Universally Ideal Secret Sharing Schemes (Preliminary Version)

Amos Beimel[*] and Benny Chor[**]

Department of Computer Science
Technion, Haifa 32000, Israel

"I weep for you," the Walrus said,
"I deeply sympathize."
With sobs and tears he sorted out
Those of the largest size,
Holding his pocket-handkerchief
Before his streaming eyes.

"O Oysters," said the Carpenter.
"You've had a pleasant run!
Shall we be trotting home again?"
But answer came there none -
And this scarcely odd, because
They'd eaten every one.

from "Through the looking Glass" by Lewis Caroll

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, such that only subsets in the access structure can reconstruct 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 is 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. In addition, we give an exact characterization for each of these two conditions, and show that each condition by itself is not sufficient for universally ideal access structures.

1 Introduction

A secret sharing scheme involves a dealer who has a secret, 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). 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

[*] email: beimel@cs.technion.ac.il

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

E.F. Brickell (Ed.): Advances in Cryptology - CRYPTO '92, LNCS 740, pp. 183-195, 1993.

threshold t, then the scheme is called t out of n threshold secret sharing scheme. Threshold secret sharing schemes were first introduced by Blakley [Bla79] and by Shamir [Sha79]. Secret sharing schemes for general access structures were first defined by Ito, Saito and Nishizeki in [ISN87]. Given any monotone access structure, they show how to realize a secret sharing scheme for the access structure. Benaloh and Leichter [BL88] describe a more efficient way to realize such secret sharing schemes.

Even with the more efficient scheme of [BL88], most 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 [Bri89] was the first to introduce the notion of $m-$ideal access structures. Brickell and Davenport [BD91] 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 [KGH83]. This qualitative result was improved by Kilian and Nisan [KN90], 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, it 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 and known related results, that will be used in the rest of this paper.

2.1 Secret Sharing Schemes

The definition of secret sharing schemes is based on [CK89].

Definition 1. Let $S = \{0, \ldots, m-1\}$ be a finite set of secrets. Let $\mathcal{A} \subseteq 2^{\{1,\ldots,n\}}$ be a monotone set (such that $\emptyset \notin \mathcal{A}$) called the *access structure.* We say that a *secret-sharing scheme* Π realizes an access structure $\mathcal{A}$ with domain of secrets S if Π is a mapping $\Pi : S \times R \rightarrow S_1 \times S_2 \times \ldots \times S_n$ from the cross product of secrets and a set of random inputs to a set of n-tuples (the shares) such that the following two requirements hold:

1. The secret s can be reconstructed by any subset in $\mathcal{A}$. That is, for any subset $A \in \mathcal{A}$ $(A = \{i_1, \ldots, i_{|A|}\})$, there exists a function $h_A : S_{i_1} \times \ldots \times S_{i_{|A|}} \rightarrow S$ such that for every random inputs r it holds that if $\Pi(s, r) = \{s_1, s_2, \ldots, s_n\}$ then $h_A(\{s_i\}_{i \in A}) = s$.
2. Every subset not in $\mathcal{A}$ can not reveal any partial information about the secret (in the information theoretic sense). Formally, for any subset $A \notin \mathcal{A}$, for every two secrets $a, b \in S$, and for every possible shares $\{s_i\}_{i \in A}$:

$$\Pr_r[\,\{s_i\}_{i \in A} \mid a\,] = \Pr_r[\,\{s_i\}_{i \in A} \mid b\,]$$

We denote the shares of party i by $\Pi_i(s, r)$.

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 (if $B \in \mathrm{cl}(\Gamma)$ and $B \subseteq C$ then $C \in \mathrm{cl}(\Gamma)$). 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 $\mathcal{A} = \{A : |A| \geq t\}$, then a secret sharing 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. A secret sharing scheme $\Pi : S \times R \rightarrow S_1 \times \ldots \times S_n$ 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

Before we continue, we recall the definition of matroids . Matroids are well studied combinatorial objects (see for example Welsh [Wel76]). 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 $|X| = |Y| + 1$ 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 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 any two elements in V, there is a circuit containing both of them. The maximal independent sets are called *bases*. In every matroid, all bases have the same cardinality, which is defined as the *rank* of a matroid. 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 $\phi : V \rightarrow \mathcal{F}^k$ that satisfies:

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

2.3 Relation between Secret Sharing Schemes and Matroids

The next definition relates access structures and matroids.

Definition 3. 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. Intuitively, 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. 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 [Wel76], Theorem 5.4.1). Brickell and Davenport [BD91] 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.

Theorem 4 (necessary condition) [BD91]. *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 5 (sufficient condition) [BD91]. [3] *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.*

3 The Characterization Theorem

The two theorems of Brickell and Davenport almost characterize $q-$ideal access structures for q a prime power. However, 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. While we do not close the remaining gap for $q-$ideal access structures, we do give a complete characterization for universally ideal ones. We recall that an access structure $\mathcal{A}$ is universally ideal if it is $q-$ideal for any finite domain of secrets. Our main result is:

Theorem 6. *The 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 4 of Brickell and Davenport for the binary and ternary domains of secrets. We show that over these domains, every reconstruction function 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 *any* field. Thus, by Theorem 5 of Brickell and Davenport, the access structure is $q-$ideal for any prime power q. Using the Chinese remainder Theorem, $\mathcal{A}$ is $m-$ideal over any finite domain, namely is universally ideal, as desired.

Definition 7. 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. Let $A \subseteq \{0,\ldots,n\}$ and $i \in \{0,\ldots,n\}$. The parties in A *cannot reveal any information* about the share of i if for every distribution on the secrets, every possible shares $\{s_a\}_{a\in A}$, and every possible shares s_i, s_i'

$$\Pr_{s,r}[\ \Pi_i(s,r) = s_i \mid \{s_a\}_{a\in A}\ ] = \Pr_{s,r}[\ \Pi_i(s,r) = s_i' \mid \{s_a\}_{a\in A}\ ]$$

We also say that i is independent of A with respect to Π.

[3] The Theorem in [BD91] had a slightly weaker condition, which we omit for simplicity.

Definition 1 implies that if $A \subseteq \{1, \ldots, n\}$ and $A \notin \mathcal{A}$, then in every secret sharing scheme realizing $\mathcal{A}$ the *secret* (i.e. the share of the dealer) is independent of the shares of the parties in A.

Definition 8. Let Π be a secret sharing scheme. We say that a subset $A \subseteq \{0, 1, \ldots, n\}$ is ***dependent*** with respect to Π if there exists an $i \in A$ such that the parties in $A \setminus \{i\}$ can reconstruct the share of i (in the sense of definition 1). A subset $A \subseteq \{0, \ldots, n\}$ is *independent* if for every $i \in A$, i is independent of $A \setminus \{i\}$ 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 A of parties which could neither reconstruct the share of any of its members (and thus A in not dependent), yet could reveal some information on the share of one of its members (and thus A is not independent). However, for *ideal* secret sharing scheme, the following theorem of Brickell and Davenport [BD91] establishes the desired relation between the two notions.

Theorem 9 [BD91]. *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 $A \subseteq \{0, \ldots, n\}$. Then*

1. *The subset A is either dependent or independent with respect to Π.*
2. *The subset A is independent with respect to Π if and only if A is an independent set in a matroid $\mathcal{T}$ which is appropriate for $\mathcal{A}$.*

Definition 10. 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 $A \subseteq \{0, \ldots, n\}$ and every $0 \leq i \leq n$ such that $i \notin A$ and i depends on A with respect to Π, there are constants $\{\alpha_j\}_{j \in A}$, σ (all in GF(q)) such that for every secret $s \in$ GF(q) and choice of random inputs $r \in R$

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

where the sum is mod q.

We remark that the secret sharing scheme of Shamir [Sha79] is linear. The secret (or any other share) is reconstructed from the shares by substitution in the interpolating polynomial. The sufficient condition of Brickell and Davenport [BD91] (theorem 5) states that if an access structure $\mathcal{A}$ has an appropriate matroid which is representable over GF(q), then $\mathcal{A}$ is q–ideal. Their scheme, using our terminology, is a linear q–ideal secret sharing scheme. Our next lemma states the reverse direction.

Lemma 11. *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 (sketch). By Theorem 4 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, $\{0,\dots,n\}$, into a vector space over $\mathrm{GF}(q)$.

The mapping ϕ will be constructed in two stages. In the first stage we will map $V = \{0,\dots,n\}$ to $\mathrm{GF}(q)^{q\times|R|}$, where R is the source of randomness used in Π. For every $a \in V$ we define

$$\phi_1(a) = (\ \Pi_a(s_1,r_1), \Pi_a(s_1,r_2), \dots, \Pi_a(s_q,r_{|R|})\ )$$

intuitively $\phi_1(a)$ describes the shares of party a with every secret and every random input. In the second stage we construct a mapping ϕ_2 which fixes some remaining technicalities. We leave the details to the final version of this paper. These two mappings ϕ_1 and ϕ_2 have the property that $A \subseteq V$ is dependent in $\mathcal{T}$ if and only if $\phi_2 \circ \phi_1(A)$ 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 $\mathrm{GF}(q)$. □

Definition 12. We say that a function $f : S^t \rightarrow S$ is *component sensitive* if for every $1 \leq i \leq t$, every $s_1,\dots,s_{i-1},s_i,s_i',s_{i+1},\dots,s_t \in S$ $(s_i' \neq s_i)$:

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

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

Lemma 13. *Let Π be a $q-$ideal secret sharing scheme. Let $i \in \{0,\dots,n\}$, and $A \subseteq \{0,\dots,n\}$ be a minimal subset such that i depends on A and $i \notin A$. Let $f : S^{|A|} \rightarrow S$ be the reconstruction function of the $i-$th share from the shares of the parties in A. Then f is component sensitive.*

Proof. Omitted from this preliminary version.

We now show that the only component sensitive functions for the binary and for the ternary domains are linear. We start with the binary case.

Lemma 14. *Let $f : \mathrm{GF}(2)^t \rightarrow \mathrm{GF}(2)$ be a component sensitive function. Then f can be expressed as a linear function with non-zero coefficients over* $\mathrm{GF}(2)$*:*

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

Proof. Omitted from this preliminary version.

We use Lemma 14 to give an exact characterization of binary-ideal access structures.

Corollary 15. *An access structure $\mathcal{A}$ is binary-ideal if and only if there is a matroid which is representable over* $\mathrm{GF}(2)$ *and is appropriate for $\mathcal{A}$.*

Proof. Let Π be a binary-ideal secret sharing scheme that realizes the access structure $\mathcal{A}$. By lemma 13 the reconstruction function of every dependent set is component sensitive. Therefore by lemma 14 every reconstruction function is linear over GF(2), or in other words Π is a linear scheme. By lemma 11, We conclude that if $\mathcal{A}$ is binary-ideal then $\mathcal{A}$ has an appropriate matroid that is representable over GF(2). The other direction is implied by the sufficient condition of Brickell and Davenport [BD91] (theorem 5). □

The next lemma paralles Lemma 14, this time for the ternary case.

Lemma 16. *Let* $f : \mathrm{GF}(3)^t \rightarrow \mathrm{GF}(3)$ *be a component sensitive function. Then* f *can be expressed as a linear function with non-zero coefficients over* GF(3)*:*

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

Proof (sketch). 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 GF(q), any function which maps GF$(q)^t$ into GF(q) can be expressed as a multivariable polynomial over the field, in which every monomial of f contains variables whose powers do not exceed $q - 1$ (since $x^q \equiv x$). In our case the power will 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 arbitary 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 not zero. This substitution to f yeilds a polynomial in x_1, of the form $ax_1^2 + bx_1 + c$. The coefficient of x_1, a, is non-zero. By the observation mentioned above, the resulting function of x_1 should also be component sensitive. It is not hard to check that any degree 2 polynomial over GF(3) is not a permutation[4], and therefore is not component sensitive. Thus f contains no variable of degree 2, so all its monomials are multilinear.

We still have to show that f contains no monomial with two variables. We leave the details to the final version of the paper. □

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

[4] 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.

functions. Now using the same arguments as in the proof of Corollary 15 (for the binary case), we conclude with the following charcterization of ternary-ideal access structures.

Corollary 17. *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 $\mathcal{A}$.*

We saw that representation over GF(2) determines if an access structure is binary-ideal, and representation 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 from [Wel76] states strong implications of the representatability over the two finite fields. It will be used to complete the proof of our main theorem.

Proposition 18. *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 19. *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 15 and 17 the access structure $\mathcal{A}$ has an appropriate matroid $\mathcal{T}$ that is representable over GF(2) and over GF(3) (remember that there can be only one appropriate matroid for $\mathcal{A}$). Hence proposition 18 implies that $\mathcal{T}$ is representable over any field. From Theorem 4 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. □

Corollary 20. *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 $s \in S$ for every $1 \leq j \leq t$, independently, we use the ideal secret sharing scheme to share $s \bmod p_j^{i_j}$. Every subset of parties $A \in \mathcal{A}$ can reconstruct $s \bmod p_j^{i_j}$, therefore using the Chinese remainder Theorem, they can reconstruct the secret. Since for each j the secret $s \bmod p_j^{i_j}$ is shared independently, then every subset $A \notin \mathcal{A}$ does not know anything about the secret s. □

This last corollary is a restatement of Theorem 6, and it completes the arguments in the proof of our main result.

4 Examples

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 6 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 1 (the 2 out of 3 access structure) . We recall that the 2 out of 3 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. The appropriate matroid for this access structure is the matroid with $V = \{0, 1, 2, 3\}$ and $\mathcal{I} = \{A : |A| \leq 2\}$. It is not difficult to verify that this matroid is not representable over GF(2), hence the 2 out of 3 access structure is not 2-ideal. But this access structure is 3-ideal, as the following scheme demonstrates:
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.

Example 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 matroid that is appropriate for this access structure is the Fano matroid [Wel76], 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.

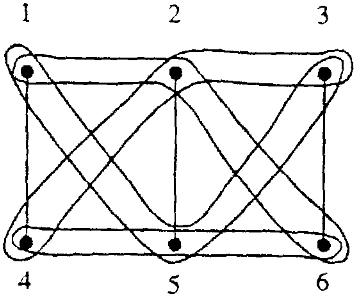

Fig. 1. The minimal sets of the access structure $\mathcal{F}$

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) [Wel76]. Actually, the 3−ideal

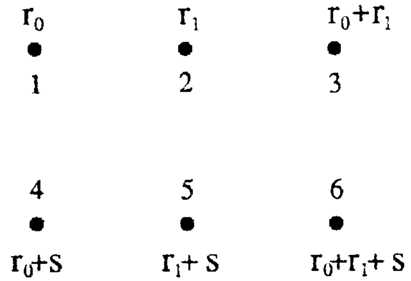

Fig. 2. An ideal scheme for $\mathcal{F}$ with secret s and random independent inputs r_0, r_1.

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 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 $\{1,\ldots,i-1,i+1,\ldots,n,n+1,\ldots,n+\ell\}$, and reconstructing sets

$$\mathcal{A}' = \{e : e \in \mathcal{A} \text{ and } i \notin e\} \cup \left\{(e \setminus \{i\}) \bigcup e_1 \ : e \in \mathcal{A},\ i \in e, \text{ and } e_1 \in \mathcal{A}_1\right\}.$$

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

- The sets from $\mathcal{A}$ that do not contain party i.
- The sets from $\mathcal{A}$ that do contain party i, in which we replace the party i with each set 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 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 a 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 a 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 the two parties). 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 $s+r \bmod m$). 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 is graphic, a class which we discuss next.

Example 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 $A \subseteq E$ is an independent set of $\mathcal{T}(G)$ if A does not contain cycles, i.e. A 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 [Wel76]. 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 $e_0 = (0, 1) \in E$ 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 $r =< r_1, r_2, \ldots, r_{|V|-1} >$ be the random input ($|V| - 1$ independent values). Then for every $(i, j) \in E$ $(i \leq j)$

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

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 equel to the secret s. This scheme was found previously (not in the context of graphic matroids) by Benaloh and Rudich [BR89].

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 $r_1 + s - r_2$ respectably and they can reconstruct the secret by substructing their shares.

Example 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 [Wel76]. Therefore if an access structure $\mathcal{A}$ has a cographic 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 $e_0 = (0, 1) \in E$ be a special edge which coresponds to the dealer. Let

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

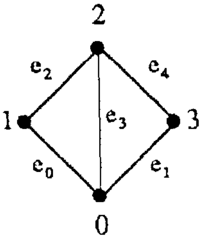

Fig. 3. The graph G_0.

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 $\mathcal{T}^{\star}(G_0)$.

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

References

[BD91] E.F. Brickell and D.M. Davenport. On the classification of ideal secret sharing schemes. *Journal of Cryptology*, 4(73):123–134, 1991.

[BL88] J.C. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advanced in Cryptology - CRYPTO '88 proceeding*, volume 403 of *Lecture notes in computer Science*, pages 27–35. Springer-Verlag, 1988.

[Bla79] G.R. Blakley. Safeguarding cryptographic keys. In *Proc. AFIPS 1979 NCC, vol. 48*, pages 313–317, June 1979.

[BR89] J.C. Benaloh and S. Rudich. Private communication, 1989.

[Bri89] E.F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.

[CK89] B. Chor and E. Kushilevitz. Secret sharing over infinite domains. In G. Brassard, editor, *Advanced in Cryptology - CRYPTO '89 proceeding*, volume 435 of *Lecture notes in computer Science*, pages 299–306. Springer-Verlag, 1989. To appear in Jour. of Cryptology.

[ISN87] 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.

[KGH83] 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.

[KN90] J. Kilian and N. Nisan. Private communication, 1990.

[Sha79] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, November 1979.

[Wel76] D.J.A. Welsh. *Matroid theory*. Academic press, London, 1976.