Universally Ideal Secret Sharing Schemes *

Amos Beimel[†] Benny Chor [‡]

Department of Computer Science
Technion, Haifa 32000, Israel

Abstract

Given a set of parties $\{1, \ldots, n\}$, an access structure is a monotone collection of subsets of the parties. For a certain domain of secrets, a secret sharing scheme for an access structure is a method for a dealer to distribute shares to the parties. These shares enable subsets in the access structure to reconstruct the secret, while subsets not in the access structure get no information about the secret. A secret sharing scheme is *ideal* if the domains of the shares are the same as the domain of the secrets. An access structure is *universally ideal* if there exists an ideal secret sharing scheme for it over every finite domain of secrets. An obvious necessary condition for an access structure to be universally ideal is to be ideal over the binary and ternary domains of secrets. In this work, we prove that this condition is also sufficient. We also show that being ideal over just one of the two domains does not suffice for universally ideal access structures. Finally, we give an exact characterization for each of these two conditions.

Index terms: Secret Sharing, Ideal access structures, Matroids, Cryptography

1 Introduction

A secret sharing scheme involves a dealer who has a secret taken from a finite domain, a finite set of n parties, and a collection $\mathcal{A}$ of subsets of the parties called the access structure. A secret-sharing scheme for $\mathcal{A}$ is a method by which the dealer distributes shares to the parties such that any subset in $\mathcal{A}$ can reconstruct the secret from its shares, and any subset not in $\mathcal{A}$ cannot reveal any partial information about the secret in the information theoretic sense (such schemes are sometimes referred to as *perfect*). 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. If the subsets that can reconstruct the secret are all the sets whose cardinality is at least a certain threshold t, then the scheme is called t out of n threshold secret sharing scheme. Secret sharing schemes were first introduced for the threshold case by Blakley [3] and by Shamir [15]. Secret sharing schemes for general access structures were first

*A preliminary version of this paper appears in Advances in Cryptology – Crypto '92 proceedings, Springer-verlag, E.F. Brickell, ed.

[†]email: beimel@cs.technion.ac.il

[‡]Supported by the Fund for Promotion of Research at the Technion. email: benny@cs.technion.ac.il

defined by Ito, Saito and Nishizeki in [8]. Given any monotone access structure, they show how to build a secret sharing scheme that realizes the access structure. Benaloh and Leichter [1] describe a more efficient way to realize general secret sharing schemes.

Even with the more efficient scheme of [1], most general access structures require shares of exponential size: Even if the domain of the secret is binary, the shares are strings of length $2^{\Theta(n)}$, where n is the number of participants. The question of lower bounds on the size of shares for some (explicit or random) access structures is still open. On the other hand, 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. An access structure is called $m-$ideal if there is an ideal secret sharing scheme which realizes the access structure over a domain of secrets of size m.

Brickell [5] was the first to introduce the notion of ideal access structures. Brickell and Davenport [6] have shown that such structures are closely related to matroids over a set containing the participants plus the dealer. They give a necessary condition for an access structure to be $m-$ideal (being a matroid) and a somewhat stronger sufficient condition (the matroid should be representable over a field or algebra of size m). Certain access structures, such as the threshold ones, are $m-$ideal for m that is at least n. However, for domains of secrets which contain m elements where m is smaller then n, the threshold access structures are *not* $m-$ideal (for threshold t such that $2 \leq t \leq n-1$), as proved by Karnin, Greene and Hellman [10]. This qualitative result was improved by Kilian and Nisan [11], who showed that the t out of n threshold secret sharing scheme over a binary domain of secrets requires shares from a domain that is at least of size $n-t+2$ (for $2 \leq t \leq n-1$).

We say that an access structure is *universally* ideal if for every positive integer $m \geq 2$, the access structure is $m-$ideal. Universally ideal access structures are particularly convenient to work with because they are very efficient no matter what the domain of secrets is. A simple example of a universally ideal access structure is the n out of n threshold access structure. In this work we give a complete characterization of universally ideal access structures. Our work builds upon results of Brickell and Davenport which relate ideal access structures to matroids, as well as some known results from matroid theory. An obvious necessary condition for an access structure to be universally ideal is to be both $2-$ideal and $3-$ideal. Interestingly, our main result states that this condition is also sufficient. We give examples which demonstrate that just one of these two requirements is not a sufficient condition to be universally ideal.

The remaining of this paper is organized as following. In section 2 we give formal definitions and quote the results of Brickell and Davenport. Section 3 states our main theorem, and details its proof. Section 4 illustrates some clarifying examples.

2 Definitions and Related Results

This section contains formal definitions of secret sharing schemes, some background on matroids, and known related results, that will be used in the rest of this paper.

2.1 Secret Sharing Schemes

Definition 2.1: Let $\{1,\ldots,n\}$ be a set, called the set of parties. A collection $\mathcal{A} \subseteq 2^{\{1,\ldots,n\}}$ is monotone if $B \in \mathcal{A}$ and $B \subseteq C$ implies $C \in \mathcal{A}$. An *access structure* is a monotone collection

$\mathcal{A}$ of non-empty subsets of $\{1,\ldots,n\}$. The sets in $\mathcal{A}$ are called the *reconstructing sets.*

Definition 2.2: Let $S = \{0,\ldots,m-1\}$ be a finite set of secrets, let $\mathcal{A} \subseteq 2^{\{1,\ldots,n\}}$ be an access structure, and let R be a set of random input. Let $\{\mu_s\}_{s\in S}$ be a set of of probability distributions on the random inputs R (that is, for every $s \in S$, $\mu_s : R \to [0,1]$ is a probability distribution). A *secret-sharing scheme* Π with domain of secrets S is a mapping $\Pi : S \times R \to S_1 \times S_2 \times \ldots \times S_n$ from the cross product of the secrets and the random inputs to a set of n-tuples (the shares). We denote the share of party i by $\Pi_i(s,r)$. A secret-sharing scheme Π realizes an access structure $\mathcal{A}$ if following two requirements hold:

1. The secret s can be reconstructed by any subset in $\mathcal{A}$. That is, for any subset $B \in \mathcal{A}$ ($B = \left\{i_1,\ldots,i_{|B|}\right\}$), there exists a function $h_B : S_{i_1} \times \ldots \times S_{i_{|B|}} \to S$ such that for every random input r, if $\Pi(s,r) = (s_1,s_2,\ldots,s_n)$, then $h_B(s_{i_1},\ldots,s_{i_{|B|}}) = s$.

2. Every subset not in $\mathcal{A}$ cannot reveal any partial information about the secret (in the information theoretic sense). Formally, for any subset $B \notin \mathcal{A}$, for every two secrets $a,b \in S$, and for every possible shares $\{s_i\}_{i\in B}$:

$$\Pr_{\mu_a(r)}[\bigwedge_{i\in B} \Pi_i(a,r) = s_i] = \Pr_{\mu_b(r)}[\bigwedge_{i\in B} \Pi_i(b,r) = s_i] .$$

Given a collection $\Gamma \subseteq 2^{\{1,\ldots,n\}}$ the closure of Γ, denoted by $\mathrm{cl}(\Gamma)$, is the minimum collection that contains Γ and is monotone. Given an access structure $\mathcal{A}$, we denote $\mathcal{A}_m$ to be the collection of minimal sets of $\mathcal{A}$. That is, $B \in \mathcal{A}_m$ if $B \in \mathcal{A}$, and for every $C \subsetneq B$ it holds that $C \notin \mathcal{A}$. If $\mathcal{A} = \{B : |B| \geq t\}$, then a secret sharing scheme for $\mathcal{A}$ is called a t out of n threshold secret sharing scheme, and the access structure $\mathcal{A}$ is called the t out of n threshold access structure.

Definition 2.3: An access structure $\mathcal{A}$ is a *non-degenerate* access structure if for every $i \in \{1,\ldots,n\}$ there exists $B \in \mathcal{A}_m$ such that $i \in B$. That is, every party is an element of at least one minimal subset that can reconstruct the secret, therefore his share is "essential".

Definition 2.4: A secret sharing scheme $\Pi : S \times R \to S_1 \times \ldots \times S_n$ is $m-$*ideal* if $|S_1| = |S_2| = \ldots = |S_n| = |S| = m$. That is, the domain of the shares of each party has the same size as the domain of the secrets, and this domain contains m elements. An *access structure $\mathcal{A}$ is $m-$ideal* if there exists a $m-$ideal secret sharing scheme that realizes $\mathcal{A}$. An access structure $\mathcal{A}$ is *universally ideal* if for every positive integer m, the access structure $\mathcal{A}$ is $m-$ideal.

2.2 Matroids

In this subsection we recall the definition of matroids for the sake of completeness. Matroids are well studied combinatorial objects (see for example Welsh [18]). A matroid is an axiomatic abstraction of linear independence. We give here one of the equivalent axiom systems that define matroids. A matroid $\mathcal{T} = (V,\mathcal{I})$ is a finite set V and a collection $\mathcal{I}$ of subsets of V such that **(I1)** through **(I3)** are satisfied.

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $X \in \mathcal{I}$ and $Y \subseteq X$ then $Y \in \mathcal{I}$.

(I3) If X,Y are members of $\mathcal{I}$ with $|X| = |Y| + 1$, then there exists $x \in X \setminus Y$ such that $Y \cup \{x\} \in \mathcal{I}$.

For example every finite vector space is a matroid, in which V is the set of vectors and $\mathcal{I}$ is the collection of the linearly independent sets of vectors. The elements of V are called the *points* of the matroid and the sets in $\mathcal{I}$ are called *independent sets.* A *dependent set* of a matroid is any subset of V that is not independent. The minimal dependent sets are called *circuits.* A matroid is said to be *connected* if for every two elements of V, there is a circuit containing both of them. The maximal independent sets are called *bases.* Axiom **I3** implies that in every matroid all bases have the same cardinality. This cardinality is called the *rank* of the matroid.

Definition 2.5: A matroid is *representable* over a field $\mathcal{F}$ if there exists a dependence preserving mapping from the points of the matroid into the set of vectors of a vector space over the field. In other words, there exist k and a mapping $\phi : V \to \mathcal{F}^k$ that satisfies:

$A \subseteq V$ is a dependent set of the matroid if and only if $\phi(A)$ is linearly dependent.

For more background on matroids the reader can refer to [18]. Discussion on representable matroids can be found in [16].

2.3 Relation between Secret Sharing Schemes and Matroids

The next definition relates access structures and matroids.

Definition 2.6: Let $\mathcal{A}$ be an access structure with n parties $\{1, \ldots, n\}$ and let $\mathcal{T} = (V, \mathcal{I})$ be a connected matroid. We say that the matroid $\mathcal{T}$ is *appropriate* for the access structure $\mathcal{A}$ if $V = \{0, \ldots, n\}$ and

$$\mathcal{A} = \mathrm{cl}(\{C \setminus \{0\} : 0 \in C \text{ and } C \text{ is a minimal dependent set of } \mathcal{T}\})$$

That is, the minimal sets of the access structure $\mathcal{A}$ correspond to the minimal dependent sets in the matroid which contain 0. Informally, the point 0 is added to the set $\{1, \ldots, n\}$ to "play the role" of the dealer.

There are various properties which the collection of minimal dependent sets in a matroid must satisfy, and these properties do not necessarily hold for an arbitrary access structure. Therefore not every access structure has an appropriate matroid. But if a connected matroid is appropriate for an access structure, then it is the only matroid with this property (see [18] Theorem 5.4.1, and [13, 9]). Brickell and Davenport [6] have found relations between the two notions when $\mathcal{A}$ is an ideal access structure. The next two theorems almost characterize $m-$ideal access structures. The formulation of Theorem 2.7 is implicit in [6] and explicit in the works of Jackson and Martin [9, 13].

Theorem 2.7: [6, 9, 13](necessary condition) If a non-degenerate access structure $\mathcal{A}$ is $m-$ideal for some positive integer m, then there exists a connected matroid $\mathcal{T}$ that is appropriate for $\mathcal{A}$.

Theorem 2.8: [6](sufficient condition) [1] Let q be a prime power, and $\mathcal{A}$ be a non-degenerate access structure. Suppose that there is a connected matroid $\mathcal{T}$ that is appropriate for $\mathcal{A}$. If $\mathcal{T}$ is representable over the field GF(q), then $\mathcal{A}$ is $q-$ideal.

The two theorems of Brickell and Davenport almost characterize $q-$ideal access structures for q which is a prime power. However, there is still a remaining gap. If there is a connected matroid $\mathcal{T}$ that is appropriate for $\mathcal{A}$ but is not representable over the field GF(q), then the theorems do not determine whether or not $\mathcal{A}$ is $q-$ideal. Recently, Seymour [14] has proved that there exists an access structure which has an appropriate matroid, but is *not* $m-$ideal for any integer m. Therefore the necessary condition of [6] is not sufficient (even in a weak sense).

3 The Characterization Theorem

In this section we give a complete characterization for universally ideal access structure, and prove it. We recall that an access structure $\mathcal{A}$ is universally ideal if it is $m-$ideal for every integer $m \geq 2$. Our main result is:

Theorem 3.1: An access structure $\mathcal{A}$ is universally ideal if and only if $\mathcal{A}$ is binary-ideal (2-ideal) and ternary-ideal (3-ideal).

The proof of the theorem proceeds along the following lines: We strengthen Theorem 2.7 of Brickell and Davenport for ideal schemes over the binary and ternary domains of secrets. We show that over these domains, every reconstruction function (of the secrets from the shares) can be expressed as a linear combination of the shares of the parties. This enables us to show that if an access structure $\mathcal{A}$ is binary ideal, then there is a matroid $\mathcal{T}$ that is appropriate for $\mathcal{A}$ and is representable over the binary field. The same result is proved for the ternary field. Then, using a known result from matroid theory, we conclude that if an access structure $\mathcal{A}$ is binary and ternary ideal, then there is a matroid $\mathcal{T}$ appropriate for $\mathcal{A}$ which is representable over *every* field. Thus, by Theorem 2.8 of Brickell and Davenport, the access structure is $q-$ideal for every prime power q. Using the Chinese remainder Theorem, $\mathcal{A}$ is $m-$ideal over any finite domain, namely is universally ideal, as desired.

3.1 Dependent and Independent Sets with Respect to Secret Sharing Schemes

Definition 3.2: Let Π be a secret sharing scheme for n parties $\{1, \ldots, n\}$, and the dealer which we denote by 0. The secret will be considered as the share of party 0 – the dealer – and will denoted by $\Pi_0(s,r)$. Let $B \subseteq \{0, \ldots, n\}$ and $i \in \{0, \ldots, n\} \setminus B$. The parties in B *cannot reveal any information* about the share of i if for every distribution on the secrets, every possible shares $\{s_j\}_{j \in B}$, and every possible shares s_i, s_i':

$$\Pr_{s,\mu_s(r)}[\ \Pi_i(s,r) = s_i \mid \bigwedge_{j \in B} \Pi_j(s,r) = s_j\ ] = \Pr_{s,\mu_s(r)}[\ \Pi_i(s,r) = s_i' \mid \bigwedge_{j \in B} \Pi_j(s,r) = s_j\ ]$$

In this case we say that i is independent of B with respect to Π.

[1] The Theorem in [6] had a slightly weaker condition, which we omit for simplicity.

This definition is related to the requirement for non-reconstructing sets in secret sharing schemes (definition 2.2). The reader can verify that if $B \notin \mathcal{A}$ $(B \subseteq \{1, \ldots, n\})$, then in every secret sharing scheme realizing $\mathcal{A}$, party 0 (the dealer) is independent of the set B. The difference between this definition and definition 2.2 is that here we treat the secret as the share of party 0, therefore we have to define a distribution on the secrets as well.

Definition 3.3: A set $B = \left\{j_1, \ldots, j_{|B|}\right\}$ can *reconstruct the share* of party i if there exists a function $h : S_{j_1} \times \ldots \times S_{j_{|B|}} \to S_i$ such that for every $s \in S_i$ and every $r \in R$ (satisfying $\mu_s(r) > 0$) it holds that:

$$h(\ \Pi_{j_1}(s, r), \ldots, \Pi_{j_{|B|}}(s, r)\ ) = \Pi_i(s, r)\ .$$

In this case we say that i depends on B with respect to Π.

Definition 3.4: Let Π be a secret sharing scheme. We say that a subset $B \subseteq \{0, 1, \ldots, n\}$ is *dependent* with respect to Π if there exists an $i \in B$ such that i depends on $B \setminus \{i\}$. A subset $B \subseteq \{0, \ldots, n\}$ is *independent* if for every $i \in B$, i is independent of $B \setminus \{i\}$ with respect to Π.

Notice that the notions of dependent and independent set with respect to a given secret sharing schemes are *not* complementary. There could be a subset B of parties which can neither reconstruct the share of any of its members (and thus B in not dependent), yet can reveal some information on the share of one of its members (and thus B is not independent). However, for *ideal* secret sharing scheme, the following theorem of Brickell and Davenport [6] establishes the desired relation between the two notions.

Theorem 3.5: [6] Let Π be an ideal secret sharing scheme realizing a non-degenerate access structure $\mathcal{A}$ with n parties $\{1, \ldots, n\}$ over some domain of secrets S. Let $B \subseteq \{0, \ldots, n\}$. Then

1. Every party i either depends on the subset B with respect to Π, or is independent of B.
2. The subset B is independent with respect to Π if and only if B is an independent set in $\mathcal{T}$, the appropriate matroid for $\mathcal{A}$.

3.2 Linear Secret Sharing Schemes

Definition 3.6: Let q be a prime power, and Π a $q-$ideal secret sharing scheme. We say that Π is *linear* if for every set that is dependent with respect to Π, the reconstruction function is linear. That is, for every $B \subseteq \{0, \ldots, n\}$ and every $0 \leq i \leq n$ such that $i \notin B$ and i depends on B with respect to Π, there are constants $\{\alpha_j\}_{j \in B}$, σ such that for every secret $s \in \mathrm{GF}(q)$ and choice of random inputs $r \in R$

$$\Pi_i(s, r) = \sigma + \sum_{j \in B} \alpha_j \Pi_j(s, r)$$

where the constants and the arithmetic is in $\mathrm{GF}(q)$.

For example, we describe the t out of n threshold secret sharing scheme of Shamir [15], and show that it is linear. Let q be the size of the domain of secrets, where q is a prime-power that is bigger than n (the number of parties in the access structure). Let $s \in \mathrm{GF}(q)$ be the secret. The dealer chooses independently with uniform distribution $t-1$ random elements in GF(q), which we denote by $r_1,\ldots,r_{t-1}$. These elements and the secret s define a polynomial

$$p(x) = r_{t-1}x^{t-1} + r_{t-2}x^{t-2} + \ldots + r_1 x + s$$

We observe that $p(0) = s$. The dealer gives the share $p(i)$ to party i. Now each set of cardinality at least t can reconstruct $p(x)$ by interpolation. That is, the set $\{i_1,\ldots,i_t\}$ holding the shares $\{s_{i_1},\ldots,s_{i_t}\}$, computes the polynomial

$$p(x) = \sum_{j=1}^{t} s_{i_j} \prod_{k\neq j} \frac{i_k - x}{i_k - i_j}.$$

The secret is reconstructed by substituting 0 for x in this polynomial. Notice that the secret is a linear combination of the shares $\{s_{i_1},\ldots,s_{i_t}\}$, where the coefficient of s_{i_j} is $\prod_{k\neq j}\frac{i_k}{i_k-i_j}$. The share of party ℓ is computed by substituting ℓ in the polynomial, and, in a similar manner, it is also a linear combination of the other shares and the secret.

The sufficient condition of Brickell and Davenport [6] (theorem 2.8) states that if an access structure $\mathcal{A}$ has an appropriate matroid which is representable over GF(q), then $\mathcal{A}$ is $q-$ideal. The scheme in their proof is a linear $q-$ideal secret sharing scheme, using our terminology. Our next lemma states the reverse direction.

Lemma 3.7: If an access structure $\mathcal{A}$ has a linear $q-$ideal secret sharing scheme, then $\mathcal{A}$ has an appropriate matroid which is representable over GF(q).

Proof: By Theorem 2.7 there is a matroid which is appropriate for $\mathcal{A}$. Let Π be a linear $q-$ideal secret sharing scheme for the access structure $\mathcal{A}$. Using Π, we will construct a dependence preserving mapping ϕ from the set of points of the matroid, $\{0,\ldots,n\}$, into a vector space over GF(q).

The mapping ϕ will be constructed in two stages. In the first stage we will map $V=\{0,\ldots,n\}$ to GF$(q)^{q\times|R|}$, where R is the source of randomness used in Π. (For simplicity of notations, we assume that R is finite, but this assumption is not essential.) For every $a\in V$ we define

$$\phi_1(a) = (\ \Pi_a(0,r_1), \Pi_a(0,r_2), \ldots, \Pi_a(q-1, r_{|R|})\ )$$

intuitively $\phi_1(a)$ describes the shares of party a with respect to all secrets and all random inputs. For $\sigma\in$ GF(q), let $\vec{\sigma}$ denote the vector in GF$(q)^{q\times|R|}$ in which every coordinate equals σ. By Theorem 3.5 The set $B\subseteq\{0,\ldots,n\}$ is dependent with respect to $\mathcal{T}$ if and only if B is dependent with respect to the scheme Π, i.e. if there exists a party $i\in B$ such that the parties in $B\setminus\{i\}$ can reconstruct the share of i. Since Π is linear, the reconstruction function is linear, or in other words there exists constants $\{\alpha_j\}_{j\in B\setminus\{i\}}, \sigma$ (all in GF(q)) such that for every secret s and every choice of random input r

$$\Pi_i(s,r) = \sum_{j\in B\setminus\{i\}} \alpha_j \Pi_j(s,r) - \sigma$$

This condition is equivalent to $\sum_{j\in B}\alpha_j\phi_1(j) = \vec{\sigma}$, where $\alpha_i = -1$. Therefore, the mapping ϕ_1 satisfies: The set $B\subseteq\{0,\ldots,n\}$ is dependent with respect to the matroid $\mathcal{T}$ if and only if there exist constants $\{\alpha_j\}_{j\in B}, \sigma\in$ GF(q) (with at least one α_j not equal to zero) such that $\sum_{j\in B}\alpha_j\phi_1(j)=\vec{\sigma}$. The mapping ϕ_1 almost satisfies the requirements of a dependence preserving mapping. The problem is that the linear combination of dependent elements should sum to $\vec{0}$, while ours sums to $\vec{\sigma}$ which is not necessary $\vec{0}$.

We now continue to the second stage of the construction of ϕ, which will fix the problem of the first stage. Let us denote by Y the following linear subspace of $\mathrm{GF}(q)^{q\times|R|}$,

$$Y = \mathrm{span}\left\{\vec{1}, \phi_1(0), \phi_1(1), \ldots, \phi_1(n)\right\},$$

and let us denote the rank of Y by $t+1$. Let $\phi_2 : Y \to \mathrm{GF}(q)^t$ be a linear mapping with $\mathrm{kernel}(\phi_2) = \mathrm{span}\left\{\vec{1}\right\}$, i.e. $\phi_2(x) = 0$ if and only if $x = \vec{\sigma}$ for some $\sigma \in \mathrm{GF}(q)$. Such mapping exists by elementary linear algebra arguments. For every $X \subseteq Y$ the set $\{\phi_2(x) : x \in X\} \subseteq \mathrm{GF}(q)^t$ is linearly dependent if and only if there is a non-zero combination of the elements in X that is in $\mathrm{span}\left\{\vec{1}\right\}$:

$$\textstyle\sum_{x\in X} \alpha_x x = \vec{\sigma} \text{ for some } \sigma \in \mathrm{GF}(q) \text{ and } \alpha_x \in \mathrm{GF}(q),\ \alpha_x \text{ not all identically } 0.$$

We conclude that these two mappings ϕ_1 and ϕ_2 have the property that $B \subseteq V$ is dependent in $\mathcal{T}$ if and only if $\phi_2 \circ \phi_1(B)$ is linearly dependent in $\mathrm{GF}(q)^t$. Thus $\phi = \phi_2 \circ \phi_1$ is a dependence preserving mapping, and by definition the appropriate matroid $\mathcal{T}$ is representable over $\mathrm{GF}(q)$. $\square$

3.3 Sensitive Functions

By definition 3.3 a party i depends on a subset B if there exists a reconstruction function of the share of party i from the shares of the parties in B. In this subsection we study the reconstruction functions in ideal secret sharing schemes. We show that these functions must be sensitive to every change in any of their arguments.

Definition 3.8: We say that a function $f : S^t \to S$ is *component sensitive* if for every $1 \le i \le t$, every $s_1, \ldots, s_{i-1}, s_i, s'_i, s_{i+1}, \ldots, s_t \in S$ ($s'_i \neq s_i$):

$$f(s_1, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_t) \neq f(s_1, \ldots, s_{i-1}, s'_i, s_{i+1}, \ldots, s_t).$$

In other words, every change in the value of one variable of f, changes the value of f.

Lemma 3.9: Let Π be a $q-$ideal secret sharing scheme. Denote $S = \{0, \ldots, q-1\}$. Let $i \in \{0, \ldots, n\}$, and $B \subseteq \{0, \ldots, n\}$ be a minimal subset such that i depends on B and $i \notin B$. Let $f : S^{|B|} \to S$ be the reconstruction function of the $i-$th share from the shares of the parties in B. Then:

1. The reconstructing function f is defined over all the domain $S^{|B|}$.

2. The reconstructing function f is component sensitive.

Proof: Without loss of generality we assume that $B = \{1, 2, \ldots, t\}$. First, we prove that f is defined over all $S^{|B|}$. That is, we prove that for every vector of shares in S^t there exists a secret s and a random input r with $\mu_s(r) > 0$, such that the dealer, having s and r, will distribute this vector of shares to the parties in B. Assume, by way of contradiction, that f is not defined for the vector of shares $< s_1, s_2, \ldots, s_t >$. There exists an index j ($1 \le j \le t$) and shares $s'_j, \ldots, s'_t \in S$

such that $f(s_1, \ldots, s_{j-1}, s'_j, s'_{j+1}, \ldots, s'_t)$ is well defined. This is true since we can choose $j = 1$ and the shares will be any shares that are distributed to the parties. Let j be the maximal such index. It holds that

$$\Pr_{s,\mu_s(r)}[\ \Pi_j(s,r) = s_j \mid \bigwedge_{1 \leq k \leq j-1} \Pi_k(s,r) = s_k\ ] = 0$$

But

$$\Pr_{s,\mu_s(r)}[\ \Pi_j(s,r) = s'_j \mid \bigwedge_{1 \leq k \leq j-1} \Pi_k(s,r) = s_k\ ] > 0$$

Therefore the parties in $\{1, \ldots, j-1\}$ can reveal some partial information about the share of party j, and by definition 3.2, this means that party j is not independent of the set $B \setminus \{j\}$. Since the scheme Π is $q-$ideal, Theorem 3.5 implies that party j depends on the set $B \setminus \{j\}$, so the parties in $B \setminus \{j\}$ can reconstruct the share of party j. Therefore the parties in $B \setminus \{j\}$ can also reconstruct the share of party i, contradicting the choice of B as a minimal set that i depends upon.

After establishing the fact that f is defined over all $S^{|B|}$, assume now, by way of contradiction, that f is *not* component sensitive. In other words, there is some $j \in B$, shares $s_1, \ldots, s_{j-1}, s_j, s'_j, s_{j+1}, \ldots, s_t \in S$, and share $s_i \in S$ such that $s_j \neq s'_j$ and

$$f(s_1, \ldots, s_{j-1}, s_j, s_{j+1}, \ldots, s_t) = f(s_1, \ldots, s_{j-1}, s'_j, s_{j+1}, \ldots, s_t) = s_i.$$

Since f is defined over all $S^{|B|}$, there exist secrets $s, s' \in S$ and random inputs $r, r' \in R$ with $\mu_s(r) > 0, \mu_{s'}(r') > 0$ such that:

- For every $k \in B \setminus \{j\}$ it holds that $\Pi_k(s,r) = \Pi_k(s',r') = s_k$.
- $\Pi_j(s,r) = s_j$ and $\Pi_j(s',r') = s'_j$, which means that $\Pi_j(s,r) \neq \Pi_j(s',r')$.
- $\Pi_i(s,r) = \Pi_i(s',r') = s_i$.

The set $B \setminus \{j\}$, holding the vector of shares $(s_1, \ldots, s_{j-1}, s_{j+1}, \ldots, s_t)$, reconstructs the same value of the share of party i for two different values of the share of party j. Since there are only q possible values for the $j-$th share, then there are at most $q-1$ possible shares for party i, i.e. there are $s_i, s'_i \in S$ such that

$$\Pr_{s \in S,\mu_b(r)}[\ \Pi_i(s,r) = s'_i \mid \bigwedge_{k \in B \setminus \{j\}} \Pi_k(s,r) = s_k\ ] = 0$$

While

$$\Pr_{s \in S,\mu_b(r)}[\ \Pi_i(s,r) = s \mid \bigwedge_{k \in B \setminus \{j\}} \Pi_k(s,r) = s_k\ ] > 0$$

Which means that the shares in $B \setminus \{j\}$ do reveal some partial information about the $i-$th share. Therefore i is not independent of $B \setminus \{j\}$. By Theorem 3.5, this implies that i depends on $B \setminus \{j\}$, contradicting the fact that B was a minimal set such that i depends upon. $\square$

3.4 Binary and Ternary Domains of Secrets

In this subsection we show that the only component sensitive functions for the binary and for the ternary domains are linear. This is used to exactly characterize binary-ideal and ternary ideal access structures. We start with the binary case.

Lemma 3.10: Let $f : \mathrm{GF}(2)^t \to \mathrm{GF}(2)$ be a component sensitive function. Then f can be expressed as a linear function with non-zero coefficients over GF(2):

$$f(x_1, \ldots, x_t) = \sigma + \sum_{i=1}^{t} x_i \quad (\ \sigma \in \{0,1\}\ ).$$

Proof: Stated differently, this lemma claims that XOR and not-XOR are the only component sensitive functions over GF(2). Suppose, without loss of generality, that $f(0, \ldots, 0) = 0$. In this case we show that $f(x_1, \ldots, x_t) = \sum_{i=1}^{t} x_i = XOR(x_1, \ldots, x_t)$. Given an element $< x_1, \ldots, x_t >$ $\in \mathrm{GF}(q)^t$ of Hamming weight k, set up a sequence of elements in $\mathrm{GF}(2)^t$ which starts at $< 0, 0, \ldots, 0 >$, ends at $< x_1, \ldots, x_t >$, has length $k+1$, and successive elements in this sequence are at Hamming distance 1. Since f is component sensitive and its range is binary, we get that for the $\ell-$th element in the sequence ($\ell = 0, 1, \ldots, k$) f attains the value $\ell \bmod 2$. In particular, for the $k-$th element, $f(x_1, \ldots, x_t) = k \bmod 2 = XOR(x_1, \ldots, x_t)$. □

We use Lemma 3.10 to give an exact characterization of binary-ideal access structures.

Corollary 3.11: An access structure $\mathcal{A}$ is binary-ideal if and only if there is a matroid which is representable over GF(2) and is appropriate for $\mathcal{A}$.

Proof: Let Π be a binary-ideal secret sharing scheme which realizes the access structure $\mathcal{A}$. By lemma 3.9 the reconstruction function of every dependent set is component sensitive. Therefore by lemma 3.10 every reconstruction function is linear over GF(2), so by definition 3.6, Π is a linear scheme. By lemma 3.7, we conclude that if $\mathcal{A}$ is binary-ideal then $\mathcal{A}$ has an appropriate matroid which is representable over GF(2). The other direction is implied by the sufficient condition of Brickell and Davenport [6] (theorem 2.8). □

The next lemma parallels Lemma 3.10, this time for the ternary case.

Lemma 3.12: Let $f : \mathrm{GF}(3)^t \to \mathrm{GF}(3)$ be a component sensitive function. Then f can be expressed as a linear function with non-zero coefficients over GF(3):

$$f(x_1, \ldots, x_t) = \sigma + \sum_{i=1}^{t} \alpha_i x_i \quad (\alpha_i \neq 0 \text{ for all } i).$$

Proof: The proof relies on the observation that any partial assignment to the variables of a component sensitive function results in a new component sensitive function (of the remaining variables). In addition, a component sensitive function of *one* variable is a permutation of its domain.

For any finite field $\mathrm{GF}(q)$, any function which maps $\mathrm{GF}(q)^t$ into $\mathrm{GF}(q)$ can be expressed as a multi-variable polynomial over the field, in which every monomial of f contains variables whose powers do not exceed $q-1$ (since $x^q \equiv x$ for every x in $\mathrm{GF}(q)$). In our case $q = 3$ so the powers do not exceed 2.

We first show that no term in the polynomial f contains a variable of degree 2. Suppose, without loss of generality, that x_1^2 appears in some monomial. The polynomial f will have the form:

$$x_1^2 \cdot p_1(x_2, \ldots, x_n) + x_1 \cdot p_2(x_2, \ldots, x_n) + p_3(x_2, \ldots, x_n)$$

where the polynomial p_1 is not identically zero, and p_2, p_3 are arbitrary polynomials. Hence there exists a substitution to the variables $x_2, \ldots, x_n$ such that the value of p_1 after the substitution is non-zero. This substitution to f yields a polynomial in x_1, of the form $ax_1^2 + bx_1 + c$, where a, the coefficient of x_1, is non–zero. By the observation mentioned above, the resulting function of x_1 should also be component sensitive namely a permutation. It is not hard to check that any degree 2 polynomial over GF(3) is not a permutation. (Every polynomial of the form $a \cdot x_1 + b$ where $a \neq 0$ is a permutation. There are 6 such polynomials and there are 6 permutations over GF(3), therefore every degree 2 polynomial cannot be a permutation.) Thus f contains no variable of degree 2, so all its monomials are multi-linear.

Suppose f has a monomial with two or more variables. Take a minimum length monomial containing two variables, and assume that these variables are x_1 and x_2. We set all variables in this minimum length monomial (except x_1 and x_2) to 1, and all remaining variables to 0. This leaves us with a function of x_1 and x_2 of the form $ax_1x_2 + bx_1 + cx_2 + d$, where $a \neq 0$. This two argument function should also be component sensitive. But rewriting it as $x_1(ax_2 + b) + cx_2 + d$, and setting $x_2 = -b/a$, we get a function of x_1 which does not depend on x_1, and in particular is not component sensitive – a contradiction.

Therefore f contains no degree 2 variables and no monomials with two or more variables, and so is linear, of the form $\sigma + \sum_{i=1}^{t} \alpha_i x_i$. All α_i must be non-zero, for otherwise f would not depend on the corresponding variable. $\square$

We remark that GF(3) is the largest field where every component sensitive function is linear. Already for GF(4), there are $4! = 24$ component sensitive functions of one variable (permutations), but only $3 \cdot 4 = 12$ non-constant linear functions. Now using the same arguments as in the proof of Corollary 3.11 (for the binary case), we conclude with the following characterization of ternary-ideal access structures.

Corollary 3.13: An access structure $\mathcal{A}$ is ternary-ideal if and only if there is a matroid which is representable over $GF(3)$ and is appropriate for $\mathcal{A}$.

3.5 Conclusion of the Proof

We saw that representability over GF(2) determines if an access structure is binary-ideal, and representability over GF(3) determines if an access structure is ternary-ideal. Therefore, if an access structure is both binary-ideal and ternary-ideal, then it has an appropriate matroid that is representable over GF(2) and over GF(3). The next proposition is due to Tutte [17] and can be found in Truemper [16] Theorem 9.2.9. The proposition states strong implications of the representability over the two finite fields. It will be used to complete the proof of our main theorem.

Proposition 3.14: *[17]* A matroid $\mathcal{T}$ is representable over GF(2) and over GF(3) if and only if $\mathcal{T}$ is representable over any field.

Using this proposition we get:

Corollary 3.15: If an access structure $\mathcal{A}$ is binary-ideal and ternary-ideal then for every q such that q is a prime power, $\mathcal{A}$ is $q-$ideal.

Proof: If an access structure $\mathcal{A}$ is binary-ideal and ternary-ideal, then by corollaries 3.11 and 3.13 the access structure $\mathcal{A}$ has an appropriate matroid $\mathcal{T}$ that is representable over GF(2) and it has an appropriate matroid that is representable over GF(3). Remember that there can be only one appropriate matroid for $\mathcal{A}$, therefore $\mathcal{A}$ has an appropriate matroid $\mathcal{T}$ that is representable over both fields. Hence proposition 3.14 implies that $\mathcal{T}$ is representable over any field. From Theorem 2.7 we conclude that the access structure $\mathcal{A}$ is ideal over any finite field, i.e. $\mathcal{A}$ is $q-$ideal for every prime-power q. $\square$

Corollary 3.16: If an access structure $\mathcal{A}$ is binary-ideal and ternary-ideal then for every positive integer m, the access structure $\mathcal{A}$ is $m-$ideal.

Proof: Let S be a finite domain of secrets of size m. Let $m = p_1^{i_1} \cdot p_2^{i_2} \cdot \ldots \cdot p_t^{i_t}$ where p_j are distinct primes. Given a secret $s \in S$, we use the $p_j^{i_j}$-ideal secret sharing scheme to share $s \bmod p_j^{i_j}$ for every $1 \leq j \leq t$, independently. Every subset of parties $B \in \mathcal{A}$ can reconstruct $s \bmod p_j^{i_j}$, and so, using the Chinese remainder Theorem, they can reconstruct the secret, s. Since for each j the secret $s \bmod p_j^{i_j}$ is shared independently, then every subset $B \notin \mathcal{A}$ does not get any partial information about the secret s. $\square$

This last corollary is a restatement of Theorem 3.1, so it completes the arguments in the proof of our main result.

4 Examples and Concluding Remarks

In this section we formulate several known constructions from matroid theory as ideal access structures. Our first two examples show that the condition of Theorem 3.1 cannot be relaxed: Being either just $2-$ideal or just $3-$ideal is not sufficient for being universally ideal. Then, we demonstrate how graphic and cographic matroids give rise to interesting classes of universally ideal access schemes.

Example 4.1: (the 2 out of 3 threshold access structure) We recall that the 2 out of 3 threshold access structure is the access structure with 3 parties in which every two parties together can reconstruct the secret, and every party by itself does not know anything about the secret. Karnin, Greene, and Hellman [10] proved that this access structure is not $2-$ideal. This access structure has an appropriate matroid, $\mathcal{U}$, in which $V = \{0, 1, 2, 3\}$ and $\mathcal{I} = \{B : |B| \leq 2\}$. It is easy to check that the matroid $\mathcal{U}$ is not representable over GF(2) (which, by corollary 3.11, gives an alternative proof that the access structure is not 2-ideal). But the matroid $\mathcal{U}$ is representable over GF(3), therefore the access structure is 3-ideal.

Here is corresponding $3-$ideal scheme: Let $s \in \{0, 1, 2\}$ be the secret. The dealer chooses at random a number $r \in \{0, 1, 2\}$. The share of party 1 is r, the share of party 2 is $r + s$, and the share of party 3 is $r + 2s$.

This access structure demonstrates that being $3-$ideal does not suffice to guarantee that an access scheme is universally ideal. An additional example of this type is the following.

Example 4.2: Consider the following access structure $\mathcal{F}$ (see Fig. 1). The set of parties is $\{1,2,3,4,5,6\}$. The access structure is the closure of the set

$$\mathcal{F}_m = \{\{1,4\},\{2,5\},\{3,6\},\{1,2,6\},\{1,3,5\},\{2,3,4\},\{4,5,6\}\}.$$

The appropriate matroid of this access structure is the Fano matroid [18], which is representable only over fields of characteristic 2. Hence $\mathcal{F}$ is 2−ideal, and is not 3−ideal. The 2−ideal secret sharing scheme for $\mathcal{F}$ uses two random bits r_0, r_1 which are chosen independently with uniform distribution. The scheme is described in Fig. 2. This access structure demonstrates that being 2−ideal does not suffice to guarantee that an access scheme is universally ideal.

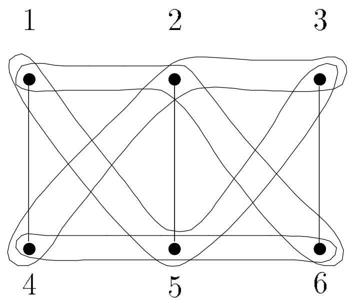

Figure 1: The minimal sets of the access structure $\mathcal{F}$

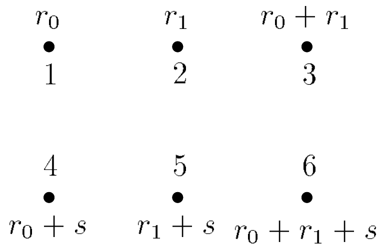

Figure 2: An ideal scheme for $\mathcal{F}$ with secret s and random independent inputs r_0, r_1.

The access structure $\mathcal{F}' = \mathrm{cl}(\mathcal{F}_m \cup \{3,4,5\})$ has a appropriate matroid that is representable over GF(3) but not over GF(2) [18]. Actually, the 3−ideal secret sharing scheme for $\mathcal{F}'$ is the same as the binary scheme for $\mathcal{F}$, except here r_0, r_1 are chosen uniformly and independently from $\{0,1,2\}$. Notice that the parties $\{3,4,5\}$ can reconstruct $2s$ over the two fields, which is useless over GF(2), but enables to reconstruct the secret over GF(3). This access structure demonstrates again that being 3−ideal does not suffice to guarantee that an access scheme is universally ideal.

Example 4.3: Here we give a method for combining two ideal access structures for n and ℓ parties into a new ideal access structure for $n+\ell-1$ parties. Let $\mathcal{A}$ be a non-degenerate access structure with parties $\{1,\ldots,n\}$, and let $\mathcal{A}_1$ be an access structure with parties $\{n+1,\ldots,n+\ell\}$.

We denote by $\mathcal{A}' = \mathcal{A}(i, \mathcal{A}_1)$ the access structure with $n+\ell-1$ parties $\{1, \ldots, i-1, i+1, \ldots, n, n+1, \ldots,$ and reconstructing sets

$$\mathcal{A}' = \mathrm{cl}(\{B : B \in \mathcal{A} \text{ and } i \notin B\}) \bigcup \{(B \setminus \{i\}) \cup B_1 \ : B \in \mathcal{A}, \ i \in B, \text{ and } B_1 \in \mathcal{A}_1\}.$$

That is, the sets that can reconstruct the secret in the new access structure are:

- The super-sets of sets from $\mathcal{A}$ that do not contain party i.
- The sets from $\mathcal{A}$ that do contain party i, in which party i is replaced with the sets of $\mathcal{A}_1$.

Let $\mathcal{A}$ be a non-degenerate access structure, let i be a party in $\mathcal{A}$, and let $\mathcal{A}_1$ be an access structure. We will show that if $\mathcal{A}$ and $\mathcal{A}_1$ are universally ideal then $\mathcal{A}' = \mathcal{A}(i, \mathcal{A}_1)$ is also universally ideal, by describing (for every m) an $m-$ideal secret sharing scheme for $\mathcal{A}'$. Given a secret s use an $m-$ideal scheme to generate shares for the parties in $\mathcal{A}$. Let s_i be the random variable that denotes the share of party i in the scheme for $\mathcal{A}$. Now use an $m-$ideal scheme for $\mathcal{A}_1$ with secret s_i to generate shares for the parties in $\mathcal{A}_1$.

It is easy to see that the 1 out of 2 threshold access structure is universally ideal (give the secret to each party). The 2 out of 2 threshold access structure is also universally ideal (give the first party a random input r, and to the second party deal $s + r \bmod m$). Using these two access structures as building blocks, and using the above construction recursively, we get a class of universally ideal access structures. The resulting class of access structures is a special case of access structures whose appropriate matroids are graphic, a class which we discuss next.

Example 4.4: Let $G = (V, E)$ be an undirected graph. The cycles of G (as defined in graph theory) are the minimal dependent sets of a matroid $\mathcal{T}(G)$ on the edge set E. In other words, the sets of points of the matroid $\mathcal{T}(G)$ is the set of *edges* of G, and $B \subseteq E$ is an independent set of $\mathcal{T}(G)$ if B does not contain cycles, i.e. B is a forest in G. A matroid $\mathcal{T}$ is *graphic* if there exists some graph G such that $\mathcal{T}$ is isomorphic to the cycle matroid $\mathcal{T}(G)$. Every graphic matroid is representable over any field [18]. Therefore if an access structure $\mathcal{A}$ has a graphic appropriate matroid, then $\mathcal{A}$ is universally ideal. To be more precise, let $G = (V, E)$ where $V = \{0, 1, \ldots, n\}$, $E \subseteq V \times V$, and let $e_0 = (0, 1) \in E$ be a special edge which corresponds to the dealer. Let

$$\mathcal{A}(G) = \mathrm{cl}(\{C \setminus \{e_0\} : C \subseteq E \text{ is a minimal cycle that contains } e_0\})$$

Then $\mathcal{A}(G)$ is universally ideal. The scheme Π for graphic matroids is actually quite simple. Let m be the cardinality of the domain of secrets. Let $r = < r_1, r_2, \ldots, r_{|V|-1} >$ be the random input ($|V| - 1$ independent values from the domain $\{0, \ldots, m-1\}$). Then the share of edge $(i, j) \in E$ (where $i \leq j$) is:

$$\Pi_{(i,j)}(s, r) = \begin{cases} r_i - r_j & i \neq 0 \\ r_1 + s - r_j & i = 0 \end{cases}$$

For every simple path which starts at node 1, and ends at node 0, it is possible to assign ± 1 weights to the shares along the path, such that the weighted sum is equal to the secret s.

We demonstrate this construction on a specific graph G_0, shown in Fig. 3. The cycles in the graph are:

$$\{e_0, e_2, e_3\}, \{e_0, e_1, e_2, e_4\}, \{e_1, e_3, e_4\},$$

and these sets are the minimal dependent sets of $\mathcal{T}(G_0)$. The access structure $\mathcal{A}\ (G_0)$ is the closure of $\{\{e_2, e_3\}, \{e_1, e_2, e_4\}\}$. The dealer is the edge e_0. The shares of the parties e_2 and e_3 are $r_1 - r_2$ and $r_1 + s - r_2$, respectively, and these parties can reconstruct the secrets by subtracting their shares.

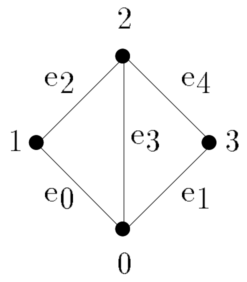

Figure 3: The graph G_0.

This scheme was found previously (not in the context of graphic matroids) by Benaloh and Rudich [2]. Their motivation was different: Given any monotone access structure $\mathcal{A}$ Benaloh and Leicher [1] show how to realize a secret sharing scheme for $\mathcal{A}$. One of the problems that Benaloh and Leicher raise in their paper [1] is that for most access structures their scheme is not efficient: if there are n parties in the access structure and the domain of secrets is S, then the domain of shares is of cardinality $|S|^{\theta(2^n)}$. The question is if there are more efficient schemes, or are most access structures "not efficient" and require large shares. Attempts to prove such lower bounds can be found in [7, 4, 11]. The best lower bound that was proved is $|S|^{2-\epsilon}$ for any constant $\epsilon > 0$ [4].

Let us focus on one approach to prove such lower bounds, and show that it fails. The secret sharing scheme of [1] uses a monotone formula, that describes the access structure, to build a secret sharing scheme. If the formula is of length L and the domain of secrets is S, then the domain of shares is of cardinality $|S|^{O(L)}$. Therefore every lower bound on the cardinality of the shares in secret sharing schemes implies a lower bound on the length of a formula that describes the access structure. Since there are known exponential lower bounds on the length of monotone formulas for some functions, one would hope that they would imply lower bounds on the size of the domain of shares. We show that this approach is wrong by describing an access structure with a super-polynomial gap between the cardinality of the domain of shares (in an efficient scheme) and the length of every formula that describes it.

Let C be the clique with ℓ nodes. We consider the access structure CON whose appropriate matroid is the cycle matroid of C (using our notation $CON = \mathcal{A}\ (C)$). This access structure has $n = \binom{\ell}{2} - 1$ parties, which are all the edges except $(0, 1)$ which is the dealer. The reconstructing sets of CON are all the undirected graphs such that adding the edge $(0, 1)$ to the graph closes a cycle. In other words, the access structure CON is the collection of all the graphs that contains a path from node 0 to node 1. Hence, the formula that describes CON is the $0-1-$connectivity formula. Krachmer and Wigderson [12] prove that every monotone formula for the function $0-1-$connectivity is of length $n^{\Omega(\log n)}$. On the other hand, CON is universally ideal.

Example 4.5: Let $G = (V, E)$ be an undirected graph. A cut in G is a collection of edges, such that deleting them from G increases the number of connected components in the remaining graph. The cuts of G are the minimal dependent sets of a matroid $\mathcal{T}^\star(G)$ on the edge set E. A matroid $\mathcal{T}$ is cographic if there exists some graph G such that $\mathcal{T}$ is isomorphic to the cut matroid $\mathcal{T}^\star(G)$. Every cographic matroid is representable over any field [18]. Therefore if an access structure $\mathcal{A}$ has a cographic appropriate matroid, then $\mathcal{A}$ is universally ideal. Unlike graphic matroids, we do not know of a simple construction of universally ideal secret sharing schemes for cographic matroids.

To be more precise, let $G = (V, E)$ where $V = \{0, 1, \ldots, n\}$, $E \subseteq V \times V$, and $e_0 = (0, 1) \in E$ is a special edge which corresponds to the dealer. Let

$$\mathcal{A}^\star(G) = \mathrm{cl}(\{C \setminus \{e_0\} : C \subseteq E \text{ is a minimal cut that contains } e_0\})$$

Then $\mathcal{A}^\star(G)$ is universally ideal. We again demonstrate this example on the graph G_0 shown in Fig. 3. The cuts of G_0 are

$$\{e_0, e_1, e_3\}, \{e_0, e_2\}, \{e_0, e_3, e_4\}, \{e_1, e_2, e_3\}, \{e_1, e_4\}, \{e_2, e_3, e_4\},$$

and these are the minimal dependent sets of the matroid $\mathcal{T}^\star(G_0)$.

Acknowledgments. We would like to thank Guy Even, Oded Goldreich, and Eyal Kushilevitz for their useful comments and suggestions.

References

[1] J.C. Benaloh and J. Leichter. Generalized Secret Sharing and Monotone Functions. In S. Goldwasser, editor, *Advances in Cryptology - CRYPTO '88 proceeding*, volume 403 of *Lecture notes in computer Science*, pages 27–35. Springer-Verlag, 1990.

[2] J.C. Benaloh and S. Rudich. Private Communication, 1989.

[3] G.R. Blakley. Safeguarding Cryptographic Keys. In *Proc. AFIPS 1979 NCC, vol. 48*, pages 313–317, June 1979.

[4] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the Information Rate of Secret Sharing Schemes. In *Advances in Cryptology - CRYPTO '92 proceeding*, 1992.

[5] E.F. Brickell. Some Ideal Secret Sharing Schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.

[6] E.F. Brickell and D.M. Davenport. On the Classification of Ideal Secret Sharing Schemes. *Journal of Cryptology*, 4(73):123–134, 1991.

[7] R.M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the Size of Shares for Secret Sharing Schemes. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91 proceeding*, volume 576 of *Lecture notes in computer Science*, pages 101–113. Springer-Verlag, 1992.

[8] M. Ito, A. Saito, and T. Nishizeki. Secret Sharing Schemes Realizing General Access Structure. In *Proc. IEEE Global Telecommunication Conf., Globecom 87*, pages 99–102, 1987.

[9] W. Jackson and K. M. Martin. On Ideal Secret Sharing Schemes. submitted for publication, 1992.

[10] E.D. Karnin, J.W. Greene, and M.E. Hellman. On Secret Sharing Systems. *IEEE Trans. on Inform. Theory*, IT-29 no. 1:35–41, 1983.

[11] J. Kilian and N. Nisan. Private Communication, 1990.

[12] M. Krachmer and A. Wigderson. Monotone Circuits for Connectivity Require Super-Logarithmic Depth. In *Proceeding 20th Annual Symposium on the Theory of Computing*, pages 539–550, 1988.

[13] K. M. Martin. *Discrete Structures in the Theory of Secret Sharing.* PhD thesis, University of London, 1991.

[14] P. D. Seymour. On Secret-Sharing Matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.

[15] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22:612–613, November 1979.

[16] K. Truemper. *Matroid Decomposition.* Academic press, Boston, 1992.

[17] W.T. Tutte. A Homotopy Theorem for Matroids I,II. *Transactions of the American Mathematical Society*, 88:144–160,161–174, 1958.

[18] D.J.A. Welsh. *Matroid Theory.* Academic press, London, 1976.