{\mathcal{F}}$ does not have an ideal scheme with domain of secrets of size k. If $\mathcal{F} \wedge \overline{\mathcal{F}}$ has an ideal secret-sharing scheme with domain of secrets of size k for some k, then, both $\mathcal{F}$ and $\overline{\mathcal{F}}$ have an ideal secret-sharing scheme with domain of secrets of size k. But this is impossible by the result of [13]. ■

Using known schemes and the representation of the appropriate matroids, we construct a "nearly" ideal secret-sharing schemes realizing $\mathcal{F} \wedge \overline{\mathcal{F}}$.

Claim 6.4: For any $i \in \mathbb{N}$, there is a secret-sharing scheme realizing $\mathcal{F} \wedge \overline{\mathcal{F}}$ with domain of secrets of size 2^i such that the size of the domain of shares of each participants is bounded by $2^i + 1$.

Proof: Since every minimal authorized subset of $\mathcal{F} \wedge \overline{\mathcal{F}}$ is a union of two minimal authorized subsets of $\mathcal{F}$ and $\overline{\mathcal{F}}$, we can use a known paradigm to construct a scheme realizing $\mathcal{F} \wedge \overline{\mathcal{F}}$: Let $K = \{0, \ldots, 2^i - 1\}$ be the domain of secrets. The dealer chooses a random integer $r \in K$, and independently shares r among the participants $\{a_1, \ldots, a_6\}$ with access structure $\mathcal{F}$, and $r \oplus s$ among the participants $\{b_1, \ldots, b_6\}$ with access structure $\overline{\mathcal{F}}$. We have reduced the question of sharing a secret from K in the access structure $\mathcal{F} \wedge \overline{\mathcal{F}}$ to the question of sharing a secret from K in the access structure $\mathcal{F}$ and sharing a secret from K in the access structure $\overline{\mathcal{F}}$. Thus, to complete the description of the scheme, we need to explain how to construct secret-sharing schemes realizing $\mathcal{F}$ and $\overline{\mathcal{F}}$ with domain of secrets of size 2^i and domain of shares of size at most $2^i + 1$.

Brickell [5] has proved that if an access structure has an appropriate matroid representable over a finite field with k elements, then it has an ideal secret-sharing scheme with domain of secrets of size k. Since the Fano matroid is representable over every field of characteristic 2, for every $i \in \mathbb{N}$, there is an ideal scheme realizing $\mathcal{F}$ with domain of secrets of size 2^i.

The construction for $\overline{\mathcal{F}}$ requires more details. We will use a result by [58], showing that if an access structure $\mathcal{A}$ has ideal schemes with domain of secrets of size q_1 and q_2, then it has an ideal scheme with domain of secrets of size $q_1 \cdot q_2$. For completeness, we describe this construction. Denote the ideal schemes realizing $\mathcal{A}$ over a domain secrets (and shares) of size q_i by Σ_i for $i \in \{1, 2\}$. By using any bijection from $\mathbb{Z}_{q_i}$ to the domain of secrets, we can assume without loss of generality that the domain of secrets and shares in Σ_i is $\mathbb{Z}_{q_i}$. We construct a scheme Σ realizing $\mathcal{A}$ with domain of secrets and shares $\{1, \ldots, q_1\} \times \{1, \ldots, q_2\}$. Notice that $|\{1, \ldots, q_1\} \times \{1, \ldots, q_2\}| = q_1 q_2$ as required. To share a secret $s = \langle s_1, s_2 \rangle \in \{1, \ldots, q_1\} \times \{1, \ldots, q_2\}$, we share s_i using Σ_i for $i \in \{1, 2\}$. The share of each participant is a pair: the share of s_1 using Σ_1 and the share of s_2 using Σ_2.

Given any odd integer $k \in \mathbb{N}$, we consider its decomposition into prime powers, $k = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_\ell^{e_\ell}$ (for some ℓ). Since the nonFano matroid is representable over every field whose characteristic is not 2, for every i, there is an ideal scheme realizing $\overline{\mathcal{F}}$ with domain of secrets of size $p_i^{e_i}$. Using the construction of [58] inductively, there is an ideal scheme realizing $\overline{\mathcal{F}}$ with domain of secrets of size k. Now using the ideal scheme with $k = 2^i + 1$, there is a scheme realizing $\overline{\mathcal{F}}$ with domain of secrets and shares of size $2^i + 1$. By only sharing secrets from a domain of size 2^i, we get a scheme with domain of secrets of size 2^i and domain of shares of size $2^i + 1$ (by Definition 2.3 such restriction is allowed as it does not effect the correctness and the privacy of the scheme).

We have constructed the schemes for $\mathcal{F}$ and $\overline{\mathcal{F}}$, thus, by the discussion above, there is a secret-sharing scheme realizing $\mathcal{F} \wedge \overline{\mathcal{F}}$ with domain of secrets of size 2^i and domain of shares of size 2^i. ■

VII. Conclusions and Open Problems

Ideal secret-sharing schemes and matroids are closely related as proved by Brickell and Davenport [11]: If an access structure is ideal then it is induced by a matroid. That is, being induced by a matroid is a necessary condition for an access structure to be ideal. Seymour [12] showed that this condition is not necessary by proving that the access structures induced by the Vamos matroid is not ideal. In this paper we consider the question if being induced by a matroid implies that the access structure has an efficient secret-sharing scheme. We prove that in any secret-sharing realizing an access structure induced by the Vamos matroid the size of the domain of shares is at least $k + \Omega(k)$, where k is the size of the domain of secrets (compared to the lower bound of $k + 1$ implied by [12]).

Recently, our result was improved by [21], proving that in any secret-sharing realizing the access structures induced by the Vamos matroid the size of the domain of shares is at least $k^{1.1}$. In another recent result, Martí-Farré and Padró [16] constructed a scheme realizing the access structures induced by the Vamos matroid in which the size of the domain of shares is $O(k^{4/3})$. Thus, the access structures induced by the Vamos matroid solve Question 1 (mentioned in the introduction) in the affirmative. This should be contrasted with access structures not induced by matroids in which the size of the domain of shares is at least $k^{1.5}$ (as proved in [17]).

Although secret-sharing schemes have been studied for nearly three decades, there are many remaining open problems. The most important question is if there are efficient schemes for general access structures. In the best known secret-sharing schemes realizing general access structures (e.g., in [6]) the size of the shares is $2^{O(n)}$ even if the secret is one bit. On the other hand, the strongest known lower bound, proved by Csirmaz [35], states that for every n there is an access structure $\mathcal{A}_n$ with n participants such that for every secret-sharing scheme realizing $\mathcal{A}_n$ with 1-bit secrets the size of the shares of at least one participant is $\Omega(n/\log n)$, and the sum of the size of shares over the n participants is at least $\Omega(n^2/\log n)$. Thus, there is a huge gap between the best known lower bounds and the best known upper bounds. The question of super-polynomial lower bounds on the size of shares for some (explicit or implicit) access structures is still open.

We want to point one possible direction for proving lower bounds for secret-sharing schemes. The proof given by Csirmaz [35] uses the so-called Shannon type information inequalities. However, Csirmaz observed that only using Shannon type inequalities cannot prove a lower bound better than $\Omega(n^2)$ on the sum of the size of shares over the n participants. However, in the last decade there have been a series of works [57], [59], [60], [61], [62] proving so called non-Shannon inequalities. Such an inequality is used in [21] to improve the lower bound for the access structures induced by the Vamos matroid. We believe that these inequalities can be used to improve the lower bounds for general secret-sharing schemes.

A specific class of access structures, which is discussed in this paper, is the class of access structures induced by matroids. For these access structures there is no better schemes than the schemes for general access structures; in these schemes the shares are $2^{O(n)}$-bit long even for sharing a 1-bit secret. It is open if there are better upper-bounds for access structures induced by matroids than for general access structures. In other words, it is open if being induced by a matroid helps.

Finally, we want to mention some open problems concerning ideal secret-sharing schemes. The most obvious question is giving an exact characterization of ideal access structures. As discussed in the introduction, Brickell and Davenport [11] give a necessary condition and a sufficient condition for being ideal. However, there is a gap between these conditions. Seymour [12] proved that the necessary condition (being induced by a matroid) is not sufficient, and Simonis and Ashikmin [39] proved that the sufficient condition (being induced by a *representable* matroid) is not necessary. Even though several interesting results have been given in [39], [13], [22], the question of exact characterization of ideal access structures, which is in some sense is a problem about representability of matroids, is far from being solved.

A related open problem is characterizing access structures that are nearly ideal.

Definition 7.1 (Nearly-Ideal Access Structure): We say that an access structure $\mathcal{A}$ is nearly ideal if there exists a function $f : \mathbb{N} \to \mathbb{N}$ such that $\lim_{k\to\infty} f(\ell)/\ell = 1$ and for every ℓ there is a secret-sharing scheme realizing $\mathcal{A}$ in which the secret is an ℓ-bit string and the shares are $f(\ell)$-bit strings. The result of Section VI implies that the access structure $\mathcal{F} \wedge \overline{\mathcal{F}}$ is nearly ideal as for every ℓ there is a secret-sharing scheme realizing $\mathcal{F} \wedge \overline{\mathcal{F}}$ in which the secret is an ℓ-bit string and the shares are $(\ell+1)$-bit strings. Thus, there is an access structure that is not ideal but is nearly ideal. By [17], every nearly-ideal access structure is induced by a matroid. However, by the new result of [21], this condition is not sufficient. The question of giving an exact characterization of nearly-ideal access structures is open.

ACKNOWLEDGMENT

We thank Enav Weinreb for very helpful discussions.

REFERENCES

[1] A. Beimel and N. Livne, "On matroids and non-ideal secret sharing," in *Proc. of the Third Theory of Cryptography Conference – TCC 2006*, ser. Lecture Notes in Computer Science, S. Halevi and T. Rabin, Eds., vol. 3876, 2006, pp. 482–501.
[2] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing schemes realizing general access structure," in *Proc. of the IEEE Global Telecommunication Conf., Globecom 87*, 1987, pp. 99–102, journal version: Multiple assignment scheme for sharing secret. *J. of Cryptology*, 6(1):15-20, 1993.
[3] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Advances in Cryptology – CRYPTO '88*, ser. Lecture Notes in Computer Science, S. Goldwasser, Ed., vol. 403. Springer-Verlag, 1990, pp. 27–35.
[4] G. J. Simmons, W. Jackson, and K. M. Martin, "The geometry of shared secret schemes," *Bulletin of the ICA*, vol. 1, pp. 71–88, 1991.
[5] E. F. Brickell, "Some ideal secret sharing schemes," *Journal of Combin. Math. and Combin. Comput.*, vol. 6, pp. 105–113, 1989.
[6] M. Karchmer and A. Wigderson, "On span programs," in *Proc. of the 8th IEEE Structure in Complexity Theory*, 1993, pp. 102–111.
[7] D. R. Stinson, "Decomposition construction for secret sharing schemes," *IEEE Trans. on Information Theory*, vol. 40, no. 1, pp. 118–125, 1994.
[8] M. v. Dijk, "A linear construction of secret sharing schemes," *Designs, Codes and Cryptography*, vol. 12, no. 2, pp. 161–201, 1997.
[9] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.
[10] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. on Information Theory*, vol. 29, no. 1, pp. 35–41, 1983.
[11] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," *J. of Cryptology*, vol. 4, no. 73, pp. 123–134, 1991.
[12] P. D. Seymour, "On secret-sharing matroids," *J. of Combinatorial Theory, Series B*, vol. 56, pp. 69–73, 1992.
[13] F. Matúš, "Matroid representations by partitions," *Discrete Mathematics*, vol. 203, pp. 169–194, 1999.
[14] D. J. A. Welsh, *Matroid Theory*. London: Academic press, 1976.
[15] P. Vamos, "On the representation of independence structures," 1968, unpublished manuscript.
[16] J. Martí-Farré and C. Padró, "On secret sharing schemes, matroids and polymatroids," 2007, journal version of [17], in preparation.
[17] ——, "On secret sharing schemes, matroids and polymatroids," in *Proc. of the Fourth Theory of Cryptography Conference – TCC 2007*, ser. Lecture Notes in Computer Science, S. Vadhan, Ed., vol. 4392. Springer-Verlag, 2007, pp. 253–272.
[18] A. Beimel and M. Franklin, "Weakly-private secret sharing schemes," in *Proc. of the Fourth Theory of Cryptography Conference – TCC 2007*, ser. Lecture Notes in Computer Science, S. Vadhan, Ed., vol. 4392. Springer-Verlag, 2007, pp. 253–272.
[19] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, "On the size of shares for secret sharing schemes," *J. of Cryptology*, vol. 6, no. 3, pp. 157–168, 1993.
[20] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii, "Nonperfect secret sharing schemes and matroids," in *Advances in Cryptology – EUROCRYPT '93*, ser. Lecture Notes in Computer Science, vol. 765. Springer-Verlag, 1994, pp. 126–141.
[21] A. Beimel, N. Livne, and C. Padró, "Matroids do not imply ideal secret sharing," 2007, submitted for publication.
[22] F. Matúš, "Two constructions on limits of entropy functions," *IEEE Trans. on Information Theory*, vol. 53, no. 1, pp. 320–330, 2007.
[23] J. Martí-Farré and C. Padró, "Secret sharing schemes with three or four minimal qualified subsets," *Designs, Codes and Cryptography*, vol. 34, no. 1, pp. 17–34, 2005.
[24] ——, "Secret sharing schemes on access structures with intersection number equal to one," *Discrete Appl. Math.*, vol. 154, no. 3, pp. 552–563, 2006.
[25] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. of the 1979 AFIPS National Computer Conference*, ser. AFIPS Conference proceedings, R. E. Merwin, J. T. Zanca, and M. Smith, Eds., vol. 48. AFIPS Press, 1979, pp. 313–317.
[26] M. O. Rabin, "Randomized Byzantine generals," in *Proc. of the 24th IEEE Symp. on Foundations of Computer Science*, 1983, pp. 403–409.
[27] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for noncryptographic fault-tolerant distributed computations," in *Proc. of the 20th ACM Symp. on the Theory of Computing*, 1988, pp. 1–10.
[28] D. Chaum, C. Crépeau, and I. Damgård, "Multiparty unconditionally secure protocols," in *Proc. of the 20th ACM Symp. on the Theory of Computing*, 1988, pp. 11–19.
[29] R. Cramer, I. Damgård, and U. Maurer, "General secure multi-party computation from any linear secret-sharing scheme," in *Advances in Cryptology – EUROCRYPT 2000*, ser. Lecture Notes in Computer Science, B. Preneel, Ed., vol. 1807. Springer-Verlag, 2000, pp. 316–334.
[30] Y. Desmedt and Y. Frankel, "Shared generation of authenticators and signatures," in *Advances in Cryptology – CRYPTO '91*, ser. Lecture Notes in Computer Science, J. Feigenbaum, Ed., vol. 576. Springer-Verlag, 1992, pp. 457–469.

[31] M. Naor and A. Wool, "Access control and signatures via quorum secret sharing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 9, no. 1, pp. 909–922, 1998.
[32] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, "On the information rate of secret sharing schemes," *Theoretical Computer Science*, vol. 154, no. 2, pp. 283–306, 1996.
[33] M. v. Dijk, "On the information rate of perfect secret sharing schemes," *Designs, Codes and Cryptography*, vol. 6, pp. 143–169, 1995.
[34] L. Csirmaz, "The size of a share must be large," *J. of Cryptology*, vol. 10, no. 4, pp. 223–231, 1997.
[35] ——, "The dealer's random bits in perfect secret sharing schemes," *Studia Sci. Math. Hungar.*, vol. 32, no. 3–4, pp. 429–437, 1996.
[36] T. Tassa, "Hierarchical threshold secret sharing," *J. of Cryptology*, vol. 20, no. 2, pp. 237–264, 2007, conference version in *Proc. of the First Theory of Cryptography Conference – TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 473–490. Springer-Verlag, 2004.
[37] T. Tassa and N. Dyn, "Multipartite secret sharing by bivariate interpolation." in *Proc. of the 33rd International Colloquium on Automata, Languages and Programming*, ser. Lecture Notes in Computer Science, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds., vol. 4052. Springer-Verlag, 2006, pp. 288–299.
[38] K. M. Martin, "Discrete structures in the theory of secret sharing," Ph.D. dissertation, University of London, 1991.
[39] J. Simonis and A. Ashikhmin, "Almost affine codes," *Designs, Codes and Cryptography*, vol. 14, no. 2, pp. 179–197, 1998.
[40] A. Beimel and B. Chor, "Universally ideal secret sharing schemes," *IEEE Trans. on Information Theory*, vol. 40, no. 3, pp. 786–794, 1994.
[41] W. Jackson, K. M. Martin, and C. M. O'Keefe, "Ideal secret sharing schemes with multiple secrets," *J. of Cryptology*, vol. 9, no. 4, pp. 233–250, 1996.
[42] S.-L. Ng and M. Walker, "On the composition of matroids and ideal secret sharing schemes," *Designs, Codes and Cryptography*, vol. 24, no. 1, pp. 49 – 67, 2001.
[43] S.-L. Ng, "A representation of a family of secret sharing matroids," *Designs, Codes and Cryptography*, vol. 30, no. 1, pp. 5–19, 2003.
[44] O. Farràs, J. Martí-Farré, and C. Padró, "Ideal multipartite secret sharing schemes," in *Advances in Cryptology – EUROCRYPT 2007*, ser. Lecture Notes in Computer Science, M. Naor, Ed., vol. 4515. Springer-Verlag, 2007, pp. 448–465.
[45] D. R. Stinson, "An explication of secret sharing schemes," *Designs, Codes and Cryptography*, vol. 2, pp. 357–390, 1992.
[46] W. Jackson and K. M. Martin, "Perfect secret sharing schemes on five participants," *Designs, Codes and Cryptography*, vol. 9, pp. 267–286, 1996.
[47] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, "Graph decomposition and secret sharing schemes," *J. of Cryptology*, vol. 8, no. 1, pp. 39–64, 1995.
[48] C. Padró and G. Sáez, "Secret sharing schemes with bipartite access structure," *IEEE Trans. on Information Theory*, vol. 46, pp. 2596–2605, 2000.
[49] A. Beimel, T. Tassa, and E. Weinreb, "Characterizing ideal weighted threshold secret sharing," in *Proc. of the Second Theory of Cryptography Conference – TCC 2005*, ser. Lecture Notes in Computer Science, J. Kilian, Ed., vol. 3378. Springer-Verlag, 2005, pp. 600–619.
[50] P. Morillo, C. Padró, G. Sáez, and J. L. Villar, "Weighted threshold secret sharing schemes," *Inform. Process. Lett.*, vol. 70, no. 5, pp. 211–216, 1999.
[51] M. Bertilsson and I. Ingemarsson, "A construction of practical secret sharing schemes using linear block codes," in *Advances in Cryptology – AUSCRYPT '92*, ser. Lecture Notes in Computer Science, J. Seberry and Y. Zheng, Eds., vol. 718. Springer-Verlag, 1993, pp. 67–79.
[52] A. Beimel and Y. Ishai, "On the power of nonlinear secret-sharing," *SIAM J. on Discrete Mathematics*, vol. 19, no. 1, pp. 258–280, 2005.
[53] A. Beimel and E. Weinreb, "Separating the power of monotone span programs over different fields," *SIAM J. on Computing*, vol. 34, no. 5, pp. 1196–1215, 2005.
[54] J. G. Oxley, *Matroid Theory*. Oxford University Press, 1992.
[55] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 1991.
[56] C. Blundo, A. D. Santis, and A. G. Gaggia, "Probability of shares in secret sharing schemes," *Inform. Process. Lett.*, vol. 72, pp. 169–175, 1999.
[57] Z. Zhang and R. W. Yeung, "On characterization of entropy function via information inequalities," *IEEE Trans. on Information Theory*, vol. 44, no. 4, pp. 1440–1452, 1998.
[58] E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes," *J. of Cryptology*, vol. 5, no. 3, pp. 153–166, 1992.
[59] K. Makarychev, Y. Makarychev, A. Romashchenko, and N. Vereshchagin., "A new class of non-Shannon type inequalities for entropies," *Communications in Information and Systems*, vol. 2, no. 2, pp. 147–166, 2002.
[60] Z. Zhang, "On a new non-Shannon type information inequality," *Communications in Information and Systems*, vol. 3, no. 1, pp. 47–60, 2003.
[61] F. Matúš, "Inequalities for Shannon entropies and adhesivity of polymatroids," in *Proc. of 9th Canadian Workshop on Information Theory*, 2005, pp. 28–31.
[62] R. Dougherty, C. Freiling, and K. Zeger, "Six new non-Shannon information inequalities," in *IEEE International Symposium on Information Theory (ISIT)*, 2006, pp. 233–236.

Amos Beimel received the B.A., M.Sc., and D.Sc. degrees in Computer Science from the Technion – Israel Institute of Technology, Haifa, in 1989, 1992, and 1996, respectively. His doctoral thesis was titled secure schemes for secret sharing and key distribution. After graduating from the Technion, he spent one year as a Postdoctoral Fellow at the Center for Discrete Mathematics and Computer Science (DIMACS) at Rutgers University, and two years as a Postdoctoral Fellow at the Division of Engineering and Applied Science at Harvard University. In 1999 he joined the Department of Computer Science at Ben-Gurion University, where he is now a senior lecturer. In 2005-2006, he spent a year as a visiting assistant professor at the University of California, Davis. His research interests include cryptography and complexity theory.

Noam Livne received the B.A. degree in 2002 and the M.Sc. degree in 2005, both in Computer Science, from the Ben Gurion University, in Beer Sheva, Israel. The work presented here was done as part of his masters thesis, which was titled the same. He is currently doing his PhD degree in the Weizmann Institute of Science in Rehovot, Israel, under the supervision of Prof. Oded Goldreich. His research interests include cryptography and complexity theory.