J. Cryptology (1991) 4: 123–134

Journal of Cryptology

On the Classification of Ideal Secret Sharing Schemes[1]

Ernest F. Brickell and Daniel M. Davenport
Sandia National Laboratories, Albuquerque, NM 87185, U.S.A.

Abstract. In a secret sharing scheme a dealer has a secret key. There is a finite set P of participants and a set Γ of subsets of P. A secret sharing scheme with Γ as the access structure is a method which the dealer can use to distribute shares to each participant so that a subset of participants can determine the key if and only if that subset is in Γ. The share of a participant is the information sent by the dealer in private to the participant. A secret sharing scheme is ideal if any subset of participants who can use their shares to determine any information about the key can in fact actually determine the key, and if the set of possible shares is the same as the set of possible keys. In this paper we show a relationship between ideal secret sharing schemes and matroids.

Key words. Secret sharing, Matroids, Representable matroids, Nearfields.

1. Introduction

In a secret sharing scheme a dealer has a key. There is a finite set P of participants and a set Γ of subsets of P. A secret sharing scheme with Γ as the access structure is a method which the dealer can use to distribute shares to each participant so that a subset of participants can determine the key if and only if that subset of is in Γ. A secret sharing scheme is said to be *perfect* if any subset of participants who can use their shares to determine any information about the key can in fact actually determine the key. The *share* of a participant is the information sent by the dealer in private to the participant.

In any practical implementation of a secret sharing scheme, it is important to keep the size of the shares as small as possible. The reason for this is obvious. The most secure place for a participant to store a share is in his own memory. However, if his share is too large, he will be inclined to write down information which will help him to remember his share. This, of course, will degrade the security of the scheme. This paper deals with secret sharing shemes in which the shares are as small as possible, i.e., the shares are the same size as the keys.

[1] Date received: December 8, 1989. Date revised: September 7, 1990. This work was performed at the Sandia National Laboratories and was supported by the U.S. Department of Energy under Contract No. DE-AC04-76DP00789.

Let $\mathscr{K}$ be the set of keys and let S be the set of shares used in a secret sharing scheme, i.e., the share for each participant is an $s \in S$. The *information rate* for the secret sharing scheme is defined to be $\log_2 |\mathscr{K}| / \log_2 |S|$. A perfect secret sharing scheme is said to be *ideal* if it has information rate 1.

The first constructions of perfect secret sharing schemes were the threshold schemes of Blakley [2] and Shamir [6]. In a threshold scheme, there is a threshold t such that the access structure is $\Gamma = \{A \subseteq P: |A| \geq t\}$.

A set of subsets Γ of a set P is said to be *monotone* if $B \in \Gamma$ and $B \subseteq C$ implies that $C \in \Gamma$ for any $B, C \subseteq P$. Ito *et al.* [5], and also Benaloh and Leichter [1], showed that, for any monotone set of subsets Γ of P, there exists a perfect secret sharing scheme with Γ as the access structure. However, for both the Ito *et al.* and the Benaloh and Leichter constructions, the information rate could be exponentially small in $|P|$.

The schemes of Blakley and Shamir can be implemented so that they are ideal secret sharing schemes for certain values of $|\mathscr{K}|$. Benaloh and Leichter [1], Brickell [3], and Simmons [7] have constructed ideal secret sharing schemes for other access structures.

The main contribution of the current paper is to give a description of ideal secret sharing schemes in terms of classical combinatorial objects by showing a direct relationship between ideal secret sharing schemes and matroids.

In order to make the definitions more precise, we define a secret sharing scheme to be a finite matrix, M, in which no two rows are identical. We identify the columns of M as the set of participants, P, and use $M(r, p)$ to denote the entry of M in row r and column p. We denote the first column as p_0 and assume that p_0 always receives the key as his share. It is sometimes useful to think of this special participant p_0 as the dealer. For $p \in P$, let $S(p) = \{M(r, p) | r \text{ is a row in } M\}$. That is, $S(p)$ is the set of the elements occurring in column p and $S(p_0) = \mathscr{K}$. The dealer can distribute a key, $\alpha \in S(p_0)$, by picking a row r of the matrix in which $M(r, p_0) = \alpha$ using the uniform distribution over all such rows, and by giving $M(r, p)$ as the share for participant p for each $p \in P$. We assume that the matrix is public knowledge, but that the dealer's choice of r is private.

Let $A \subseteq P$. Each participant $a \in A$ receives a share, say α_a, from the dealer. If the participants in A pool their information, they will know that the dealer picked a row r in which $M(r, a) = \alpha_a$ for each $a \in A$. For $A \subseteq P$, let $M(r, A)$ be the row r in M restricted to the columns indexed by A. It is now easy to define the access structure Γ. A subset $A \subseteq P$ will be in Γ if and only if any two rows r and $\hat{r}$ such that $M(r, A) = M(\hat{r}, A)$ also satisfy $M(r, p_0) = M(\hat{r}, p_0)$.

Given a subset $A \subseteq P$ and a participant $b \in P$ with $b \notin A$, we say that A has *no information* about the share given to b, denoted $A \not\to b$, if for all rows r of M and $\beta \in S(b)$ there is a row r' such that $M(r, a) = M(r', a)$ for all $a \in A$, and $M(r', b) = \beta$. Symbolically, $A \not\to b$ iff

$$\forall r \, \forall \beta \, \exists r': \qquad M(r, A) = M(r', A) \quad \text{and} \quad M(r', b) = \beta.$$

Otherwise, we say that A has *some information* about b, and denote this by $A \to b$. We say that A *knows* the share given to b, denoted by $A \Rightarrow b$, if all rows that are

identical on the participants in A are also identical on b. Symbolically, $A \Rightarrow b$ iff

$$\forall r \forall r' \text{ such that } M(r, A) = M(r', A): \quad M(r, b) = M(r', b).$$

Then $\Gamma = \{A \subseteq P | A \Rightarrow p_0\}$ is the collection of access sets.

A secret sharing scheme is *perfect* iff, for all subsets $A \subseteq P$, $A \to p_0$ implies that $A \Rightarrow p_0$. A secret sharing scheme is *ideal* iff it is perfect and $|S(p)| = |S(p_0)|$ for all $p \in P$. Thus if a secret sharing scheme is ideal, we assume without loss of generality that $S(p) = S(p_0)$ for all $p \in P$ and we denote $S(p)$ as simply S.

Let Γ_m denote the set of minimal elements of Γ. If there is a participant $p \in P$ such that p is not contained in any subset in Γ_m, then this participant is not needed since there is never a case in which his share is useful in determining the key. It is not interesting to study secret sharing schemes in which some participants receive useless shares. Therefore, we say that the secret sharing scheme is *connected* if every participant $p \in P$ is contained in some subset in Γ_m, and, for the remainder of this paper, only consider connected secret sharing schemes.

For M an ideal secret sharing scheme, let $D(M) = \{A \subseteq P | \text{there exists } y \in A \text{ such that } A \backslash y \Rightarrow y\}$. Intuitively, a set of participants is in $D(M)$ if there is a dependency among them.

Before we state the main results of this paper, we need to introduce the definitions of matroids and nearfields.

Matroids are well-studied combinatorial objects (see, for example, [11]). A matroid $\mathcal{T} = (V, \mathcal{I})$ is a finite set V and a collection $\mathcal{I}$ of subsets of V such that (I1)–(I3) are satisfied:

(I1) $\varnothing \in \mathcal{I}$.
(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 $x \in X \backslash Y$ such that $Y \cup \{x\} \in \mathcal{I}$.

The elements of V are called the *points* of the matroid and the sets $\mathcal{I}$ 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, there is a circuit containing both of them.

A *right nearfield* is a set R with distinguished elements 0 and 1 and binary operations $+$ and $*$ such that $(R, +)$ is an Abelian group, $(R \backslash 0, *)$ is a group, and $(R, +, *)$ is right distributive (i.e., $(a + b) * c = a * c + b * c$ for all $a, b, c \in R$). If a right nearfield is also left distributive, then it is a field. When R is finite its cardinality is always a power of a prime (see [10]). The nearfields we consider are finite. A right near vector space and its dot product, $\cdot$, are defined analogously to a vector space only defined over a right nearfield instead of a field. A vector v in a right near vector space V is said to be *dependent* on a set A of vectors iff every vector $u \in V$ that satisfies $u \cdot a = 0$ for all $a \in A$ also satisfies $u \cdot v = 0$. In the case that the right nearfield is actually a field, this definition of dependence is equivalent to stating that a vector v is dependent on a set A of vectors iff v is a linear combination of the vectors in A. A set A of vectors is said to be a *dependent set* if there exists $a \in A$ such that a is dependent on $A \backslash a$. A matroid is representable over a right nearfield if there is a

dependence-preserving injection from the points of the matroid into the set of vectors of a right near vector space.

In this paper we prove the following two theorems which together almost characterize ideal secret sharing schemes.

Theorem 1. *Let M be a connected ideal secret sharing scheme. Then the sets $D(M)$ are the dependent sets of a connected matroid.*

Theorem 2. *Let $\mathscr{T} = (V, \mathscr{I})$ be a connected matroid representable over a nearfield, R. Let $v_0 \in V$. Then there exists a connected ideal secret sharing scheme M such that $R = \mathscr{K}$, $p_0 = v_0$, $P = V$, and $D(M) =$ the dependent sets of $\mathscr{T}$.*

We say that this almost characterizes ideal secret sharing schemes because there may be connected matroids that are not representable over any nearfield, and, for any such matroids, we do not know if there exist corresponding ideal secret sharing schemes.

Another interesting result that can be easily proven from the methods used in proving Theorem 1 is the following.

Theorem 3. *Let M be a connected ideal secret sharing scheme. Let $A \subseteq P$ and $b \in P$. If $A \to b$, then $A \Rightarrow b$.*

This theorem shows that any participant in a connected ideal secret sharing scheme can be thought of as the special participant, p_0.

We also explore an alternate definition for perfect secret sharing. Let $A \subseteq P$ and $b \in P \backslash A$. We say that A has *no probabilistic information* about the share given to b, denoted $A \nrightarrow b$, if, for each row r of M, there exists an integer n such that, for all $\beta \in S(b)$, there are exactly n distinct rows $r_1', \ldots, r_n'$ such that, for $1 \leq i \leq n$, $M(r, a) = M(r_i', a)$ for all $a \in A$ and $M(r_i', b) = \beta$. Otherwise we say that A has *probabilistic information* about the share given to b and denote this by $A \rightsquigarrow b$.

It would be reasonable to define a perfect secret sharing scheme as one in which $A \rightsquigarrow p_0$ implies that $A \Rightarrow p_0$. Theorem 9 will show that, at least for connected secret sharing schemes with information rate 1, this definition is equivalent to our original definition.

The rest of the paper is organized as follows. In Section 2 we consider a special case in which we are able to establish necessary and sufficient conditions for the existence of an ideal secret sharing scheme. Section 3 contains the proof of Theorems 1 and 3, and Section 4 the proof of Theorem 2. In Section 5 we examine the probabilistic definition of perfect secret sharing. We finish the paper with some comments about applications and some open problems in Section 6.

2. Example: The Rank 2 Case

In this section we prove Theorems 1 and 2 in a special case that is much easier to prove and more intuitive than the general case. First we need some lemmas that will hold for the general case as well.

Let M be a connected ideal secret sharing scheme. Let $q = |S|$. Recall that, for $A \subseteq P$, $M(r, A)$ is the row r in M restricted to the columns indexed by A. Define $s(A) = \{M(r, A)\colon r \text{ is a row of } M\}$. That is, $s(A)$ is the set of distinct tuples of entries in M under A. Let $\#A = |s(A)|$.

Lemma 1. *Let $A \subseteq P$ and $p \in P$. If $A \Rightarrow p$, then $\#A = \#(A \cup p)$.*

Proof. Clearly, $\#(A \cup p) \geq \#A$. If $\#(A \cup p) > \#A$, then there exists rows r_1 and r_2 such that $M(r_1, a) = M(r_2, a)$ for all $a \in A$ and $M(r_1, p) \neq M(r_2, p)$. However, this contradicts $A \Rightarrow p$. □

In the proofs of Lemmas 2 and 3, it will be useful to recall that M is perfect and $A \not\Rightarrow p_0$ together imply that $A \not\to p_0$.

Lemma 2. *Let $A \subseteq P$ and $p \in P$. Suppose $A \not\Rightarrow p_0$ and $A \cup p \Rightarrow p_0$. Then $A \cup p_0 \Rightarrow p$.*

Proof. Let r_1 be a row of M. Define a function φ from S into S by $\varphi(\beta) = \gamma$ iff there exists a row r such that $M(r, a) = M(r_1, a)$ for all $a \in A$, and $M(r, p) = \beta$ and $M(r, p_0) = \gamma$. Since $A \cup p \Rightarrow p_0$, this function is well defined. Since $A \not\to p_0$, φ must be onto and hence 1–1. □

For a secret sharing scheme M, let $\hat{P} = \{p \in P | p \not\Rightarrow p_0\}$. Let $G(M)$ be a graph with vertices the participants in $\hat{P}$ and with $p_1, p_2 \in \hat{P}$ joined with an edge iff $\{p_1, p_2\} \in \Gamma$.

A connected ideal secret sharing scheme, M, is said to have rank 2 iff (S1)–(S3) are satisfied.

(S1) There exists a set in Γ_m of cardinality 2.
(S2) All sets in Γ_m have cardinality 1 or 2.
(S3) $G(M)$ is connected.

We then have the following theorem.

Theorem 4. *Let M be a rank 2 connected ideal secret sharing scheme. Let G' be the complementary graph of $G(M)$. Then G' is a disjoint union of cliques.*

Proof. Let $\{p_1, p_2\} \in \Gamma_m$. If there exists α_1, α_2 both in S such that there is no row r of M with $M(r, p_i) = \alpha_i$ for $i = 1, 2$, then $p_1 \to p_2$. Hence, $p_1 \to p_0$ and thus $p_1 \Rightarrow p_0$. Contradiction. Thus, $\#\{p_1, p_2\} = q^2$.

Let $A \subseteq P$ be maximal set such that $\#A = q^2$ and $\{p_1, p_2\} \subseteq A$. By Lemma 1, $p_0 \in A$ and $P \backslash \hat{P} \subseteq A$. Suppose $P \backslash A \neq \varnothing$. Since $G(M)$ is connected, there exists $b \in P \backslash A$ and $a \in A$ such that $\{a, b\} \in \Gamma$. By Lemma 2, $\{a, p_0\} \Rightarrow b$. Since $\{a, p_0\} \in A$, $\#A = \#(A \cup b)$. Contradiction. Thus $\#P = q^2$.

Suppose $\{a, b\} \subseteq \hat{P}$ and $\{a, b\} \notin \Gamma$. Let r be a row of M. Then, for all $\beta \in S$, there exists a row r_β such that $M(r_\beta, a) = M(r, a)$, $M(r_\beta, b) = M(r, b)$, and $M(r_\beta, p_0) = \beta$. Thus, $q\#\{a, b\} = \#\{a, b, p_0\} \leq q^2$. Since $\#a = q$, $\#\{a, b\} = q$. Since $\#b$ is also q, we must have $a \Rightarrow b$. Suppose now that $\{a, b, c\} \subseteq \hat{P}$ and $\{a, b\} \notin \Gamma$ and $\{b, c\} \notin \Gamma$. Since $a \Rightarrow b$ and $b \Rightarrow c$ implies $a \Rightarrow c$, we also have $\{a, c\} \notin \Gamma$. Theorem 4 now follows. □

The converse to Theorem 4 is also true.

Theorem 5. *Let G' be a graph which is a disjoint union of n cliques. Then there exists a rank 2 connected ideal secret sharing scheme M for any $\mathscr{K}$ with $|\mathscr{K}|$ a prime power $>n$, with $P = V(G') \cup p_0$ such that $G(M) =$ complement of G'.*

Proof. Let C be the set of distinct components of G'. Let n be the number of components of G'. Let $\hat{C} = C \cup p_0$. Let $\hat{S} = (\hat{C}, S, \hat{M})$ be an ideal 2 out of n threshold scheme with $|S| = q$. Using the Shamir construction, such a threshold scheme exists for all prime power q such that $q > n$. Let M be a matrix with the same number of rows as $\hat{M}$ and with columns indexed by the vertices of G'. For a vertex $v \in G'$ contained in component $c \in C$, and r a row of $\hat{M}$, let $M(r, v) = \hat{M}(r, c)$. Let $M(r, p_0) = \hat{M}(r, p_0)$ for all rows r of $\hat{M}$. It is straightforward to check that M is a rank 2 connected ideal secret sharing scheme. □

These two theorems now make it easy to prove Theorems 1 and 2 for this special case.

For M a rank 2 connected ideal secret sharing scheme, let $\mathscr{I}(M) = \{\varnothing\} \cup \{p | p \in P\} \cup \{\{p_1, p_2\} | p_1 \Rightarrow p_0$ and $p_2 \not\Rightarrow p_0\} \cup \{\{p_1, p_2\} | \{p_1, p_2\} \subseteq \Gamma_m\}$.

It is easy to see that $\mathscr{I}(M) = 2^P \backslash D(M)$ (where 2^P is the set of all subsets of P).

Theorem 6. *Let M be a rank 2 connected ideal secret sharing scheme. Then the sets $D(M)$ are the dependent sets of a connected matroid.*

Proof. We need to show that the set $\mathscr{I}(S)$ satisfies (I1)–(I3). Conditions (I1) and (I2) are trivially satisfied. The same applies to (I3) if $Y = \varnothing$ or $Y \subset X$. Thus assume that $|Y| = 1$ and $Y \not\subseteq X$. Let $Y = \{y\}$ and $X = \{x_1, x_2\}$. Without loss of generality, we may assume that $x_1 \in \hat{P}$. If $y \in P \backslash \hat{P}$, then $\{y, x_1\} \subseteq \mathscr{I}(S)$. If $y \notin P \backslash \hat{P}$ and $x_2 \in P \backslash \hat{P}$, then $\{y, x_2\} \in \mathscr{I}(S)$. So we can assume that $y, x_2 \in \hat{P}$. Since $(x_1, x_2) \in E(G)$, then, by Theorem 4, for at least one of $i = 1$ or 2, $(y, x_i) \in E(G)$ and so $\{y, x_i\} \in \mathscr{I}(S)$. □

Let $\mathscr{T} = (V, \mathscr{I})$ be a matroid. For a set $X \subseteq V$, the rank of X, $\rho(X)$, is defined as

$$\rho(X) = \max\{|A| : A \subseteq X, A \in \mathscr{I}\}.$$

The rank of $\mathscr{T}$ is defined to be $\rho(V)$.

Theorem 7. *Let $\mathscr{T} = (V, \mathscr{I})$ be a rank 2 connected matroid. Let $v_0 \in V$. Then there exists a connected ideal secret sharing scheme M such that $p_0 = v_0$, $P = V$, and $D(M) =$ the dependent sets of $\mathscr{T}$.*

Proof. Let $\hat{V} = \{v \in V | \{v, v_0\} \in \mathscr{I}\}$. Let G be the graph on $\hat{V}$ such that $\{u, v\}$ is an edge of G iff $\{u, v\} \in \mathscr{I}$. From (I3), it follows that the complement of G is a disjoint union of cliques. For if $u, v, w \in \hat{V}$, and $\{u, v\}$ is an edge of G, then, since $\{w\} \in \mathscr{I}$, either $\{u, w\}$ or $\{v, w\}$ must be an edge of G. By Theorem 5, there exists a rank 2 connected ideal secret sharing scheme $\hat{M}$, with $\hat{P} = \hat{V} \cup p_0$ such that $G(\hat{M}) = G$. Let

M be the matrix with columns $P = \hat{P} \cup V \backslash \hat{V}$ and with the same set of rows as $\hat{M}$ such that, for all rows r of $\hat{M}$, $M(r, p) = \hat{M}(r, p)$ for all $p \in \hat{P}$ and $M(r, p) = \hat{M}(r, p_0)$ for all $p \in P \backslash \hat{P}$. It is straightforward to check that M is a connected ideal secret sharing scheme and the sets $D(M)$ are exactly the dependent sets of $\mathscr{T}$. □

Thus in the rank 2 case, we did not need the condition used in Theorem 2 that the matroid was representable over a nearfield and therefore we were able to characterize the connected ideal secret sharing schemes completely. One possible reason why we were successful in this case but not in the general case is that all rank 2 matroids are representable over fields.

3. Connected Ideal Secret Sharing Schemes

As in Section 2, let M be a connected ideal secret sharing scheme and let $q = |S|$. The main work involved in proving Theorems 1 and 3 is the proof of the following proposition.

Proposition 1. *For every $A \subseteq P$, $\# A$ is a power of q.*

Theorem 3 follows immediately from Proposition 1.

Proof of Theorem 3. Suppose $A \to b$. Then $\#(A \cup b) < q \# A$. So by Proposition 1, $\#(A \cup b) = \# A$ and $A \Rightarrow b$. □

Lemmas 3–6 are used to prove Proposition 1, and then we finish with the Proof of Theorem 1.

Lemma 3. *Let $A \subseteq P$ and $p \in P$. Suppose $A \not\to p_0$ and $A \cup p \Rightarrow p_0$. Then $\#(A \cup p) = q \# A$.*

Proof. Let r be a row of M. Since $A \not\to p_0$, then, for each $\beta \in S$, there exists a row r_β such that $M(r, a) = M(r_\beta, a)$ for each $a \in A$ and $\beta = M(r_\beta, p_0)$. Since $A \cup p \Rightarrow p_0$, if $\beta \neq \hat{\beta}$, then $M(r_\beta, p) \neq M(r_{\hat{\beta}}, p)$. Thus, for each $\gamma \in S$, there exists a row t_γ such that $M(r, a) = M(t_\gamma, a)$ for each $a \in A$ and $\gamma = M(t_\gamma, p)$. □

Lemma 4. *If $A \in \Gamma_m$, then $\# A = q^{|A|}$.*

Proof. Let $k = |A|$. Let $A = \{a_1, \ldots, a_k\}$. Suppose there exists $\alpha_1, \ldots, \alpha_k \in S$ such that there is no row r with $M(r, a_i) = \alpha_i$. Let j be as large as possible such that there exists a row r' with $M(r', a_i) = \alpha_i$ for $1 \leq i \leq j$. Since all elements of S appear under a_1 in M, then $j \geq 1$. Then $\{a_1, \ldots, a_j\} \to a_{j+1}$. Hence $\{a_1, \ldots, a_j, a_{j+2}, \ldots, a_k\} \to p_0$, so $\{a_1, \ldots, a_j, a_{j+2}, \ldots, a_k\} \Rightarrow p_0$. However, this contradicts $A \in \Gamma_m$. □

Lemma 5. *Let $A \subseteq P$, $A \neq \varnothing$. If $A \not\Rightarrow p_0$, then $\# A = q^n$ for some integer n.*

Proof. Let A be a minimal set such that $A \not\Rightarrow p_0$ and $\#A$ is not a power of q. Let $B \in P\backslash A$ such that $A \cup B \Rightarrow p_0$ but $B \not\Rightarrow p_0$ and $(A \cup B\backslash b) \not\Rightarrow p_0$ for all $b \in B$. To see that such a B exists, let $a \in A$, and let $C \in \Gamma_m$ such that $a \in C$. (Such a C exists since M is connected.) Then let $B \subseteq C\backslash A$ be minimal such that $B \cup A \Rightarrow p_0$. If $\#(A \cup B) = q^{|A \cup B|}$, then $\#A = q^{|A|}$, so assume that $\#(A \cup B) < q^{|A \cup B|}$.

We need to show that, for all $a \in A$, $\#(A\backslash a) = q^{|A|-1}$. To show this we let n be an integer such that $q^n < \#A < q^{n+1}$. Let $a \in A$. Since $\#(A\backslash a)$ is a power of q, $\#(A\backslash a) = q^n$. Let $A = \{a_1, \ldots, a_k\}$ such that $a_k = a$. If $n < |A| - 1$, then there exists j, with $1 \leq j \leq k-2$ such that $\#(\{a_1, \ldots, a_j\}) = \#(\{a_1, \ldots, a_j, a_{j+1}\})$. So $\#(A\backslash a_{j+1}) = \#A$, but this contradicts the minimality of A.

To show that, for all $a \in A$, $\#(A \cup B\backslash a) = q^{|A \cup B|-1}$, let $B = \{b_1, \ldots, b_l\}$. By Lemma 3, $\#(A \cup B) = q\#(A \cup B\backslash b)$, so for each j, with $1 \leq j \leq l$, $\#((A\backslash a) \cup \{b_1, \ldots, b_j\}) = q\#((A\backslash a) \cup \{b_1, \ldots, b_{j-1}\})$.

This shows that, for all $a \in A$, $A \cup B\backslash a \to a$ (since $\#(A \cup B) < q^{|A \cup B|}$) and hence $A \cup B\backslash a \Rightarrow p_0$.

Next we need to show that $\#(A \cup B) = q^{|A \cup B|-1}$. Let $D \in \Gamma_m$ such that $B \subset D \subseteq A \cup B$. Let $a \in D \cap A$. $D\backslash a \not\Rightarrow p_0$, but $A \cup B\backslash a \Rightarrow p_0$. Let $A\backslash D = \{a_1, \ldots, a_m\}$. There exists j with $0 \leq j < m$ such that $((D\backslash a) \cup \{a_1, \ldots, a_j\}) \not\Rightarrow p_0$ but $((D\backslash a) \cup \{a_1, \ldots, a_j, a_{j+1}\}) \Rightarrow p_0$. Then $((D\backslash a) \cup \{a_1, \ldots, a_j\} \cup p_0) \Rightarrow a_{j+1}$. So $(A \cup B)\backslash a_{j+1} \Rightarrow a_{j+1}$ and $\#(A \cup B) = \#(A \cup B\backslash a_{j+1}) = q^{|A \cup B|-1}$.

Since $q^{|A|-1} < \#A$ and $\#(A \cup B) = q^{|A \cup B|-1}$, there exists j with $1 \leq j \leq l-1$ such that $\#(A \cup \{b_1, \ldots, b_{j+1}\}) < q\#(A \cup \{b_1, \ldots, b_j\})$. So $A \cup \{b_1, \ldots, b_j\} \to b_{j+1}$. Hence $A \cup B\backslash b_{j+1} \to p_0$ which implies that $A \cup B\backslash b_{j+1} \Rightarrow p_0$, but this contradicts the minimality of B. □

Lemma 6. *Let $A \subseteq P$. If $A \Rightarrow p_0$, then $\#A = q^k$ for some integer k.*

Proof. Let A be a minimal set such that $\#A$ is not a power of q. It follows from Lemma 5 that $A \Rightarrow p_0$.

We want to establish that there exists $a \in A$ such that $A\backslash a \not\Rightarrow p_0$. Let $B \subseteq A$ such that $B \in \Gamma_m$. Let $a \in B$. If $A\backslash a \Rightarrow p_0$, then there exists $C \subseteq A\backslash a$ with $C \in \Gamma_m$. Since $C \Rightarrow p_0$ and $(B\backslash a) \cup p_0 \Rightarrow a$, we have $C \cup (B\backslash a) \Rightarrow a$. Thus $\#A = \#(A\backslash a)$ which contradicts the minimality of A.

Now, from Lemma 3, we have $\#A = q\#(A\backslash a)$ which implies that $\#A$ is a power of q. Contradiction. □

Before we complete the proof of Theorem 1, we need to give an alternate definition of a matroid in terms of the rank function (for a proof, see [11]).

Theorem 8. *A function ρ on a set V is a rank function of a matroid iff* (A1)–(A3) *are satisfied*:

(A1) $\rho(\varnothing) = 0$.
(A2) *If $X \subseteq V$ and $y \in V$, then* $\rho(X) \leq \rho(X \cup y) \leq \rho(X) + 1$.
(A3) *If $X \subseteq V$ and $y, z \in V$ and $\rho(X) = \rho(X \cup y) = \rho(X \cup z)$, then* $\rho(X) = \rho(X \cup y \cup z)$.

The proof of the next proposition may be found in [11].

Lemma 7. *Let $\mathcal{T} = (V, \mathcal{I})$ be a matroid and let x, y, z be distinct elements of V. If there is a circuit C_1 containing x and y and a circuit C_2 containing y and z, then there exists a circuit C_3 containing x and z.*

We are now ready to complete the proof of Theorem 1.

Proof of Theorem 1. Let $\rho(\varnothing) = 0$ and $\rho(A) = \log_q(\#A)$ for all $A \subseteq P$. ρ satisfies the rank axioms of a matroid since if $A \subseteq P$ and $p_1, p_2 \in P$ such that $\#(A \cup p_i) = \#A$ for $i = 1, 2$, then $A \Rightarrow p_i$ for $i = 1, 2$, and hence $\#(A \cup \{p_1, p_2\}) = \#A$.

Let $\mathcal{T}$ be the matroid on the set S with rank function ρ.

$A \in D(M)$ iff there exists $a \in A$ such that $\#(A \backslash a) = \#A$ iff A is a dependent set in $\mathcal{T}$. This shows that $D(M)$ is the set of dependent sets of $\mathcal{T}$.

Finally, M is connected implies that every $p \in P \backslash p_0$ is on a circuit with p_0. By Lemma 7, for any pair $p_1, p_2 \in P$, there is a circuit containing both of them. Thus, $\mathcal{T}$ is connected. □

4. Ideal Secret Sharing Schemes and Nearfields

This section contains the proof of Theorem 2.

Lemma 8. *Let R be a finite right nearfield. Then, if $\alpha, \beta, \delta \in R$ and $\alpha \neq \beta$, there exists a unique $x \in R$ such that $x\alpha - x\beta = \delta$.*

Proof. Suppose $x\alpha - x\beta = y\alpha - y\beta$. Then $(x - y)\alpha = (x - y)\beta = \gamma$. At least one of α or β is nonzero. So if $x \neq y$, then $\gamma \neq 0$ and thus $\alpha = \beta$. Thus, as x ranges over all elements of R, $x\alpha - x\beta$ also ranges over all elements of R. □

Proof of Theorem 2. Let R be a nearfield such that $\mathcal{T}$ is representable over R. Let k be the rank of $\mathcal{T}$. Let $\varphi: V \to R^k$ be a dependence-preserving injection into the right near vector space R^k.

We define a secret sharing scheme M in which $P = V, p_0 = v_0, S = R$, and the set of rows in M is R^k. For $r \in R^k$ and $v \in V$, let $M(r, v) = r \cdot \varphi(v)$.

First we show that M is perfect. Suppose that $A \subseteq V$ and $A \not\Rightarrow p_0$. There exists $r_1, r_2 \in R^k$ such that $r_1 \cdot \varphi(a) = r_2 \cdot \varphi(a)$ for every $a \in A$ but $r_1 \cdot \varphi(v_0) \neq r_2 \cdot \varphi(v_0)$. Let $r \in R^k$. For $\delta \in R, (r + \delta r_1 - \delta r_2) \cdot \varphi(a) = r \cdot \varphi(a)$. Let $\beta \in R$. By Lemma 8, there exists δ such that $\delta r_1 \cdot \varphi(v_0) - \delta r_2 \cdot \varphi(v_0) = \beta - r \cdot \varphi(v_0)$. Then $(r + \delta r_1 - \delta r_2) \cdot \varphi(v_0) = \beta$. Thus $r' = r + \delta r_1 - \delta r_2$ is a row of M such that $M(r, A) = M(r', A)$ and $M(r', p_0) = \beta$. So $A \not\to v_0$.

To show that M is ideal, let $v \in \varphi(V)$ and let $\varphi(v) = (v_1, v_2, \ldots, v_k)$. Since $\mathcal{T}$ is connected, $\{v\}$ is an independent set, which implies that $\varphi(v) \neq 0$. Thus, some component, v_i, of $\varphi(v)$ is nonzero. Choose $\alpha \in R$ and define $r = (\rho_1, \rho_2, \ldots, \rho_k)$ where all components of r are zero except ρ_i which is $\alpha \cdot v_i^{-1}$. Then $r \cdot \varphi(v) = \alpha$ and, for all $v \in V, |S(v)| = |R|$.

To show that $D(M)$ is the set of dependent sets of $\mathcal{T}$, let $A \subseteq P$. $A \in D(M)$ iff there exists $b \in A$ such that all $r_1, r_2 \in R^k$ with $r_1 \cdot \varphi(a) = r_2 \cdot \varphi(a)$ for all $a \in A \backslash b$, also satisfy $r_1 \cdot \varphi(b) = r_2 \cdot \varphi(b)$; iff there exists $b \in A$ such that for all $r_1, r_2 \in R^k$ with

$(r_1 - r_2)\cdot\varphi(a) = 0$ for all $a \in A\backslash b$, also satisfy $(r_1 - r_2)\cdot\varphi(b) = 0$; iff all $u \in R^k$ such that $u\cdot\varphi(a) = 0$ for all $a \in (A\backslash b)$, also satisfy $u\cdot\varphi(b) = 0$; iff A is dependent in $\mathscr{T}$.

The fact that M is connected follows directly from the fact that $\mathscr{T}$ is connected. □

5. An Alternate Definition

In this section we explore an alternate definition for ideal secret sharing. For the convienience of the reader, we review some definitions. Let $A \subseteq P$ and $b \in P\backslash A$. We say that A has *no probabilistic information* about the share given to b, denoted $A \not\rightsquigarrow b$, if, for each row r of M, there exists an integer n such that, for all $\beta \in S(b)$, there are exactly n distinct rows $r'_1, \ldots, r'_n$ such that, for $1 \leq i \leq n$, $M(r, a) = M(r'_i, a)$ for all $a \in A$ and $M(r'_i, b) = \beta$. Otherwise we say that A has *probabilistic information* about the share given to b and denote this by $A \rightsquigarrow b$.

It would be reasonable to define a perfect secret sharing scheme as one in which $A \rightsquigarrow p_0$ implies that $A \Rightarrow p_0$. But the next theorem shows that, at least for connected secret sharing schemes with information rate 1, this definition would be equivalent to our original definition.

Theorem 9. *Let M be a connected ideal secret sharing scheme. Then $A \rightsquigarrow p_0$ implies that $A \Rightarrow p_0$.*

Proof. As before, let $q = |S|$. From the proof of Theorem 1 we know that the sets $D(M)$ are the dependent sets of a matroid where the rank function is defined as $\rho(A) = \log_q \# A$. Suppose $A \not\Rightarrow p_0$. Let $\# A = q^k$. Then $\#(A \cup p_0) = q^{k+1}$. Let $\# P = q^{k+1+l}$. Let $a_1, \ldots, a_k$ be a maximal independent set of A. Then $a_1, \ldots, a_k, p_0$ is a maximal independent set of $A \cup p_0$. Since any independent set can be extended to a maximal independent set (for a proof of this, see [11]), let $a_1, \ldots, a_k, p_0, b_1, \ldots, b_l$ be a maximal independent set of P. For any row r of M and any vector $(\alpha_1, \ldots, \alpha_l)$ of elements of S, there exists a unique row r' such that $M(r, a) = M(r', a)$ for all $a \in A$, $M(r, p_0) = M(r', p_0)$ and $M(r', b_i) = \alpha_i$ for $1 \leq i \leq l$. Thus, for any row r of M, there exists exactly q^l rows r' such that $M(r, a) = M(r', a)$ for all $a \in A$ and $M(r, p_0) = M(r', p_0)$. So $A \not\rightsquigarrow p_0$. □

6. Comments and Open Questions

There are several problems involved in applying these results to practical situations. When using a secret sharing scheme in an application, it seems likely that the key size, $|\mathscr{K}|$, and the access structure, Γ, would be given and the designer would want a perfect secret sharing scheme in which the number of shares $|S|$ was as small as possible. This is a slightly different question than the one we have been addressing in this paper. Suppose for instance that the sets $D(M)$ were indeed the dependent sets of a matroid that was representable over a nearfield. Let q be as small as possible such that $q > |\mathscr{K}|$ and the above matroid is representable over a nearfield of size q. It could be the case that there was a perfect secret sharing scheme with access

structure Γ, with keys $\mathscr{K}'$, and shares S such that $|\mathscr{K}| \leq |\mathscr{K}'| < |S| < q$. Such a scheme would not be ideal, but it would be more efficient in terms of the size of the share space than an ideal scheme with q keys.

The designer of an application might also wish to know whether the sets $D(M)$ were the dependent sets of a matroid and, if so, whether this matroid was representable over a nearfield. In considering the computational complexity of these questions, we need a model for how independence is determined. An *independence system* is a finite set V together with a set $\mathscr{I}$ of subsets of V called independent sets such that $\varnothing \in \mathscr{I}$ and if $A \subseteq B \subseteq V$ and $B \in \mathscr{I}$, then $A \in \mathscr{I}$. A common computational model for an independence system is that of an independence oracle which can be given any set of points and will respond by telling whether that set of points is independent or not. Given such an independence oracle, it is easy to show that determining whether a given independence system is a matroid could require an exponential number of calls to the independence oracle. Suppose, for example, that in an independence system on n points, all subsets of size $k-1$ were independent for some k, with $2 < k < n-1$. If all subsets of size k were dependent, then the independence system would be a matroid, but if there were one subset of size k that was independent and all of the other sets of size k were dependent, then it would not be a matroid. Thus determining whether such an independence system was a matroid would require at least $\binom{n}{k}$ calls to the independence oracle. Truemper [9] has also shown that given an independence oracle for a matroid on n points, determining whether the matroid is representable over a given field could require $\Omega(2^{n/2}/n^{1/2})$ calls to the independence oracle. These negative results do not imply that it is always infeasible to determine whether a given independence system is a matroid or whether a given matroid can be representable over a given field. For, in a practical situation, it is conceivable that there would be a simple discription of the independent sets from which it would be easy to determine if it was a matroid and if so whether the matroid was representable over a given field or nearfield.

The constructions for ideal threshold schemes resulting from Shamir [6] and Blakley [2] and the constructions described in [3] for ideal secret sharing schemes for other access structures all require the use of finite fields and thus restrict the size of the key set, $|\mathscr{K}|$, to be a prime power. Since all finite nearfields have prime power orders, $|\mathscr{K}|$ will also be a prime power for any ideal secret sharing scheme constructed using Theorem 2. But this restriction to $|\mathscr{K}|$ being a prime power is not necessary. For example, a 2 out of n ideal threshold scheme with $|\mathscr{K}| = k$ can be constructed from n orthogonal latin squares of side k (see [4] for definitions). Stinson and Vanstone [8] have studied some secret sharing schemes in which $|\mathscr{K}|$ is not a prime power which can be constructed from combinatorial designs.

There are several open questions that are suggested by the results presented in this paper. The most obvious open question is to determine if Theorem 2 is still true if the condition of the matroid being representable over a nearfield is removed.

Other open questions include:

1. Characterize the perfect secret sharing schemes that have a fixed information rate.

2. Characterize the perfect secret sharing schemes that have an information rate that is at least 1/(polynomial in $|P|$).
3. Find a nontrivial lower bound on the information rate of all perfect secret sharing schemes.
4. Find an algorithm that, given a secret sharing scheme, will determine the smallest information rate that could be used to implement that scheme.

Yao [12] has made some progress on problem 2. He uses a different measure for the security of a secret sharing scheme. In the current paper and in the original papers [6], [2] on secret sharing, the definitions demanded unconditional security, i.e., the security did not depend on any assumptions about the computational difficulty of any problems or the computational resources of an attacker. Yao gives a construction for secret sharing schemes which are secure if trap-door functions exists. Using this modified notion of security, he has shown that if trap door functions exist, then any set Γ which can be recognized by a polynomial (in $|P|$) size monotone circuit can be the access structure of a secret sharing scheme in which the information rate is at least 1/(polynomial in $|P|$). His scheme should be "perfect" under a modified definition of perfect which fits his security definitions.

Acknowledgments

We would like to thank Mike Saks for useful conversations concerning this research. We would also like to thank Kevin McCurley and two anonymous referees for very helpful comments which corrected a number of errors in the paper and made the paper more readable.

References

[1] J. C. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology—Crypto '88*, New York, pp. 27–36, 1990.
[2] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the AFIPS 1979 National Computer Conference*, vol. 48, pp. 313–317, 1979.
[3] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing*, **6**:105–113, 1989.
[4] M. Hall, Jr. *Combinatorial Theory*. Wiley, New York, 1986.
[5] M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. In *Proceedings of IEEE Globecom '87*, Tokyo, pp. 99–102, 1987.
[6] A. Shamir. How to share a secret. *Communications of the ACM*, **22**(11):612–613, 1979.
[7] G. J. Simmons. Robust shared secret schemes. *Congressus Numerantium*, **68**:215–248, 1989.
[8] D. R. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. *SIAM Journal of Discrete Mathematics*, 1(2):230–236, 1988.
[9] K. Truemper. On the efficiency of representability tests for matroids. *European Journal of Combinatorics*, **3**:275–291, 1982.
[10] S. Vajda. *Patterns and Configurations in Finite Spaces*. Hafner, New York, 1967.
[11] D. J. A. Welsh. *Matroid Theory*. Academic Press, London, 1976.
[12] A. Yao. Presentation at the Cryptography Conference in Oberwolfach, F.R. Germany, September, 1989.