Designs, Codes and Cryptography, 2, 357–390 (1992)

An Explication of Secret Sharing Schemes

D.R. STINSON*
Computer Science and Engineering Department and Center for Communication and Information Science, University of Nebraska, Lincoln, NE 68588-0115, U.S.A.

Communicated by R.C. Mullin
Received March 2, 1992; Revised May 5, 1992.

Abstract. This paper is an explication of secret sharing schemes, emphasizing combinatorial construction methods. The main problem we consider is the construction of perfect secret sharing schemes, for specified access structures, with the maximum possible information rate.

In this paper, we present numerous direct constructions for secret sharing schemes, such as the Shamir threshold scheme, the Boolean circuit construction of Benaloh and Leichter (for general access structures), the vector space construction of Brickell, and the Simmons geometric construction. We discuss the connections between ideal schemes (i.e., those with information rate equal to one) and matroids. We also mention the entropy bounds of Capocelli et al. Then we give a very general construciton, called the decomposition construction, and numerous applications of it. In particular, we study schemes for access structures based on graphs and the many interesting bounds that can be proved; and we determine the exact value of the optimal information rate for all access structures on at most four participants.

1. Introduction: The Shamir Threshold Scheme

In a bank, there is a vault which must be opened every day. The bank employs three senior tellers; but it is not desirable to entrust the combination to any one person. Hence, we want to design a system whereby any two of the three senior tellers can gain access to the vault, but no individual can do so. This problem can be solved by means of a secret sharing scheme (also called a shared control scheme).

We first study a special type of secret sharing scheme called a threshold scheme. Let t, w be positive integers, $t \leq w$. Informally, a (t, w)-*threshold scheme* is a method of sharing a secret key K among a finite set $\mathcal{P}$ of w participants, in such a way that any t participants can compute the value of K, but no group of $T - 1$ participants can do so. The value of K is chosen by a special participant called the *dealer*. The dealer is denoted by D and we assume $D \notin \mathcal{P}$. When D wants to share the key K among the participants in $\mathcal{P}$, he gives each participant some partial information called a *share*. The shares should be distributed secretly, so no participant knows the share given to another participant.

At a later time, a subset of participants $B \subseteq \mathcal{P}$ will pool their shares in an attempt to compute the secret key K. If $|B| \geq t$, then they should be able to compute the value of K as a function of the shares they collectively hold; if $|B| < t$, then they should not be able to compute K. In the example described above, we desire a (2, 3)-threshold scheme.

*Research supported by NSERC (Canada) grant A9287.

We will use the following notation. Let $\mathcal{P} = \{P_i : 1 \leq i \leq w\}$ be the set of w participants. $\mathcal{K}$ is *key set* (i.e., the set of all possible keys); and $\mathcal{S}$ is the *share set* (i.e., the set of all possible shares).

The problem of constructing threshold schemes was solved independently by Shamir [21] and Blakley [5] in 1979. Blakley's solution uses finite geometries, while Shamir's scheme is based on polynomial interpolation. We present the Shamir threshold scheme here. Let $\mathcal{K} = GF(q)$, where $q \geq w + 1$ is a prime power. Also, let $\mathcal{S} = GF(q)$. Hence, the key will be an element of $GF(q)$, as will be each share given to a participant.

In the initialization phase, D chooses w distinct, nonzero elements of $GF(q)$, denoted x_i, $1 \leq i \leq w$ (note that this is where we require $q \geq w + 1$). For $1 \leq i \leq w$, D gives the value x_i to P_i. The values x_i are *not* the shares; in fact they can be made public.

Now when D actually wants to share a secret $K \in \mathcal{K}$, he performs the following steps:

1. D secretly chooses (independently at random) $t - 1$ elements of $GF(q)$, $a_1, \ldots, a_{t-1}$.
2. For $1 \leq i \leq w$, D computes $y_i = a(x_i)$, where

$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j.$$

3. For $1 \leq i \leq w$, D gives the share y_i to P_i.

Let's look at how a subset B of t participants will reconstruct the secret. Suppose participants $P_{i_1}, \ldots, P_{i_t}$ want to determine K. They know that $y_{i_j} = a(x_{i_j})$, $1 \leq j \leq t$, where $a(x)$ is the (secret) polynomial chosen by D. Since $a(x)$ has degree at most $t - 1$, $a(x)$ can be written as

$$a(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1},$$

where the coefficients $a_0, \ldots, a_{t-1}$ are unknown and $a_0 = K$ is the key. Since $y_{ij} = a(x_{i_j})$, $1 \leq j \leq t$, B can obtain t linear equations in the t unknowns $a_0, \ldots, a_{t-1}$. Remember that all arithmetic is done in $GF(q)$. If the equations are linearly independent, there will be a unique solution, and a_0 will be revealed as the secret.

Let's look at a small example. Suppose $q = 17$, $t = 3$ and $w = 5$; and the public x-coordinates are $x_i = i$, $1 \leq i \leq 5$. Suppose that $B = \{P_1, P_3, P_5\}$ pool their shares, which are respectively 8, 10 and 11. Since $a(x) = a_0 + a_1 x + a_2 x^2$, the following three linear equations are obtained:

$$a_0 + a_1 + a_2 = 8$$

$$a_0 + 3a_1 + 9a_2 = 10$$

$$a_0 + 5a_1 + 8a_2 = 11.$$

This system does have a unique solution in $\mathbf{Z}_{17}$: $a_0 = 13$, $a_1 = 10$ and $a_2 = 2$. The secret is therefore $K = a_0 = 13$.

Clearly, it is important that the system of t linear equations have a unique solution, as in the above example. We show now that this is always the case. In general, we have $y_{i_j} = a(x_{i_j})$, $1 \leq j \leq t$, where $a(x) = a_0 + a_1x + \ldots + a_{t-1}x^{t-1}$ and $a_0 = K$. The system obtained is the following:

$$\begin{aligned}
a_0 + a_1x_{i_1} + a_2x_{i_1}^2 + \ldots + a_{t-1}x_{i_1}^{t-2} &= y_{i_1} \\
a_0 + a_1x_{i_2} + a_2x_{i_2}^2 + \ldots + a_{t-1}x_{i_2}^{t-1} &= y_{i_2} \\
&\vdots \\
a_0 + a_1x_{i_t} + a_2x_{i_t}^2 + \ldots + a_{t-1}x_{i_t}^{t-1} &= y_{i_t}.
\end{aligned}$$

This can be written in matrix form as follows:

$$\begin{pmatrix}
1 & x_{i_1} & x_{i_1}^2 & \ldots & x_{i_1}^{t-1} \\
1 & x_{i_2} & x_{i_2}^2 & \ldots & x_{i_2}^{t-1} \\
\vdots & \vdots & \vdots & & \vdots \\
1 & x_{i_t} & x_{i_t}^2 & \ldots & x_{i_t}^{t-1}
\end{pmatrix}
\begin{pmatrix}
a_0 \\ a_1 \\ \vdots \\ a_{t-1}
\end{pmatrix}
=
\begin{pmatrix}
y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_t}
\end{pmatrix}.$$

Now, the coefficient matrix A is a so-called Vandermonde matrix, and its determinant is

$$\det A = \prod_{1 \leq k < j \leq t} (x_{i_j} - x_{i_k}).$$

The x_i's are all distinct, so no term $x_{i_j} - x_{i_k}$ is equal to zero. The product is computed in the field $GF(q)$. Since the product of nonzero terms in a field is always nonzero, we have that $\det A \neq 0$. Since the determinant of the coefficient matrix is nonzero, the system has a unique solution over the field $GF(q)$.

What happens if a group of $t - 1$ participants attempt to compute K? Proceeding as above, they will obtain a system of $t - 1$ equations in t unknowns. Suppose they guess a value y_0 for the secret. Since the secret is $a_0 = a(0)$, this will yield a tth equation, and the coefficient matrix of the resulting system of t equations in t unknowns will again be a Vandermonde matrix. As before, there will be a unique solution. Hence, for every hypothesized value y of the secret, there is a unique polynomial $a_{y_0}(x)$ such that $y_{i_j} = a_{y_0}(x_{i_j})$ for $1 \leq j \leq t - 1$ and such that $y = a_{y_0}(0)$. Hence, no value of the secret can be ruled out, and $t - 1$ participants can obtain no information about the secret.

We have analyzed the Shamir scheme from the point of view of solving systems of linear equations over $GF(q)$. There is an alternative method, based on the Lagrange interpolation formula for polynomials. The Lagrange interpolation formula is an explicit formula for the (unique) polynomial $a(x)$ of degree at most t that we computed above. The formula is as follows:

$$a(x) = \sum_{j=1}^{t} y_{i_j} \prod_{1 \le k \le t, k \ne j} \frac{x - x_{i_h}}{x_{i_j} - x_{i_h}}.$$

Now, the t participants in B do not need to know the whole polynomial $a(x)$. They only need to know the constant term $K = a(0)$. Hence, they can compute the following expression:

$$K = \sum_{j=1}^{t} y_{i_j} \prod_{1 \le k \le t, k \ne j} \frac{x_{i_h}}{x_{i_h} - x_{i_j}}.$$

If we define

$$b_j = \prod_{1 \le k \le t, k \ne j} \frac{x_{i_h}}{x_{i_h} - x_{i_j}}$$

for $1 \le j \le t$, then we have

$$K = \sum_{j=1}^{t} b_j y_{i_j}.$$

Hence, the secret is a linear combination of the t shares. Note also that the values b_j can be precomputed, if desired.

In the example above, the participants $\{P_1, P_3, P_5\}$ could precompute $b_1 = 4$, $b_2 = 3$ and $b_3 = 11$. Then given shares 8, 10 and 11, they would obtain

$$K = 4 \times 8 + 3 \times 10 + 11 \times 11 \equiv 13 \bmod 17,$$

as before.

1.1. A (t, t)-Threshold Scheme

The last topic of this section is a simplified construction for threshold schemes in the special case $w = t$, due to Karnin, Greene and Hellman [15]. This construction will work for any key set $\mathcal{K} = \mathbf{Z}_m$ with $\mathcal{S} = \mathbf{Z}_m$. (It is *not* required that m be prime, and it is *not* necessary that $m \ge w + 1$.) If D wants to share the secret $K \in \mathbf{Z}_m$, he performs the following operations:

1. D secretly chooses (independently at random) $t - 1$ elements of $\mathbf{Z}_m$, $y_1, \ldots, y_{t-1}$.
2. D computes $y_t = K - \Sigma_{i=1}^{t-1} y_i \bmod m$.
3. For $1 \le i \le t$, D gives the share y_i to P_i.

Observe that the t participants can compute K by the formula

$$K = \sum_{i=1}^{t} y_i \bmod m,$$

Can $t-1$ participants compute K? Clearly, the first $t-1$ participants cannot, since they receive $t-1$ independent random numbers as their shares. Consider the $t-1$ participants in the set $\mathcal{P}\backslash\{P_i\}$, where $1 \leq i \leq t-1$. These $t-1$ participants possess the shares $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_{t-1}$ and $K - \Sigma_{i=1}^{t-1} y_i$. By summing their shares, they can compute $K - y_i$. However, they do not know the random value y_i, and hence they have no information as to the value of K. Consequently, we have a (t, t)-threshold scheme.

2. Access Structures and General Secret Sharing

In the previous section, we desired that any t of the w participants should be able to determine the secret. A more general situation is to specify exactly which subsets of participants should be able to determine the secret and which should not. Let Γ be a set of subsets of $\mathcal{P}$; this is denoted mathematically by the notation $\Gamma \subseteq 2^{\mathcal{P}}$. The subsets in Γ are those subsets of participants that should be able to compute the secret. Γ is called an *access structure* and the subsets in Γ are called *authorized subsets*.

Let $\mathcal{K}$ be the key set and let $\mathcal{S}$ be the share set. As before, when a dealer D wants to share a secret $K \in \mathcal{K}$, he will give each participant a share from $\mathcal{S}$. At a later time a subset of participants will attempt to determine K from the shares they collectively hold. We will say that a scheme is a *perfect secret sharing scheme realizing* the access structure Γ provided the following two properties are satisfied:

1. If an authorized subset of participants $B \subseteq \mathcal{P}$ pool their shares, then they can determine the value of K.
2. If an unauthorized subset of participants $B \subseteq \mathcal{P}$ pool their shares, then they can determine nothing about the value of K.

The security of such a scheme is unconditional, since we do not place any limit on the amount of computation that can be performed by a subset of participants. Of course, in the case where B is an authorized subset, we will try to minimize the amount of computation time required to determine the secret.

Observe that a (t, w)-threshold scheme realizes the access structure

$$\{\Gamma \subseteq \mathcal{P} : |\Gamma| \geq t\}.$$

Such an access structure is called a *threshold* access structure. We showed in the previous section that the Shamir scheme is a perfect scheme realizing the threshold access structure.

Suppose that $B \in \Gamma$ and $B \subseteq C \subseteq \mathcal{P}$. Suppose the subset C wants to determine K. Since B is an authorized subset, it can already determine K. Hence, the subset C can determine K by ignoring the shares of the participants in $C\backslash B$. Stated another way, a superset of an authorized set is again an authorized set. What this says is that the access structure should satisfy the *monotone* property:

if $B \in \Gamma$ and $B \subseteq C \subseteq \mathcal{P}$, then $C \in \Gamma$.

If Γ is an access structure, then $B \in \Gamma$ is a *minimal* authorized subset of $A \notin \Gamma$ whenever $A \subseteq B$, $A \neq B$. The set of minimal authorized subsets of Γ is denoted Γ_0 and is called the *basis* of Γ. Since Γ consists of all subsets of $\mathcal{P}$ that are supersets of a subset in the basis Γ_0, Γ is determined uniquely as a function of Γ_0. Expressed mathematically, we have

$$\Gamma = \{C \subseteq \mathcal{P} : B \subseteq C, B \in \Gamma_0\}.$$

We say that Γ is the *closure* of Γ_0 and write $\Gamma = cl(\Gamma_0)$.

As an example, suppose $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ and

$$\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}.$$

Then

$$\Gamma = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}, \{P_1, P_2, P_3\}, \{P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_4\}\}.$$

In the case of a threshold access structure, the basis consists of all subsets of (exactly) t participants.

2.1. *The Monotone Circuit Construction*

In 1987, Ito, Saito and Nishizeki [13] gave a construction which shows that there exists a perfect secret sharing scheme realizing any monotone access structure. In the remainder of this section, we will give a conceptually simple and elegant proof of this result, due to Benaloh and Leichter [2]. The idea is to first build a monotone circuit that recognizes the access structure, and then to build the secret sharing scheme from the description of the circuit. We call this the *monotone circuit construction*.

Suppose we have a Boolean circuit, with w Boolean inputs, $x_1, \ldots, x_w$ (corresponding to the w participants in $\mathcal{P} = \{P_1, \ldots, P_w\}$), and one Boolean output, y. The circuit consists of *or* gates and *and* gates; we do not allow any *not* gates. Such a circuit is called a *monotone* circuit. The reason for this nomenclature is that changing any input x_i from "0" (false) to "1" (true) can *never* result in the output y changing from "1" to "0." The circuit is permitted to have arbitrary fan-in, but we require fan-out equal to 1 (that is, a gate can arbitrarily many input wires, but only one output wire).

If we specify Boolean values for the w inputs of such a monotone circuit, we can define

$$B(x_1, \ldots, x_w) = \{P_i : x_i = 1\},$$

i.e., the subset of $\mathcal{P}$ corresponding to the true inputs. Suppose C is a monotone circuit, and define

$$\Gamma_C = \{B(x_1, \ldots, x_w) : C(x_1, \ldots, x_w) = 1\},$$

where $C(x_1, \ldots, x_w)$ denotes the output of C given inputs $x_1, \ldots, x_w$. Since the circuit C is monotone, it follows that Γ_C is a monotone set of subsets of $\mathcal{P}$.

It is easy to see that there is a one-to-one correspondence between monotone circuits of this type and Boolean formulae which contain the operators $\wedge$ and $\vee$, but do not contain any negations.

If Γ is a set of subsets of $\mathcal{P}$, then it is easy to construct a monotone circuit C such that $\Gamma_C = \Gamma$. One way to do this is as follows. Let Γ_0 be the basis of Γ. Then construct the disjunctive normal form Boolean formula

$$\bigvee_{B \in \Gamma_0} \left(\bigwedge_{x_i \in B} x_i \right).$$

In the example above, where $\Gamma_0 = \{\{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3\}\}$, we would obtain the Boolean formula

$$(P_1 \wedge P_2 \wedge P_4) \vee (P_1 \wedge P_3 \wedge P_4) \vee (P_2 \wedge P_3). \tag{1}$$

Each clause in the Boolean formula corresponds to an "and" gate of the associated monotone circuit; the final disjunction corresponds to an "or" gate. The number of gates in the circuit is $|\Gamma_0| + 1$.

Suppose C is any monotone circuit that recognizes Γ (note that C need not be the circuit described above). We describe an algorithm which enables D to construct a perfect secret sharing scheme that realizes Γ. This scheme will use as a building block the (t, t)-schemes constructed at the end of the last section. Hence, we take the key set to be $\mathcal{K} = \mathbf{Z}_m$ for some integer m.

The algorithm proceeds by assigning a value $f(W) \in \mathcal{K}$ to every wire W in the circuit C. Initially, the output wire W_{out} of the circuit is assigned the value K, the secret. The algorithm iterates a number of times, until every wire has a value assigned to it. Finally, each participant P_i is given the list of values $f(W)$ such that W is an input wire of the circuit which receives input x_i.

The basic iterative step of the algorithm involves finding a gate G of C such that $f(W_G)$ is defined if W_G is the output wire of G but $f(W)$ is not defined for any of the input wires of G. We then define $f(W)$ for the input wires of G as follows:

1. If G is an *or* gate, then define $f(W) = f(W_G)$ for every input wire W of G.
2. If G is an *and* gate having input wires $W_1, \ldots, W_t$, then share the *secret* $f(W_G)$ among the t input wires using the (t, t)-scheme. That is, choose (independently at random) $t - 1$ elements of $\mathbf{Z}_m$, $y_1, \ldots, y_{t-1}$. Then compute $y_t = f(W_G) - \Sigma_{i=1}^{t-1} y_i \bmod m$ and for $1 \leq i \leq t$, define $f(W_i) = y_i$.

Let's carry out this procedure for the circuit corresponding to the Boolean formula (1). Suppose K is the secret. The value K is given to each of the three input wires of the final *or* gate. Next, we consider the *and* gate corresponding to the clause $P_1 \wedge P_2 \wedge P_4$. The three input wires are assigned values a_1, a_2, $K - a_1 - a_2$, respectively, where all arithmetic

is done in $\mathbf{Z}_m$. In a similar way, the three input wires corresponding to $P_1 \wedge P_3 \wedge P_4$ are assigned values b_1, b_2, $K - b_1 - b_2$. Finally, the two input wires corresponding to $P_2 \wedge P_3$ are assigned values c_1, $K - c_1$. Note that a_1, a_2, b_1, b_2 and c_1 are all random values in $\mathbf{Z}_m$.

The shares that the four participants receive are the following:

$$P_1 \leftarrow (a_1, b_1);$$

$$P_2 \leftarrow (a_2, c_1);$$

$$P_3 \leftarrow (b_2, K - c_1);$$

$$P_4 \leftarrow (K - a_1 - a_2, K - b_1 - b_2).$$

Let's first verify that each basis subset can compute K. $\{P_1, P_2, P_4\}$ can compute $K = a_1 + a_2 + (K - a_1 - a_2)$. $\{P_1, P_3, P_4\}$ can compute $K = b_1 + b_2 + (K - b_1 - b_2)$. Finally, $\{P_2, P_3\}$ can compute $K = c_1 + (K - c_1)$.

Can an unauthorized subset compute K? It suffices to consider the maximal unauthorized subsets, namely: $\{P_1, P_2\}$, $\{P_1, P_3\}$, $\{P_1, P_4\}$, $\{P_2, P_4\}$ and $\{P_3, P_4\}$. In each case, it is easy to see that K cannot be computed, either because some necessary piece of random information is missing, or because all the shares possessed by the subset are random. For example, the subset $\{P_1, P_2\}$ possesses only the random values a_1, b_1, a_2, c_1. The subset $\{P_3, P_4\}$ possesses the shares b_2, $K - c_1$, $K - a_1 - a_2$, $K - b_1 - b_2$. Since the values of c_1, a_1, a_2 and b_1 are unknown random values, K cannot be computed.

We can obtain a different scheme realizing the same access structure by rewriting the formula (1) in conjunctive normal form (note that this corresponds to the original construction of Ito, Saito and Nishizeki [13]):

$$(P_1 \vee P_2) \wedge (P_1 \vee P_3) \wedge (P_2 \vee P_3) \wedge (P_2 \vee P_4) \wedge (P_3 \vee P_4). \tag{2}$$

If we implement the scheme using the circuit corresponding to (2), then the following shares are distributed:

$$P_1 \leftarrow (a_1, a_2);$$

$$P_2 \leftarrow (a_1, a_3, a_4);$$

$$P_3 \leftarrow (a_2, a_3, K - a_1 - a_2 - a_3 - a_4);$$

$$P_4 \leftarrow (a_4, K - a_1 - a_2 - a_3 - a_4).$$

We leave the details for the reader to check.

How do we prove that the monotone circuit construction works in general? It seems most appropriate to proceed by induction on the number of gates in the circuit C. If C contains only one gate, then the result is fairly trivial. If C consists of one *or* gate, then every participant will be given the secret. This scheme realizes the access structure consisting of all nonempty subsets of participants. If C consists of a single *and* gate with t inputs, then

the scheme is the (t, t)-threshold scheme that we analyzed earlier, which realizes the threshold access structure.

Now, as an induction assumption, suppose that there is an integer $j > 1$ such that, for all circuits C with fewer than j gates, the construction produces a scheme that realizes Γ_C. Let C be a circuit on j gates. Consider the *last* gate, G, in the circuit; again, G could be either an *or* gate or an *and* gate. Let's first consider the case where G is an *or* gate. Denote the input wires to G by W_i, $1 \leq i \leq t$. These t input wires are the ouptuts of t subcircuits of C, which we denote C_i, $1 \leq i \leq t$. Corresponding to each C_i, we have a (sub)scheme that realizes the access structure Γ_{C_i}, by induction. Now, it is easy to see that

$$\Gamma_C = \bigcup_{i=1}^{t} \Gamma_{C_i}.$$

Since every W_i is assigned the secret K, it follows that the scheme realizes Γ_C, as desired.

The analysis is similar if G is an *and* gate. In this situation, we have

$$\Gamma_C = \bigcap_{i=1}^{t} \Gamma_{C_i}.$$

Since the secret K is shared among the t wires W_i using an (t, t)-threshold scheme, it follows again that the scheme realizes Γ_C. This completes the proof.

Of course, when an authorized subset, B, wants to compute the secret, the participants in B need to know the circuit used by D to distribute shares, and which shares correspond to which wires of the circuit. All this information will be public knowledge. Only the actual *values* of the shares are secret. The algorithm for reconstructing the secret involves combining shares according to the circuit, with the stipulation that an *and* gate corresponds to summing the values on the input wires mod$m$ (provided these values are all known), and an *or* gate involves choosing the value on any input wire (with the understanding that all these values will be identical).

3. A General Model for Secret Sharing Schemes

In this section, we will develop a general mathematical model for secret sharing and discuss the concept of security in this model. The model is similar to that of [9]. In this model, we represent a secret sharing scheme by a set $\mathcal{T}$ of *distribution rules*. A distribution rule is a function

$$f: \mathcal{P} \cup \{D\} \rightarrow \mathcal{K} \cup \mathcal{S}$$

which satisfies the conditions $f(D) \in \mathcal{K}$, and $f(P_i) \in \mathcal{S}$ for $1 \leq i \leq w$. A distribution rule f represents a possible distribution of shares to the participants, where $f(D)$ is the secret key being shared, and $f(P_i)$ is the share given to P_i.

If $\mathcal{F}$ is a set of distribution rules and $K \in \mathcal{K}$, denote

$$\mathcal{F}_K = \{f \in \mathcal{F} : f(D) = K\}.$$

If $K \in \mathcal{K}$ is the value of the secret that D wishes to share, then D will choose a random distribution rule $f \in \mathcal{F}_K$, and use it to distribute shares.

Observe that this is a completely general model in which we can study secret sharing schemes. Any of our existing schemes can be described in this setting by determining the possible distribution rules which the scheme will use. The fact that this model is mathematically precise makes it easier to give definitions and to present proofs. We also emphasize that the set of distribution rules are public knowledge.

We will sometimes find it convenient to tabulate all the values of the distribution rules in the form of an array. Each row of the array corresponds to a distribution rule $f \in \mathcal{F}$, where we place the value $f(x)$ in column x of the array, for all $x \in \mathcal{P} \cup \{D\}$.

As an example, in Figure 1 we present a secret sharing scheme from [9] for the access structure having basis

$$C_6 = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}, \{P_4, P_5\}, \{P_5, P_6\}, \{P_6, P_1\}\}.$$

C_6 is the graph which is a cycle of length six.

So, this scheme has $w = 6$, $\mathcal{K} = \{0, 1\}$ and $\mathcal{S} = \{0, 1, 2\}$. There are 12 distribution rules, six corresponding to each of the two values of the secret, K. A subset of participants, B, will attempt to determine the secret by examining the set of distribution rules, and determining which rules are consistent with the shares they collectively hold.

	D	P_1	P_2	P_3	P_4	P_5	P_6
f_1	0	0	0	1	1	2	2
f_2	0	0	0	2	2	1	1
f_3	0	1	1	2	2	0	0
f_4	0	1	1	0	0	2	2
f_5	0	2	2	0	0	1	1
f_6	0	2	2	1	1	0	0
f_7	1	0	1	1	2	2	0
f_8	1	0	2	2	1	1	0
f_9	1	1	2	2	0	0	1
f_{10}	1	1	0	0	2	2	1
f_{11}	1	2	0	0	1	1	2
f_{12}	1	2	1	1	0	0	2

Figure 1. A secret sharing scheme for C_6.

First, note that the shares given to any two participants in the basis C_6 do not determine a unique distribution rule, but they *do* determine K. For example, if P_1, P_2 receive the shares 1, 1, respectively, then they know only that the distribution function is either f_3 or f_4. However, the value of K is determined to be 1, since $f_3(D) = f_4(D) = 1$.

Next, let us consider a share given to one participant, say P_1. Knowledge of one share restricts the possible distribution rules to four out of 12. However, two of these four rules correspond to the secret being 0 and the other two correspond to the secret being 1.

If $\{P_i, P_j\}$ is an unauthorized subset, then the number of possible distribution rules consistent with the shares they hold is reduced from 12 to two, but the two possible rules always correspond to different values of the secret. $\{P_1, P_3, P_5\}$ and $\{P_2, P_4, P_6\}$ are also unauthorized subsets. If the participants in either of these subsets pool their shares, they can (again) restrict the number of possible distribution rules to two of the 12. but the two possible rules correspond to different values of the secret.

3.1. Formal Definitions

It is useful to develop conditions which ensure that a set of distribution rules for a scheme does indeed realize a specified access structure. These conditions appear rather complicated, but they are motivated by the analysis of the scheme presented in Figure 1. The conditions are equivalent to conditions presented in [9].

Suppose Γ is an access structure and $\mathcal{F}$ is a set of distribution rules. Suppose the following two properties are satisified:

(*) Let $B \in \Gamma$, and suppose $f, g \in \mathcal{F}$. If $f(P_i) = g(P_i)$ for all $P_i \in B$, then $f(D) = g(D)$.

(**) Let $B \notin \Gamma$ and suppose $f: B \to \mathcal{S}$. Then there exists a nonnegative integer $\lambda(f, B)$ such that, for every $K \in \mathcal{K}$,

$$|\{g \in \mathcal{F}_K : g(P_i) = f(P_i) \forall P_i \in B\}| = \lambda(f, B).$$

Then we claim that $\mathcal{F}$ is a perfect secret sharing scheme that realizes the access structure Γ. The property (*) is relatively straightforward: it says that the shares given to an authorized subset uniquely determine the value of the secret. (As in Figure 1, these shares need not determine the distribution rule being used.)

The property (**) will enable us to prove mathematically that the shares given to an unauthorized subset give no information as to the value of the secret. The list of shares $(f(P_i) : P_i \in B)$ given to an unauthorized subset B will restrict the possible distribution rules to some subset of $\mathcal{F}$. However, the remaining possible rules will be equally divided among the possible keys. More precisely, for any assignment of shares f to B, there will remain $\lambda(f, B)$ possible rules corresponding to each value of the secret.

As an illustration of these conditions, we compute the values $\lambda(f, B)$ for the scheme in Figure 1. If $B = \{P_i\}$ and $f(P_i) = j$, where $1 \le i \le 6$ and $0 \le j \le 2$, then $\lambda(f, B) = 2$. If B is an unauthorized subset of cardinality two and f is a one-to-one function, then $\lambda(f, B) = 1$. Similarly, if $B = \{P_1, P_3, P_5\}$ or $\{P_2, P_4, P_6\}$ and f is a one-to-one function, then $\lambda(f, B) = 1$. In all other cases where B is an unauthorized subset, $\lambda(f, B) = 0$.

The formal security proof uses probability distributions. We suppose that there is a probability distribution $p_{\mathcal{K}}$ on $\mathcal{K}$. For every $K \in \mathcal{K}$, D will choose each distribution rule in $\mathcal{F}_K$ with equal probability $1/|\mathcal{F}_K|$. When an unauthorized subset B pools their shares, they can compute a conditional probability distribution $p_{\mathcal{K}}(K|f)$, where $f: B \to \mathcal{S}$ represents the shares they collectively hold. What we will do is to prove that $p_{\mathcal{K}}(K|f) = p_{\mathcal{K}}(K)$ for every $K \in \mathcal{K}$ and for every $f: B \to \mathcal{S}$, if B is an unauthorized subset. That is, the conditional probability distribution on $\mathcal{K}$, given an assignment of shares f to an unauthorized subset B, is the same as the *a priori* probability distribution on $\mathcal{K}$. The reader will notice that this situation is very similar to the concept of perfect secrecy, and this similarity is why the resulting scheme is termed *perfect*.

The computation of the conditional probability distribution $p_{\mathcal{K}}(K|f)$ is much like other computations we have performed; the main tool is Bayes' theorem. In applying Bayes' theorem, we need to compute the probability distribution on the shares given to the participants in B. We denote the set of all possible distributions of shares to the participants in B by $\mathcal{S}(B)$; the probability distribution on $\mathcal{S}(B)$ is denoted by $p_{\mathcal{S}(B)}$.

We want to prove that $p_{\mathcal{K}}(K|f) = p_{\mathcal{K}}(K)$. By Bayes' theorem,

$$p_{\mathcal{K}}(K|f) = \frac{p_{\mathcal{K}}(K)p_{\mathcal{S}(B)}(f|K)}{p_{\mathcal{S}(B)}(f)}.$$

Hence, it suffices to prove that

$$p_{\mathcal{S}(B)}(f|K) = p_{\mathcal{S}(B)}(f).$$

First, we observe that there is a constant λ such that $|\mathcal{F}_K| = \lambda$ for every $K \in \mathcal{K}$. This can be seen easily from property (**) with $B = \emptyset$. Consequently, we have

$$p_{\mathcal{S}(B)}(f|K) = \frac{\lambda(f, b)}{\lambda}$$

for every f, B and K. We compute $p_{\mathcal{S}(B)}(f)$ as follows:

$$\begin{aligned} p_{\mathcal{S}(B)}(f) &= \sum_{k \in \mathcal{K}} p_{\mathcal{K}}(k)p_{\mathcal{S}(B)}(f|k) \\ &= \sum_{k \in \mathcal{K}} p_{\mathcal{K}}(k) \frac{\lambda(f, B)}{\lambda} \\ &= \frac{\lambda(f, b)}{\lambda} \\ &= p_{\mathcal{S}(B)}(f|K), \end{aligned}$$

as desired.

We summarize this result in the following theorem.

THEOREM 3.1 *[9] Suppose we have a collection of distribution rules $\mathcal{T}$ that satisfy the conditions (*) and (**). Then $\mathcal{T}$ is a perfect secret sharing scheme realizing the access structure* Γ.

4. Information Rate and Ideal Schemes

The results of Section 2 prove that any monotone access structure can be realized by a perfect secret sharing scheme. We now want to consider the efficiency of the resulting schemes. In the case of a (t, w)-threshold scheme, we can construct a circuit corresponding to the disjunctive normal form Boolean formula which will have

$$1 + \begin{pmatrix} w \\ t \end{pmatrix}$$

gates. Each participant will receive

$$\begin{pmatrix} w - 1 \\ t - 1 \end{pmatrix}$$

elements of $\mathbf{Z}_m$ as his or her share. This seems very inefficient, since a Shamir (t, w)-threshold scheme enables a secret to be shared by giving each participant only one *piece* of information.

In general, we measure the efficiency of a secret sharing scheme by the information rate. We use the model of Section 3. Suppose $\mathcal{T}$ is a set of distribution rules for a secret sharing scheme. For $1 \leq i \leq w$, define

$$\mathcal{S}_i = \{f(P_i) : f \in \mathcal{T}\}.$$

$\mathcal{S}_i$ represents the set of possible shares that P_i might receive; of course $\mathcal{S}_i \subseteq \mathcal{S}$. Now, since the secret key K comes from a finite set $\mathcal{K}$, we can think of K as being represented by a bit-string of length $\log_2 |\mathcal{K}|$, by using a binary encoding, for example. In a similar way, a share given to P_i can be represented by a bit-string of length $\log_2 |\mathcal{S}_i|$. Intuitively, P_i receives $\log_2 |\mathcal{S}_i|$ bits of information (in his or her share), but the information content of the secret is $\log_2 |\mathcal{K}|$ bits. The *information rate* [9] for P_i is the ratio

$$\rho_i = \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}_i|}.$$

The information rate of the scheme is denoted by ρ and is defined as

$$\rho = \min\{\rho_i : 1 \leq i \leq w\}.$$

This definition of information rate is reminiscent of the information rate of an error-correcting code. (We should mention that an alternative definition of information rate has also been studied in the literature; see [6], [17], [16], [14].)

Let's look at the two schemes from Section 2. The scheme produced using the Boolean formula (1) has $\rho = \log_2 m/\log_2 m^2 = 1/2$. Using the formula (2), we get $\rho = 1/3$. Hence, the first implementation is preferable.

In general, if we construct a scheme from a circuit C using the monotone circuit construction, the information rate $\rho_i = 1/r_i$, where r_i denotes the number of input wires to C carrying the input x_i. Equivalently, r_i denotes the number of occurrences of x_i in the related Boolean formula.

The scheme presented in Figure 1 has $\rho = \log_2 2/\log_2 3 \approx 0.63$. With respect to threshold access structures, we observe that the Shamir scheme will have information rate 1 (the optimal value). In contrast, an implementation of a (t, w)-threshold scheme using a disjunctive normal form Boolean circuit will have information rate

$$1/\begin{pmatrix} w-1 \\ t-1 \end{pmatrix},$$

which is much lower if $1 < t < w$.

Obviously, a high information rate is desirable. The first result we prove is that $\rho \leq 1$ in any scheme. Suppose $\mathcal{F}$ is the set of distribution rules for a perfect secret sharing scheme that realizes the access structure Γ. Let $B \in \Gamma_0$ and let $P_i \in B$. Define $B' = B \backslash \{P_i\}$, and choose any distribution rule $g \in \mathcal{F}$. Let f be the restriction of g to B'. Now, $B' \notin \Gamma$, so there is an integer $\lambda(f, B') > 0$ satisfying property (**). Hence, for each $K \in \mathcal{K}$, there is a distribution rule $f_K \in \mathcal{F}_K$ such that $f_K(P_j) = f(P_j)$ for all $P_j \in B'$. By property (*), $f_K(P_i) \neq f_{K'}(P_i)$ if $K \neq K'$. Hence, $|\mathcal{S}_i| \geq |\mathcal{K}|$, and thus $\rho \leq 1$.

Since $\rho = 1$ is the optimal situation, we refer to such a scheme as an *ideal* scheme. The Shamir schemes are ideal schemes. In the next subsection, we present a construction for ideal schemes that generalizes the Shamir schemes. We call this the vector space construction.

4.1. The Vector Space Construction

The vector space construction is due to Brickell [7]. Suppose Γ is an access structure, and let $GF(q)^d$ denote the vector space of all d-tuples over $GF(q)$, where q is a prime power and $d \geq 2$. Suppose there exists a function

$$\phi : \mathcal{P} \cup \{D\} \rightarrow GF(q)^d$$

which satisfies the property

$$(***) \quad \phi(D) \in \langle \phi(P_i) : P_i \in B \rangle \Leftrightarrow B \in \Gamma.$$

That is, the vector $\phi(D)$ can be expressed as a linear combination of the vectors in the set $\{\phi(P_i) : P_i \in B\}$ if and only if B is an authorized subset.

Now, suppose there is a function ϕ that satisfies (***). We construct an ideal secret sharing scheme with $\mathcal{K} = \mathcal{S}_i = GF(q)$, $1 \leq i \leq w$. The distribution rules of the scheme

are as follows: for every vector $\bar{a} = (a_1, \ldots, a_d) \in GF(q)^d$, define a distribution rule $f_{\bar{a}}$ where

$$f_{\bar{a}}(x) = \bar{a} \cdot \phi(x)$$

for every $x \in \mathcal{P} \cup \{D\}$, where the operation "$\cdot$" is the inner product in $GF(q)$.

We have the following result.

THEOREM 4.1. *[7] Suppose ϕ satisfies the conditon (***). Then the collection of distribution rules*

$$\mathcal{F} = \{f_{\bar{a}} : \bar{a} \in GF(q)^d\}$$

is an ideal scheme that realizes Γ.

Proof. First, we will show that if B is an authorized subset, then the participants in B can compute K. Since $\phi(D) \in \langle \phi(P_i) : P_i \in B \rangle$, we can write

$$\phi(D) = \sum_{\{i:P_i \in B\}} c_i \phi(P_i),$$

where each $c_i \in GF(q)$. Denote by s_i the share given to P_i. Then $s_i = \bar{a} \cdot \phi(P_i)$, where $\bar{a}$ is an unknown vector chosen by D. Now, $K = \bar{a} \cdot \phi(D)$. By the linearity of the inner product operation, $K = \Sigma_{\{i:P_i \in B\}} c_i \bar{a} \cdot \phi(P_i)$. Thus, it is a simple matter for the participants in B to compute

$$K = \sum_{\{i:P_i \in B\}} c_i s_i.$$

Hence, property (*) is satisfied.

What happens if B is not an authorized subset? Denote by e the dimension of the subspace $\langle \phi(P_i) : P_i \in B \rangle$. Choose any $K \in \mathcal{K}$, and consider the system of equations:

$$\phi(P_i) \cdot \bar{a} = s_i, \ \forall P_i \in B$$

$$\phi(D) \cdot \bar{a} = K.$$

This is a system of linear equations in the d unknowns $a_1, \ldots, a_d$. The coefficient matrix has rank $e + 1$, since $\phi(D) \notin \langle \phi(P_i) : P_i \in B \rangle$. Hence, the solution space has dimension $d - e - 1$ (independent of the value of K). Thus, $\lambda(f, B) = p^{d-e-1}$, where $f(P_i) = s_i$, for $P_i \in B$. Hence, property (**) is also satisfied. By Theorem 3.1, we have a perfect secret sharing scheme realizing the access structure Γ. □

4.2. *Some Applications*

First, we observe that the Shamir (t, w)-threshold scheme is a special case of the vector space construction. To see this, define $d = t$ and let

$$\phi(P_i) = (1, x_i, x_i^2, \ldots, x_i^{t-1})$$

for $1 \leq i \leq w$, where x_i is the x-coordinate given to P_i. Also, let

$$\phi(D) = (1, 0, \ldots, 0).$$

The resulting scheme is equivalent to the Shamir scheme; we leave the details to the reader to check.

Another general result involves access structures that have as a basis the edges of certain undirected graphs. Given a graph $G = (V, E)$ with a vertex set V and edge set E, we denote by $\Gamma(G)$ the access structure on participant set V having basis $\Gamma_0 = E$. A graph G is defined to be a *complete multipartite graph* if the vertex set V can be partitioned into subsets $V_1, \ldots, V_\ell$ such that $\{x, y\} \in E$ if and only if $x \in V_i$, $y \in V_j$, where $i \neq j$. The sets V_i are called *parts*. The complete multipartite graph is denoted by $K_{n_1,\ldots,n_\ell}$ if $|V_i| = n_i$, $1 \leq i \leq \ell$. (A complete multipartite graph $K_{1,\ldots,1}$ (with ℓ parts) is in fact a *complete graph* and is denoted K_ℓ.)

THEOREM 4.2. *Suppose $G = (V, E)$ is a complete multipartite graph. Then there is an ideal scheme realizing the access structure $\Gamma(G)$.*

Proof. Let $V_1, \ldots, V_\ell$ be the parts of G. Let $x_1, \ldots, x_\ell$ be distinct elements of $GF(q)$, where $q \geq \ell$. Let $d = 2$. For every participant $v \in V_i$, define $\phi(v) = (x_i, 1)$, and define $\phi(D) = (1, 0)$. It is straightforward to verify the condition (***). By Theorem 4.1, we have an ideal scheme. □

To illustrate further application of these constructions, we will consider the possible access structures for up to four participants. Note that it suffices to consider only the access structures in which the basis cannot be partitioned into two nonempty subsets on disjoint participant sets. (For example, $\Gamma_0 = \{\{P_1, P_2\}, \{P_3, P_4\}\}$ can be partitioned as $\{\{P_1, P_2\}\} \cup \{\{P_3, P_4\}\}$.) We list the nonisomorphic access structures of this type on two, three and four participants in Table 1. The column labelled ρ^* records the maximum possible information rates for each of these access structures, which we will discuss in the rest of the paper.

Of these 18 (nonisomorphic) access structures, we can already construct ideal schemes for ten of them. These ten access structures are either threshold access structures or have a basis which is a complete multipartite graph, so Theorem 4.2 can be applied. Eight access structures remain to be considered. We will use the vector space construction to construct ideal schemes for four of these: #11, #14, #15 and #16.

Table 1. Access structures for at most four participants.

	w	Subsets in Γ_0	ρ^*	Comments
1.	2	P_1P_2	1	(2, 2)-threshold
2.	3	P_1P_2, P_2P_3	1	$\Gamma_0 \cong K_{1,2}$
3.	3	P_1P_2, P_2P_3, P_1P_3	1	(2, 3)-threshold
4.	3	$P_1P_2P_3$	1	(3, 3)-threshold
5.	4	P_1P_2, P_2P_3, P_3P_4	2/3	Theorem 6.1 and Example 7.1
6.	4	P_1P_2, P_1P_3, P_1P_4	1	$\Gamma_0 \cong K_{1,3}$
7.	4	P_1P_2, P_1P_4, P_2P_3, P_3P_4	1	$\Gamma_0 \cong K_{2,2}$
8.	4	P_1P_2, P_2P_3, P_2P_4, P_3P_4	2/3	Theorem 6.1 and Example 7.2
9.	4	P_1P_2, P_1P_3, P_1P_4, P_2P_3, P_2P_4	1	$\Gamma_0 \cong K_{1,1,2}$
10.	4	P_1P_2, P_1P_3, P_1P_4, P_2P_3, P_2P_4, P_3P_4	1	(2, 4)-threshold
11.	4	$P_1P_2P_3$, P_1P_4	1	Example 4.1
12.	4	$P_1P_3P_4$, P_1P_2, P_2P_3	2/3	Theorem 6.1 and Theorem 8.1
13.	4	$P_1P_3P_4$, P_1P_2, P_2P_3, P_2P_4	2/3	Theorem 6.1 and Theorem 8.1
14.	4	$P_1P_2P_3$, $P_1P_2P_4$	1	Example 4.2
15.	4	$P_1P_2P_4$, $P_1P_3P_4$, P_2P_3	1	Example 4.3
16.	4	$P_1P_2P_3$, $P_1P_2P_4$, $P_1P_3P_4$	1	Example 4.4
17.	4	$P_1P_2P_3$, $P_1P_2P_4$, $P_1P_3P_4$, $P_2P_3P_4$	1	(3, 4)-threshold
18.	4	$P_1P_2P_3P_4$	1	(4, 4)-threshold

EXAMPLE 4.1 (Access structure #11). Take $d = 3$ and define ϕ as follows:

$$\phi(D) = (1, 0, 0)$$

$$\phi(P_1) = (0, 1, 0)$$

$$\phi(P_2) = (1, 0, 1)$$

$$\phi(P_3) = (0, 1, -1)$$

$$\phi(P_4) = (1, 1, 0).$$

The conditions of the vector space construction could be verified as follows. First, we have $\phi(P_4) - \phi(P_1) = \phi(D)$ and $\phi(P_2) + \phi(P_3) - \phi(P_1) = \phi(D)$, so $\phi(D) \in \langle \phi(P_1), \phi(P_2), \phi(P_3) \rangle$ and $\phi(D) \in \langle \phi(P_1), \phi(P_4) \rangle$. Now, it suffices to show that $\phi(D) \notin \langle \phi(P_i) : P_i \in B \rangle$ if B is a maximal unauthorized subset. There are three such subsets B to be considered: $\{P_1, P_2\}$, $\{P_1, P_3\}$, and $\{P_1, P_3, P_4\}$. In each case, we need to establish that a system of linear equations has no solution. For example, suppose that $\phi(D) = a_2\phi(P_2) + a_3\phi(P_3) + a_4\phi(P_4)$, where $a_2, a_3, a_4 \in GF(q)$. This is equivalent to the system

$$a_2 + a_4 = 1$$

$$a_3 + a_4 = 0$$

$$a_2 - a_3 = 0.$$

The system is easily seen to have no solution. We leave the two other subsets B for the reader to consider.

To implement the scheme, D chooses $a_1 = K$, and a_2, a_3 at random. The shares he distributes are as follows:

$$P_1 \leftarrow a_2$$

$$P_2 \leftarrow a_1 + a_3$$

$$P_3 \leftarrow a_2 - a_3$$

$$P_4 \leftarrow a_1 + a_2.$$

EXAMPLE 4.2 (Access structure #14). Take $d = 3$ and define ϕ as follows:

$$\phi(D) = (1, 0, 0)$$

$$\phi(P_1) = (0, 1, 0)$$

$$\phi(P_2) = (1, 0, 1)$$

$$\phi(P_3) = (0, 1, 1)$$

$$\phi(P_4) = (0, 1, 1).$$

EXAMPLE 4.3 (Access structure #15). Take $d = 3$ and define ϕ as follows:

$$\phi(D) = (1, 0, 0)$$

$$\phi(P_1) = (0, 1, 0)$$

$$\phi(P_2) = (1, 1, 1)$$

$$\phi(P_3) = (1, -1, -1)$$

$$\phi(P_4) = (0, 0, 1).$$

EXAMPLE 4.4 (Access structure #16). Take $d = 3$ and define ϕ as follows:

$$\phi(D) = (1, 0, 0)$$

$$\phi(P_1) = (0, 1, 0)$$

$$\phi(P_2) = (0, 0, 1)$$

$$\phi(P_3) = (1, 1, 1)$$

$$\phi(P_4) = (-1, -1, 1).$$

The property (***) is satisfied in each of the above examples, and hence ideal schemes exist for these structures.

Four access structures remain to be considered: #5, #8, #12 and #13. We shall see in Section 5 that, in each case, there does not exist an ideal scheme.

5. Ideal Schemes and Matroids

In this section, we discuss some results of Brickell and Davenport [8] and Martin [17], which show some interesting and surprising connections between ideal schemes and matroids. A *matroid* is a pair $(X, \mathcal{I})$, where X is a finite set and $\mathcal{I}$ is a set of subsets of X, such that the following properties are satisfied:

1. $\emptyset \in \mathcal{I}$
2. if $A \in \mathcal{I}$ and $B \subseteq A$, then $B \in \mathcal{I}$
3. if $A, B \in \mathcal{I}$ and $|A| = |B| + 1$, then there exists $x \in A \backslash B$ such that $B \cup \{x\} \in \mathcal{I}$.

The members of $\mathcal{I}$ are called *independent sets*. Subsets of X not in $\mathcal{I}$ are called *dependent sets*; a minimal dependent set is called a *circuit*. It is well-known that matroids can equivalently be defined in terms of their circuits, as follows. Let X be a finite set and let $\mathcal{C}$ be a set of subsets of X. Then $\mathcal{C}$ is the set of circuits of a matroid if and only if the following two properties are satisfied:

1. If $A, B \in \mathcal{C}$, $A \neq B$, then $A \not\subseteq B$
2. if $A, B \in \mathcal{C}$ and $x \in A \cap B$, then there exists $C \in \mathcal{C}$ such that $C \subseteq A \cup B \backslash \{x\}$.

Let F be a field. A matroid $\mathcal{M} = (X, \mathcal{I})$ is defined to be *coordinatizable* over F if there exists a mapping $f: X \to F^d$, where F^d is the d-dimensional vector space over F, such that a subset $A \subseteq X$ is an independent set in $\mathcal{M}$ if and only if $\{f(x) : x \in A\}$ is a linearly independent multiset of vectors in F^d.

The results of this section concern connected access structures and matroids, which we define now. An access structure Γ is *connected* if every participant is contained in a minimal authorized subset (i.e., a subset in the basis Γ_0). A matroid $\mathcal{M}$ is said to be *connected* if, for every pair $x, y \in X$, there exists a circuit C such that $x, y \in C$.

Here is the first result linking matroids and ideal secret sharing schemes.

THEOREM 5.1. *[8] Suppose the connected matroid $\mathcal{M} = (X, \mathcal{I})$ is coordinatizable over a finite field F. Let $x \in X$ and let $\mathcal{P} = X \backslash \{x\}$. Then there exists an ideal scheme for the (connected) access structure having basis $\Gamma_0 = \{C \backslash \{x\} : x \in C \in \mathcal{C}\}$, where $\mathcal{C}$ denotes the set of circuits of $\mathcal{M}$.*

Proof. Let $f: X \to F^d$ be a coordinatization of $\mathcal{M}$. Define $D = \{x\}$. Then we can apply the vector space construction (Theorem 4.1), by taking the function $\phi = f$. We get an ideal scheme realizing the access structure Γ. □

It is interesting to note that from one representable matroid, we can sometimes obtain ideal schemes for more than one access structure, by choosing different points x to represent the dealer. For example, the set

$$\mathcal{C} = \{\{x_1, x_2, x_3, x_4\}, \{x_1, x_2, x_3, x_5\}, \{x_2, x_3, x_4, x_5\}, \{x_1, x_4, x_5\}\}$$

is the set of circuits of a matroid $\mathcal{M}_1$. In fact, $\mathcal{M}_1$ is coordinatizable:

$$f(x_1) = (1, 0, 0)$$

$$f(x_2) = (0, 1, 0)$$

$$f(x_3) = (0, 0, 1)$$

$$f(x_4) = (1, 1, 1)$$

$$f(x_5) = (1, -1, -1).$$

If we take $x = x_1$, then we obtain the ideal scheme for (an isomorphic copy of) access structure #15 which we presented in Section 4.2; if we take $x = x_2$, we get the scheme for access structure #16.

Brickell and Davenport have shown the more difficult result that this construction is reversible, i.e., the existence of an ideal scheme for a connected access structure gives rise to the existence of a connected matroid.

Let $\mathcal{F}$ denote the set of distribution rules for a scheme that realizes the connected access structure Γ. Denote $X = \mathcal{P} \cup \{D\}$. Suppose $A \subseteq X$ and $x \in X \backslash A$. Then we write $A \Rightarrow x$ if the following property is satisfied:

for every $f, g \in \mathcal{F}$ such that $f(y) = g(y)$ for all $y \in A$, $f(x) = g(x)$.

For example, if $A \in \Gamma$, then $A \Rightarrow D$. As another example, not involving D, observe that $\{P_1, P_3\} \Rightarrow \{P_5\}$ in Figure 1.

Now, define a set of subsets of X as follows:

$$\mathcal{D} = \{B \subseteq X : \exists x \in B, B \backslash \{x\} \Rightarrow \{x\}\}.$$

We observe that $A \cup \{D\} \in \mathcal{D}$ if $A \in \Gamma$. Informally, a set is in $\mathcal{D}$ if a dependence exists among the values $f(x)$, $x \in A$. The following result states that, if the scheme is ideal, then we have constructed a matroid.

THEOREM 5.2. *[8] Let $\mathcal{F}$ denote the set of distribution rules for an ideal scheme that realizes the connected access structure Γ. Define $X = \mathcal{P} \cup \{D\}$ and*

$$\mathcal{D} = \{B \subseteq X : \exists\, x \in B, B \backslash \{x\} \Rightarrow \{x\}\}.$$

Then $\mathcal{D}$ comprises the dependent sets of a connected matroid $\mathcal{M} = \mathcal{M}(\mathcal{F})$.

We call the matroid $\mathcal{M}(\mathcal{I})$ the *associated matroid* for the scheme $\mathcal{I}$. Note that if we start with a coordinatizable matroid $\mathcal{M}$, and construct an ideal scheme $\mathcal{I}$ from it, as described in Theorem 5.1, then $\mathcal{M}$ is the associated matroid for $\mathcal{I}$.

The associated matroid is defined in terms of the set of distribution rules $\mathcal{I}$. Hence, if we start with an access structure Γ, and we want to determine if there exists an ideal scheme realizing Γ, then Theorem 5.2 is not very useful. However, Martin [17] (see also [14]) has shown how the associated matroid can be computed as a function of the access structure Γ only (i.e., $\mathcal{M}(\mathcal{I})$ doesn't depend on the particular ideal scheme $\mathcal{I}$ realizing Γ). Given an access structure Γ, it is possible to compute a pair (X, C) such that C is the set of circuits of a matroid whenever an ideal scheme realizing the access structure Γ exists. This often allows us to prove the nonexistence of ideal schemes realizing certain access structures.

Here is Martin's method of computing C.

1. Compute $C_D = \{A \cup \{D\} : A \in \Gamma_0\}$.
2. For all $C, C' \in C_D$, $C \neq C'$, compute

$$E(C, C') = C \cup C' \setminus \left(\bigcap_{\{C'' \in C_D : C'' \subseteq C \cup C'\}} C'' \right).$$

3. Let $\mathcal{E}$ consist of all the minimal sets $E(C, C')$.
4. Define $C = C_D \cup \mathcal{E}$.

The following theorem can be proved.

THEOREM 5.3. *[17] Let Γ be an access structure and construct (X, C) as described in the algorithm above. If C is not the set of circuits of matroid, then there does not exist an ideal scheme realizing Γ.*

Briefly, what is happening is this. If there exists an ideal scheme realizing Γ, then C is the set of circuits of the associated matroid. C_D comprises the circuits containing D. It is well-known that the circuits through any element (D, in this case) determine all the circuits of a matroid. The computation of the remaining circuits is done in steps 2–4 of the algorithm. For details and proofs, see [17].

So, once we have constructed C, we can check the circuit axioms to see if we do have a matroid. If C is not a matroid, then we conclude that an ideal scheme for Γ does not exist. However, if C is a matroid, then we cannot yet conclude that an ideal scheme exists. If the matroid is coordinatizable, then an ideal scheme exists; but if the matroid is not coordinatizable, then we cannot reach any conclusion. The only example of this situation that has been studied is the Vamos matroid, which Seymour proves is not the associated matroid of any ideal scheme [20].

Let's do a couple of examples to illustrate this technique. The first example is from Martin's Ph.D. thesis [17, Example 6.2.6]. Suppose we have access structure #5. In step 1, we obtain

$$C_D = \{\{D, P_1, P_2\}, \{D, P_2, P_3\}, \{D, P_3, P_4\}\}.$$

Next, in step 2, we compute the following:

$$E(\{D, P_1, P_2\}, \{D, P_2, P_3\}) = \{D, P_1, P_2\} \cup \{D, P_2, P_3\} \backslash \{D, P_2\} = \{P_1, P_3\}$$

$$E(\{D, P_1, P_2\}, \{D, P_3, P_4\}) = \{D, P_1, P_2\} \cup \{D, P_3, P_4\} \backslash \{D\} = \{P_1, P_2, P_3, P_4\}$$

$$E(\{D, P_2, P_3\}, \{D, P_3, P_4\}) = \{D, P_2, P_3\} \cup \{D, P_3, P_4\} \backslash \{D, P_3\} = \{P_2, P_4\}.$$

Hence, we obtain

$$C = \{\{D, P_1, P_2\}, \{D, P_2, P_3\}, \{D, P_3, P_4\}, \{P_1, P_3\}, \{P_2, P_4\}\}.$$

However, C is not the set of circuits of a matroid, since there is no subset in C contained in the set

$$\{D, P_1, P_2\} \cup \{P_2, P_4\} \backslash \{P_2\} = \{D, P_1, P_4\}.$$

Hence, there does not exist an ideal scheme for this access structure.

As another example, we look at access structure #16. In step 1, we have

$$C_D = \{\{D, P_1, P_2, P_3\}, \{D, P_1, P_2, P_4\}, \{D, P_1, P_3, P_4\}\}.$$

In step 2, we obtain the circuit $\{P_2, P_3, P_4\}$. The resulting set of circuits produces a matroid isomorphic to matroid $\mathcal{M}_1$ described above.

By application of these techniques, the following result can be shown (see [17, Lemma 6.2.7]).

THEOREM 5.4. *Suppose Γ is a connected access structure on four participants. Then there exists an ideal scheme realizing Γ if and only if Γ is not isomorphic to one of access structures #5, #8, #12 or #13.*

6. The Entropy Bound on the Information Rate

Denote by $\rho^* = \rho^*(\Gamma)$ the maximum information rate for any perfect secret sharing scheme realizing a specified access structure Γ. The first result we mention is an entropy bound that will lead to an upper bound on ρ^* for certain access structures. The *binary entropy* of a probability distribution p on a finite set X is defined to be

$$H(\mathbf{X}) = -\sum_{\{x \in X: p(x) > 0\}} p(x) \log_2 p(x).$$

We have already defined a probability distribution $p_{\mathcal{K}}$ on $\mathcal{K}$; the entropy of this probability distribution is denoted $H(\mathbf{K})$. For any subset of participants $B \subseteq \mathcal{P}$, the set $\mathcal{F}$ of distribution rules of the scheme, together with the probability distribution on $\mathcal{K}$, induce

a probability distribution on the list of shares given to the participants in B. We will denote this probability distribution by $p_{\mathcal{S}(B)}$ and the entropy of this probability distribution by $H(\mathbf{B})$.

We state the following important theorem of Capocelli, De Santis, Gargano and Vaccaro [11] without proof.

THEOREM 6.1. *[11] Suppose* Γ *is an access structure such that*

$$\{P_1, P_2\}, \{P_2, P_3\}, \{P_1, P_3, P_4\} \in \Gamma$$

and

$$\{P_1, P_3\}, \{P_2\}, \{P_1, P_4\} \notin \Gamma.$$

Let $\mathcal{S}$ *be any perfect secret sharing scheme realizing* Γ. *Then* $H(\mathbf{P}_2\mathbf{P}_3) \geq 3H(\mathbf{K})$.

Now, suppose that Γ is an access structure that satisfies the hypotheses of Theorem 6.1. Suppose the $|\mathcal{K}|$ keys are equally probable; then $H(\mathbf{K}) = \log_2 |\mathcal{K}|$. By a basic property of entropy, we have that

$$H(\mathbf{P}_2\mathbf{P}_3) \leq \log_2 |\mathcal{S}_2 \times \mathcal{S}_3| = \log_2 |\mathcal{S}_2| + \log_2 |\mathcal{S}_3|.$$

By Theorem 6.1, we have that

$$\log_2 |\mathcal{S}_2| + \log_2 |\mathcal{S}_3| \geq 3 \log_2 |\mathcal{K}|.$$

Now, by the definition of information rate, we have $\rho \leq \log_2 |\mathcal{K}|/\log_2 |\mathcal{S}_2|$ and $\rho \leq \log_2 |\mathcal{K}|/\log_2 |\mathcal{S}_3|$. It follows that

$$\begin{aligned} 3 \log_2 |\mathcal{K}| &\leq \log_2 |\mathcal{S}_2| + \log_2 |\mathcal{S}_3| \\ &\leq \frac{\log_2 |\mathcal{K}|}{\rho} + \frac{\log_2 |\mathcal{K}|}{\rho} \\ &= 2 \frac{\log_2 |\mathcal{K}|}{\rho}. \end{aligned}$$

Hence, $\rho \leq 2/3$. This bound holds for any scheme realizing Γ, so it follows that $\rho^* \leq 2/3$. Now, for the access structures #5, #8, #12 and #13, the hypotheses of Theorem 6.1 are satisfied. Hence, $\rho^* \leq 2/3$ for these four access structures. Note that this strengthens the nonexistence result of Theorem 5.4. We record this as follows.

THEOREM 6.2. *Suppose* Γ *is connected access structure on four participants. If* Γ *is isomorphic to one of access structures #5, #8, #12 or #13, then* $\rho^*(\Gamma) \leq 2/3$.

7. The Decomposition Construction

Let us continue to study the access structures #5, #8, #12 and #13. Of course, we can use the monotone circuit construction to produce perfect schemes. However, by this method, the best we can do is to obtain information rate $\rho = 1/2$ in each case. We can get $\rho = 1/2$ in cases #5 and #12 by using a disjunctive normal form Boolean circuit. For case #8 and #13, a disjunctive normal form Boolean circuit will yield $\rho = 1/3$, but other monotone circuits exist which allow us to attain $\rho = 1/2$. However, we will show in this section that it is possible to construct schemes with $\rho > 1/2$ for each of these four access structures.

Our main construction is a recursive construction using ideal schemes as building blocks in the construction of larger schemes. We call this the decomposition construction. (A special case of this construction has appeared in [6].) Suppose Γ is an access structure having basis Γ_0. Let $\mathcal{K}$ be a specified key set. An *ideal decomposition* of Γ_0 consists of a set $\{\Gamma_1, \ldots, \Gamma_n\}$ such that the followign properties are satisfied:

1. $\Gamma_k \subseteq \Gamma_0$ for $1 \leq k \leq n$
2. $\bigcup_{k=1}^{n} \Gamma_k = \Gamma_0$
3. for $1 \leq k \leq n$, there exists an ideal scheme with key set $\mathcal{K}$, on the subset of participants $\mathcal{P}_k = \bigcup_{B \in \Gamma_k} B$, for the access structure having basis Γ_k.

In most cases, $\{\Gamma_1, \ldots, \Gamma_n\}$ will form a partition of Γ_0, but this is not a requirement.

Now, for $1 \leq j \leq \ell$, suppose $\{\Gamma_{j,1}, \ldots, \Gamma_{j,n_j}\}$ is an ideal decomposition of Γ_0. For $1 \leq j \leq \ell$, $1 \leq k \leq n_j$, we have an ideal scheme with $\mathcal{F}^{j,k}$ as its set of distribution rules. We will construct a scheme with key set $\mathcal{K}^{\ell}$. The set of distribution rules $\mathcal{F}$ is constructed according to the following recipe. Suppose D wants to share a secret $(K_1, \ldots, K_\ell)$. Then for $1 \leq j \leq \ell$, $1 \leq k \leq n_j$, he chooses a random distribution rule $f^{j,k} \in \mathcal{F}_{K_j}^{j,k}$ and distributes the resulting shares to the participants in $\mathcal{P}_{j,k}$.

Let us compute the information rate of the resulting scheme. This involves first determining the total number of shares given to each participant, and then dividing ℓ by this quantity. For every participant P_i and for $1 \leq j \leq \ell$, define

$$R_{ji} = |\{k : P_i \in \mathcal{P}_{j,k}\}|,$$

so R_{ji} denotes the number of shares given to P_i from the schemes $\mathcal{F}^{j,k}$, $1 \leq k \leq n_j$. Define

$$R_i = \sum_{j=1}^{\ell} R_{ji},$$

i.e., the total number of shares given to P_i. Then

$$\rho_i = \frac{\log_2 |\mathcal{K}|^{\ell}}{\log_2 |\mathcal{K}|^{R_i}} = \frac{\ell}{R_i}.$$

If we let

$$R = \max\{R_i : 1 \le i \le w\},$$

then the scheme realizing the access structure Γ has information rate ℓ/R.

We summarize the above discussion in the following theorem.

Theorem 7.1. *Let Γ be an access structure having basis Γ_0. For $1 \le j \le \ell$, suppose $\{\Gamma_{j,1}, \ldots, \Gamma_{j,n_j}\}$ is an ideal decomposition of Γ_0, where $\mathcal{P}_{j,k}$ denotes the partcipant set for the access structure $\Gamma_{j,k}$. Define*

$$R = \max\left\{\sum_{j=1}^{\ell} |\{k : P_i \in \mathcal{P}_{j,k}\}| : 1 \le i \le w\right\}.$$

Then $\rho^*(\Gamma) \ge \ell/R$.

7.1. Examples

Let's look at examples of this construction for our four problematic access structures. These examples will also illustrate the advantage of using $\ell > 1$ decompositions. In the case of access structure #5, for example, if we take $\ell = 1$, then any ideal decomposition will have $R \ge 2$ and hence $\rho \le 1/2$. However, by taking $\ell = 2$, we can obtain $\rho = 2/3$, which is optimal, as follows.

EXAMPLE 7.1 (Access structure #5). Take $\ell = 2$, $\mathcal{K} = GF(q)$ for any prime power q, and define the two ideal decompositions to be:

$$\Gamma_{1,1} = \{\{P_1, P_2\}\}$$

$$\Gamma_{1,2} = \{\{P_2, P_3\}, \{P_3, P_4\}\}$$

$$\Gamma_{2,1} = \{\{P_1, P_2\}, \{P_2, P_3\}\}$$

$$\Gamma_{2,2} = \{\{P_3, P_4\}\}$$

Then $R_1 = R_4 = 2$ and $R_2 = R_3 = 3$. Hence $R = 3$ and $\rho = 2/3$. One implementation of the scheme is as follows. D will choose four random elements (independently) from $GF(q)$, say b_{11}, b_{12}, b_{21}, and b_{22}. Given a key $(K_1, K_2) \in GF(q)^2$, D distributes shares as follows:

$$P_1 \leftarrow (b_{11}, b_{21});$$

$$P_2 \leftarrow (b_{11} + K_1, b_{12}, b_{21} + K_2);$$

$$P_3 \leftarrow (b_{12} + K_1, b_{21}, b_{22});$$

$$P_4 \leftarrow (b_{12}, b_{22} + K_2).$$

EXAMPLE 7.2 (Access structure #8). Take $\ell = 2$, $\mathcal{K} = GF(q)$ for any prime power q, and define the two ideal decompositions to be:

$$\Gamma_{1,1} = \{\{P_1, P_2\}\}$$

$$\Gamma_{1,2} = \{\{P_2, P_3\}, \{P_2, P_4\}, \{P_3, P_4\}\}$$

$$\Gamma_{2,1} = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}\}$$

$$\Gamma_{2,2} = \{\{P_3, P_4\}\}$$

This scheme has $\rho = 2/3$. An implementation is as follows. D will choose four random elements (independently) from $GF(q)$ ($q \neq 2^j$), say b_{11}, b_{12}, b_{21}, and b_{22}. Given a key $(K_1, K_2) \in GF(q)^2$, D distributes shares as follows:

$$P_1 \leftarrow (b_{11} + K_1, b_{21} + K_2);$$

$$P_2 \leftarrow (b_{11}, b_{12}, b_{21});$$

$$P_3 \leftarrow (b_{12} + K_1, b_{21} + K_2, b_{22});$$

$$P_4 \leftarrow (b_{12} + 2K_1, b_{21} + K_2, b_{22} + K_2).$$

EXAMPLE 7.3 (Access structure #12). Take $\ell = 3$ and define the three ideal decompositions to be:

$$\Gamma_{1,1} = \{\{P_1, P_2\}\}$$

$$\Gamma_{1,2} = \{\{P_2, P_3\}, \{P_1, P_3, P_4\}\}$$

$$\Gamma_{2,1} = \{\{P_2, P_3\}\}$$

$$\Gamma_{2,2} = \{\{P_1, P_2\}, \{P_1, P_3, P_4\}\}$$

$$\Gamma_{3,1} = \{\{P_1, P_2\}, \{P_2, P_3\}\}$$

$$\Gamma_{3,2} = \{\{P_1, P_3, P_4\}\}.$$

The resulting scheme has $\rho = 3/5$.

EXAMPLE 7.4 (Access structure #13). Take $\ell = 4$ and define the four ideal decompositions to be:

$$\Gamma_{1,1} = \{\{P_1, P_2\}\}$$

$$\Gamma_{1,2} = \{\{P_2, P_3\}, \{P_2, P_4\}, \{P_1, P_3, P_4\}\}$$

$$\Gamma_{2,1} = \{\{P_2, P_3\}\}$$

$$\Gamma_{2,2} = \{\{P_1, P_2\}, \{P_2, P_4\}, \{P_1, P_3, P_4\}\}$$

$$\Gamma_{3,1} = \{\{P_2, P_4\}\}$$

$$\Gamma_{3,2} = \{\{P_1, P_2\}, \{P_2, P_3\}, \{P_1, P_3, P_4\}\}$$

$$\Gamma_{4,1} = \{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}\}$$

$$\Gamma_{4,2} = \{\{P_1, P_3, P_4\}\}.$$

The resulting scheme has $\rho = 4/7$.

The schemes presented in Examples 7.1 and 7.2 have optimal information rates, by Theorem 6.2. The schemes presented in Examples 7.3 and 7.4 have the best possible information rate that can be obtained by application of the ideal decomposition construction. This can be seen by solving a suitable linear programming problem using techniques described in [6]. However, we shall see in the next section how to construct (optimal) schemes with information rate 2/3 for these two access structures.

8. The Simmons Geometric Construction

In this section, we describe the Simmons geometric construction [23], [26], [25], which can be thought of as a far-reaching generalization of the Blakley threshold scheme [5]. Our description is not the most general one possible, but it is sufficient for our purposes.

Let q be a prime power and consider the n-dimensional vector space over $GF(q)$. A *flat* is defined to be a subspace or a translation (i.e., coset) of a subspace. The collection of all flats constitutes the n-dimensional *affine geometry* $AG(n, q)$. A flat is called a *point* if its dimension is 0; a *line* if its dimension is 1; a *plane* if its dimension is 2; and a *hyperplane* if its dimension is $n - 1$. If $X = \{x_1, \ldots, x_m\}$ is a set of points in $AG(n, q)$, then we define $Span(X)$ to be the smallest flat containing all the points in X. It is easy to see that

$$Span(X) = \left\{ \sum_{i=1}^{m} \alpha_i x_i : \alpha_1, \ldots, \alpha_m \in GF(q), \sum_{i=1}^{m} \alpha_i = 1 \right\}.$$

Suppose V_D is a fixed line in $AG(n, q)$. We will construct a secret sharing scheme with $\mathcal{K} = V_D$, so $|\mathcal{K}| = q$. Let V_I be a hyperplane such that $|V_I \cap V_D| = 1$; the key will be the unique point $K = V_I \cap V_D$. Every participant P_i will be given a share consisting of a set $d(P_i)$ of R_i points in V_I. The sets P_i are chosen in such a way that, for every $B \subseteq \Gamma$, we have

$$Span\left(\bigcup_{\{i:P_i \in B\}} d(P_i) \right) \cap V_D = \emptyset \Leftrightarrow B \notin \Gamma. \tag{3}$$

When a subset of participants, B, wishes to compute the secret, they will compute the span of the shares they collectively hold, and intersect it with V_D. If the intersection is nonempty, then the (unique) point of intersection is the key K.

A participant P_i will receive R_i points of n-dimensional space for his or her share. Since there are only q possible keys, the information rate will be very low ($1/n$ in the (best) case where $R_i = 1$). However, a careful implementation will allow us to increase the information rate considerably; this implementation is based on the description given by Martin [17, pp. 88–96]. Suppose we can find one hyperplane V_I and one collection of sets of points $d(P_i)$, $1 \leq i \leq w$, such that the condition (3) is satisfied, where the key is K_0. This will be called a *Simmons geometric configuraiton*.

Now, for $1 \leq i \leq w$, denote

$$d(P_i) = \{x_{ij} : 1 \leq j \leq R_i\}.$$

Let L_{ij} be the (unique) line parallel to V_D that contains x_{ij}, for $1 \leq i \leq w$, $1 \leq j \leq R_i$. For every hyperplane Π such that $|\Pi \cap V_D| = 1$, define a distribution function f_Π by the rule

$$f_\Pi(D) = \Pi \cap V_D$$

$$f_\Pi(P_i) = \{L_{ij} \cap \Pi : 1 \leq j \leq R_i\},\ 1 \leq i \leq w.$$

The scheme will have q^n distribution rules and $|\mathcal{S}_i| = q^{R_i}$, $1 \leq i \leq w$. Hence, the information rate is $\rho = \min\{1/R_i : 1 \leq i \leq w\}$.

Now, let's further refine the implementation so that it is not necessary to communicate points in n-dimensional space as the shares. Observe that the shares and the secret all lie on publicly known lines. Suppose that all the x_{ij}'s and K_0 are made public, as is the direction vector e of the lines L_{ij} and V_D. Then we can fix the following parametric description of these lines:

$$V_D = \{K_0 + \lambda e : \lambda \in GF(q)\}$$

$$L_{ij} = \{x_{ij} + \lambda_{ij} e : \lambda_{ij} \in GF(q)\},\ 1 \leq i \leq w,\ 1 \leq j \leq R_i.$$

A hyperplane Π consists of the solutions to an equation $A \cdot x = B$. We are interested only in hyperplanes that meet V_D in a point; this happens if and only if $A \cdot e \neq 0$. Hence, multiplying A and B by a scalar if necessary, we can assume without loss of generality that $A \cdot e = 1$.

Now, straightforward linear algebra shows that $K = K_0 + \lambda e$, where

$$\lambda = B - A \cdot K_0,$$

and $L_{ij} \cap \Pi = x_{ij} + \lambda_{ij} e$, where

$$\lambda_{ij} = B - A \cdot x_{ij},$$

for all i, j.

There exists a $1-1$ correspondence between field elements λ and points on V_D; and likewise there is a $1-1$ correspondence between the values λ_{ij} and points on L_{ij} (for all i, j). Hence, we can take the λ_{ij}'s to be the shares and the value λ to be the secret. In this way we use only scalars (rather than n-dimensional vectors) as shares and the secret. Then our modified distribution rules are:

$$f_\Pi(D) = B - A \cdot K_0$$

$$f_\Pi(P_i) = \{B - A \cdot x_{ij} : 1 \leq j \leq R_i\},\ 1 \leq i \leq w.$$

An authorized subset B can compute the key λ as a function of the shares λ_{ij} as follows. Since

$$K_0 \in Span\left[\sum_{\{i:P_i \in B\}} \bigcup_{j=1}^{R_i} x_{ij}\right],$$

we can express K_0 as

$$K_0 = \sum_{\{i:P_i \in B\}} \sum_{j=1}^{R_i} \alpha_{ij} x_{ij},$$

where

$$\sum_{\{i:P_i \in B\}} \sum_{j=1}^{R_i} \alpha_{ij} = 1.$$

Then it is easy to see that

$$\lambda = \sum_{\{i:P_i \in B\}} \sum_{j=1}^{R_i} \alpha_{ij} \lambda_{ij},$$

8.1. Examples

We give two examples of Simmons geometric configurations due to Martin [17, p. 227] concerning the access structures #12 and #13.

EXAMPLE 8.1 (Access structure #12). Take $n = 3$ and let V_I be a plane meeting V_D in a point, K_0. Choose four points $y_1, y_2, y_3, y_4 \in V_I$ such that no three of the five points y_1, y_2, y_3, y_4, K_0 are collinear. Define $x_{11} = y_1$, $x_{21} = y_2$, $x_{22} = y_4$, $x_{31} = y_3$ and $x_{41} = y_4$. (Hence, $R_1 = R_3 = R_4 = 1$ and $R_2 = 2$.) The resulting scheme has information rate 1/2.

Here is a possible implementation. Suppose $K_0 = (0, 0, 0)$, $e = (0, 0, 1)$, and V_I is the plane $z = 0$. Suitable points are $y_1 = (-1, 0, 0)$, $y_2 = (0, 1, 0)$, $y_3 = (1, -1, 0)$ and $y_4 = (1, 1, 0)$ (provided q is not a power of two). A plane Π that meets V_D in a point has the equation $ax + by + z = K$, where K is the secret and a, b are random.

The shares that the four participants receive are the following:

$$P_1 \leftarrow (K + a);$$

$$P_2 \leftarrow (K - b, K - a - b);$$

$$P_3 \leftarrow (K - a + b);$$

$$P_4 \leftarrow (K - a - b).$$

EXAMPLE 8.2 (Access structure #13). Take $n = 3$ and let V_I be a plane meeting V_D in a point, K_0. Choose five points $y_1, y_2, y_3, y_4, y_5 \in V_I$ such that no three of the six points $y_1, y_2, y_3, y_4, y_5, K_0$ are collinear. Define $x_{11} = y_1$, $x_{21} = y_2$, $x_{22} = y_5$, $x_{31} = y_3$ and $x_{41} = y_4$. (Hence, $R_1 = R_3 = R_4 = 1$ and $R_2 = 2$.) The resulting scheme will have information rate 1/2.

8.2. Combining Geometric and Nongeometric Schemes

Theorem 7.1 combined ℓ ideal decompositions to produce a secret sharing scheme. However, there is no reason why we need to restrict ourselves to schemes arising from ideal decompositions. In particular, we can use a Simmons geometric scheme in place of an ideal decomposition. The computation of the information rate will remain unchanged since the R's in a Simmons scheme have the same function as the R's in an ideal decomposition (i.e., they count the number of elements of $GF(q)$ given to each participant).

With this observation, it is a simple matter to obtain schemes with information rate 2/3 for access structures #12 and #13. For access structure #12, take $\ell = 2$ and use the third ideal decomposition of Example 7.3 together with the Simmons scheme from Example 8.1. For access structure #13, take $\ell = 2$ and use the fourth ideal decomposition of Example 7.4 together with the Simmons scheme from Example 8.2. We have the following:

THEOREM 8.1. *If Γ is isomorphic to access structure #12 or #13, then $\rho^*(\Gamma) = 2/3$.*

9. Access Structures Based on Graphs

In this section, we survey bounds on $\rho^*(\Gamma(G))$, where G is a graph. Our first result is an upper bound on $\rho^*(\Gamma(G))$ whenever G is not a complete multipartite graph.

THEOREM 9.1. *[6] Suppose G is a connected graph that is not a complete multipartite graph. Then $\rho^*(\Gamma(G)) \leq 2/3$.*

The proof of this theorem involves showing that any connected graph which is not a multipartite graph contains an induced subgraph on four vertices that is isomorphic to the basis of access structure #5 or #8.

Since $\rho^* = 1$ for complete multipartite graphs, Theorem 9.1 tells us that it is never the case that $2/3 < \rho^* < 1$ for any access structure that is the closure of the edge set of a connected graph.

For paths, and for cycles of even length, ρ^* can be determined exactly.

THEOREM 9.2 *[6].*

1. If P_n is the path with n edges ($n \geq 3$), then $\rho^*(\Gamma(P_n)) = 2/3$.
2. If C_n is the cycle of length n, where n is even, ($n \geq 6$), then $\rho^*(\Gamma(C_n)) = 2/3$.
3. If C_n is the cycle of length n, where n is odd, ($n \geq 5$)), then

$$\frac{2n}{3n+1} \leq \rho^*(\Gamma(C_n)) \leq \frac{2}{3}.$$

The lower bounds of Theorem 9.2 are proved using the ideal decomposition construction (Theorem 7.1), by partitioning the edge sets of the relevant graphs into K_2's and $K_{1,2}$'s. In parts 1 and 2, we take $\ell = 2$; in part 3, we set $\ell = n$. With these clues, the reader can probably construct the decompositions, but the details can be found in [6].

There are some general lower bounds on ρ^* that can be proved using the decomposition construction with $\ell = 1$. Here are two such results.

THEOREM 9.3. *[9] Let G be a graph having maximum degree d. Then*

$$\rho^*(\Gamma(G)) \geq \frac{1}{\left\lceil \frac{d}{2} \right\rceil + 1}.$$

This is proved by decomposing G into comlete bipartite graphs $K_{1,m}$ (such a decomposition is called a *star decomposition*, since $K_{1,m}$ is often called a *star*). In the case where G is regular and has girth at least 5, this result is the best that can be obtained using star decompositions [9, Theorem 3.9].

To illustrate the proof technique, we prove Theorem 9.3 in the special case when G is regular of degree d, and d is even. Construct a (directed) eulerian tour of G, and for each vertex v, define G_v to consist of the $d/2$ edges directed into v. Then the subgraphs G_v, $v \in V(G)$, comprise an ideal decomposition for which $R = 1 + d/2$. The result follows from Theorem 7.1.

The lower bound of Theorem 9.3 can be improved whenever G is acyclic, as stated in the following theorem. The proof involves finding a suitable star decomposition by means of a simple recursive algorithm.

THEOREM 9.4. *[6] For any tree T, $\rho^*(\Gamma(T)) \geq 1/2$.*

Next, we discuss some very general bounds, proved in [27], that depend only on the number of vertices in the graph. These bounds use *balanced incomplete block designs* (BIBDs). A $(v, k, 1)$-BIBD is a pair $(V, \mathcal{A})$, where $|V| = v$ and $\mathcal{A}$ is a set of k-subsets of V (called *blocks*), such that every pair of elements of V occurs in exactly one block. By elementary counting, it follows that every element of V occurs in exactly $r = (v - 1)/(k - 1)$ blocks. For information on the existence of BIBDs, we refer to [3].

We will use the following notation: a $PS(G, \rho, q)$ denotes a perfect secret sharing scheme for the access structure $\Gamma(G)$, for a set of q keys, with information rate ρ.

Now, suppose $G = (V, E)$ has v vertices and suppose $(V, \mathcal{A})$ is a $(v, k, 1)$-BIBD. Fix an integer q. For every block A, suppose there is a $PS(G[A], \rho_A, q)$ where $G[A]$ denotes the induced subgraph of G on the vertices in A. Then, for every $v \in V$, let

$$\rho_v = \frac{1}{\Sigma_{\{A \in \mathcal{A}: v \in A\}} \frac{1}{\rho_A}}.$$

It follows from [9, Theorem 3.5] that

$$\rho^*(\Gamma(G)) \geq \min\{\rho_v : v \in V\}. \tag{4}$$

The bound (4) is a straightforward generalization of the ideal decomposition construction (with $\ell = 1$) to the more general situation where we use *subschemes* that are not necessarily ideal. If every $\rho_A = 1$, then we have an ideal decomposition, and the information rate is the same as that obtained from Theorem 7.1.

We will compute bounds on the information rate by using BIBDs of various block sizes. We first define $\rho(k) = \min\{\rho^*(\Gamma(G)) : |V(G)| = k\}$. We will use the following bounds:

$$\rho(3) = 1$$

$$\rho(4) = \frac{2}{3}$$

$$\rho(5) \geq \frac{4}{7}.$$

The values of $\rho(3)$ and $\rho(4)$ follow from Table 1. Information rates for the 21 connected graphs on five vertices were studied in [6], where the bound $\rho(5) \geq 4/7$ is proved. All of these bounds come from application of the ideal decomposition construction. In the case of an access structure $\Gamma(G)$, where G is a graph, an ideal decomposition consists of a decomposition into complete multipartite graphs. The number of decompositions used is at most five [6]. Since the least common multiple of 2, 3, 4 and 5 is 60, it follows from Theorem 4.2 that for any graph G with $k = |V(G)|$, where $3 \leq k \leq 5$, there exists a $PS(G, \rho, q^{60})$ with $\rho \geq \rho(k)$ for all prime powers $q \geq k + 1$.

Now, from Equation (4), we get

$$\rho^*(\Gamma(G)) \leq \frac{\rho(k)}{r} = \frac{(k - 1)\rho(k)}{v - 1}$$

whenever a $(v, k, 1)$-BIBD exists. We obtain the following bounds, depending on the value of k:

$$k = 3 \quad \rho^*(\Gamma(G)) \geq \frac{2}{v - 1}$$

$$k = 4 \quad \rho^*(\Gamma(G)) \geq \frac{2}{v - 1}$$

$$k = 5 \quad \rho^*(\Gamma(G)) \geq \frac{16}{7(v - 1)}$$

It is interesting to observe how the bounds improve as we use BIBDs with larger block size. Also, note that if there does not exist a $(v, k, 1)$-BIBD, then we take the smallest integer $v_0 > v$ such that there does exist a $(v_0, k, 1)$-BIBD, and we obtain the bound

$$\rho^*(\Gamma(G)) \leq \frac{(k - 1)\rho(k)}{v_0 - 1}.$$

This is accomplished by deleting $v_0 - v$ points from the BIBD, thereby constructing a pairwise balanced design [3] on v points, and then proceeding in a similar way.

A a final example, we pose a puzzle for the reader. Let G be the Petersen graph. The first part of the puzzle is to prove that $\rho^*(\Gamma(G)) \geq 10/21$. This can be done using the ideal decomposition construction. The second part of the puzzle is to prove that 10/21 is the best lower bound that can be obtained by application of Theorem 7.1.

10. Conclusion

Although this is a lengthy paper, we have really treated only one aspect of secret sharing schemes here, namely the construction of schemes with information rate as high as possible. There has also been considerable study of schemes with *extended capabilities*. The idea of protecting against cheating by one or more participants is addressed in [18], [28], [1], [19], [22] and [10]. Prepositioned schemes are studied in [24]. The question of how to set up a secret sharing scheme in the absence of a trusted party is solved in [12]. Finally, schemes that permit disenrollment of participants are discussed in [4].

Acknowledgment

I would like to thank Dean Hoffman, Keith Martin and John van Rees for helpful comments and discussions.

References

1. M. Ben-Or, S. Goldwasser, and A. Wigderson, Completeness theorems for noncryptographic fault-tolerant distributed computation, *Proc. 20th ACM Symp. on Theory of Computing*, (1988), pp. 1–10.
2. J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, New York, 403, (1990), pp. 27–35.
3. T. Beth, J. Jungnickel, and H. Lenz, *Design Theory*. Bibliographisches Institut, Zurich, (1985).
4. B. Blakley, G.R. Blakley, A.H. Chan, and J.L. Massey, Threshold schemes with disenrollment, presented at *CRYPTO '92*.
5. G.R. Blakley, Safeguarding cryptographic keys, *AFIPS Conference Proceedings*, Vol. 48, (1979), pp. 313–317.
6. C. Blundo, A. De Santis, D.R. Stinson, and U. Vaccaro, Graph decomposition and secret sharing schemes. Presented at EUROCRYPT '92, submitted to *Journal of Cryptology*.
7. E.F. Brickell, Some ideal secret sharing schemes, *J. Combin. Math. and Combin. Comput.*, Vol. 9, (1989), pp. 105–113.
8. E.F. Brickell and D.M. Davenport, On the classification of ideal secret sharing schemes, *J. Cryptology*, Vol. 4, (1991), pp. 123–134.
9. E.F. Brickell and D.R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, to appear in *J. Cryptology*. Preliminary version appeared in *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, New York, 537, (1991), pp. 242–252.
10. E.F. Brickell and D.R. Stinson, The detection of cheaters in threshold schemes. *SIAM J. on Discrete Math.*, Vol. 4, (1991), pp. 502–510. Preliminary version appeared in *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, New York, 403, (1990), pp. 564–577.
11. R.M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, On the size of shares for secret sharing schemes. Submitted to *J. Cryptology*. Preliminary version appeared in *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, New York, 576, (1992), pp. 101–113.
12. I. Ingemarsson and G.J. Simmons, A protocol to set up shared secret schemes without the assistance of a mutually trusted party, *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, New York, 473, (1991), pp. 266–282.
13. M. Ito, A. Saito, and T. Nishizeki, Secret sharing scheme realizing general access structure, *Proc. IEEE Globecom '87*, (1987), pp. 99–102.
14. W.-A. Jackson and K.M. Martin, On ideal secret sharing schemes. Submitted to *J. Cryptology*.
15. E.D. Karnin, J.W. Greene, and M.E. Hellman, On secret sharing systems, *IEEE Trans. Inform. Theory*, Vol. 29, (1983), pp. 35–41.
16. K.M. Martin, New secret sharing schemes from old. Submitted to *J. Comb. Math. Comb. Comp.*
17. K.M. Martin, *Discrete Structures in the Theory of Secret Sharing*. Ph.D. thesis, University of London, 1991.
18. R.J. McEliece and D.V. Sarwate, On sharing secrets and Reed-Solomon codes, *Commun. of the ACM*, Vol. 24, (1981), pp. 583–584.
19. T. Rabin and M. Ben-Or, Verifiable secret sharing and multiparty protocols with honest majority, *Proc. 21st ACM Symp. on Theory of Computing*, (1989), pp. 73–85.
20. P.D. Seymour, On secret-sharing matroids. To appear in *Journal of Combin. Theory B*.
21. A. Shamir, How to share a secret, *Commun. of the ACM*, Vol. 22, (1979), pp. 612–613.
22. G.J. Simmons, Robust shared secret schemes or 'how to be sure you have the right answer even though you don't known the question,' *Congressus Numer.*, Vol. 68, (1989), pp. 215–248.
23. G.J. Simmons, How to (really) share a secret, *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, New York, 403, (1990), pp. 390–448.
24. G.J. Simmons, Prepositioned shared secret and/or shared control schemes, *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, New York, 434, (1990), pp. 436–467.
25. G.J. Simmons, An introduction to shared secret and/or shared control schemes and their application, In (G.J. Simmons, ed.) *Contemporary Cryptology, The Science of Information Integrity*, IEEE Press, New York, (1991), pp. 441–497.
26. G.J. Simmons, W. Jackson, and K. Martin, The geometry of shared secret schemes, *Bulletin of the ICA*, Vol. 1, (1991), pp. 71–88.
27. D.R. Stinson, New general lower bounds on the information rate of secret sharing schemes. Presented at *CRYPTO '92*.
28. M. Tompa and H. Woll, How to share a secret with cheaters, *J. Cryptology*, Vol. 1, (1988), pp. 133–138.