11

Secret Sharing Schemes

11.1 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 they do not trust the combination to any individual teller. Hence, we would like to design a system whereby any two of the three senior tellers can gain access to the vault, but no individual teller can do so. This problem can be solved by means of a *secret sharing scheme*, the topic of this chapter.

Here is an interesting "real-world" example of this situation: According to *Time Magazine*[1], control of nuclear weapons in Russia involves a similar "two-out-of-three" access mechanism. The three parties involved are the President, the Defense Minister and the Defense Ministry.

We first study a special type of secret sharing scheme called a threshold scheme. Here is an informal definition.

DEFINITION 11.1 *Let t, w be positive integers, $t \leq w$. A (t, w)-**threshold scheme** is a method of sharing a **key** K among a set of w participants (denoted by $\mathcal{P}$), in such a way that any t participants can compute the value of K, but no group of $t-1$ participants can do so.*

Note that the examples described above are $(2, 3)$-threshold schemes.

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 key K. (Alternatively, they could give their shares to a trusted authority which will perform the computation for them.) If $|B| \geq t$, then

[1] Time Magazine, May 4, 1992, p. 13

FIGURE 11.1
The Shamir (t, w)-threshold scheme in $\mathbb{Z}_p$

Initialization Phase

1. D chooses w distinct, non-zero elements of $\mathbb{Z}_p$, denoted x_i, $1 \leq i \leq w$ (this is where we require $w \geq p+1$). For $1 \leq i \leq w$, D gives the value x_i to P_i. The values x_i are public.

Share Distribution

2. Suppose D wants to share a key $K \in \mathbb{Z}_p$. D secretly chooses (independently at random) $t-1$ elements of $\mathbb{Z}_p$, $a_1, \ldots, a_{t-1}$.
3. For $1 \leq i \leq w$, D computes $y_i = a(x_i)$, where
$$a(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod p.$$
4. For $1 \leq i \leq w$, D gives the share y_i to P_i.

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.

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 the *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).

In this section, we present a method of constructing a (t, w)-threshold scheme, called the **Shamir Threshold Scheme**, which was invented in 1979. Let $\mathcal{K} = \mathbb{Z}_p$, where $p \geq w+1$ is prime. Also, let $\mathcal{S} = \mathbb{Z}_p$. Hence, the key will be an element of $\mathbb{Z}_p$, as will be each share given to a participant. The Shamir threshold scheme is presented in Figure 11.1. In this scheme, the dealer constructs a random polynomial $a(x)$ of degree at most $t-1$ in which the constant term is the key, K. Every participant P_i obtains a point (x_i, y_i) on this polynomial.

Let's look at how a subset B of t participants can reconstruct the key. This is basically accomplished by means of polynomial interpolation. We will describe a couple of methods of doing this.

Suppose that 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 $a(x) \in \mathbb{Z}_p[x]$ 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 elements of $\mathbb{Z}_p$, and $a_0 = K$ is the key. Since $y_{i_j} = a(x_{i_j})$, $1 \leq j \leq t$, B can obtain t linear equations in the t unknowns $a_0, \ldots, a_{t-1}$, where all arithmetic is done in $\mathbb{Z}_p$. If the equations are linearly independent, there will be a unique solution, and a_0 will be revealed as the key.

Here is a small example to illustrate.

Example 11.1

Suppose that $p = 17$, $t = 3$, and $w = 5$; and the public x-co-ordinates 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. Writing the polynomial $a(x)$ as

$$a(x) = a_0 + a_1 x + a_2 x^2,$$

and computing $a(1)$, $a(3)$ and $a(5)$, the following three linear equations in $\mathbb{Z}_{17}$ 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 $\mathbb{Z}_{17}$: $a_0 = 13$, $a_1 = 10$, and $a_2 = 2$. The key is therefore $K = a_0 = 13$. □

Clearly, it is important that the system of t linear equations has a unique solution, as in Example 11.1. 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

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

and

$$a_0 = K.$$

The system of linear equations (in $\mathbb{Z}_p$) is the following:

$$\begin{aligned} a_0 + a_1 x_{i_1} + a_2 {x_{i_1}}^2 + \ldots + a_{t-1} {x_{i_1}}^{t-1} &= y_{i_1} \\ a_0 + a_1 x_{i_2} + a_2 {x_{i_2}}^2 + \ldots + a_{t-1} {x_{i_2}}^{t-1} &= y_{i_2} \\ &\vdots \\ a_0 + a_1 x_{i_t} + a_2 {x_{i_t}}^2 + \ldots + a_{t-1} {x_{i_t}}^{t-1} &= y_{i_t}. \end{aligned}$$

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. There is a well-known formula for the determinant of a Vandermonde matrix, namely

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

Recall that the x_i's are all distinct, so no term $x_{i_j} - x_{i_k}$ in this product is equal to zero. The product is computed in $\mathbb{Z}_p$, where p is prime, which is a field. Since the product of non-zero terms in a field is always non-zero, we have that $\det A \neq 0$. Since the determinant of the coefficient matrix is non-zero, the system has a unique solution over the field $\mathbb{Z}_p$. This establishes that any group of t participants will be able to recover the key in this threshold scheme.

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 hypothesize a value y_0 for the key. Since the key 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_0 of the key, there is a unique polynomial $a_{y_0}(x)$ such that

$$y_{i_j} = a_{y_0}(x_{i_j}),$$

$1 \le j \le t-1$, and such that

$$y_0 = a_{y_0}(0).$$

Hence, no value of the key can be ruled out, and thus a group of $t-1$ participants can obtain no information about the key.

We have analyzed the Shamir scheme from the point of view of solving systems of linear equations over $\mathbb{Z}_p$. 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:

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

It is easy to verify the correctness of this formula by substituting $x = x_{i_j}$: all terms in the summation vanish except for the jth term, which is y_{i_j}. Thus, we have a polynomial of degree at most $t - 1$ which contains the t ordered pairs (x_{i_j}, y_{i_j}), $1 \le j \le t$. We already proved above that this polynomial is unique, so the interpolation formula does yield the correct polynomial.

A group B of t participants can compute $a(x)$ by using the interpolation formula. But a simplification is possible, since the participants in B do not need to know the whole polynomial $a(x)$. It is sufficient for them to compute the constant term $K = a(0)$. Hence, they can compute the following expression, which is obtained by substituting $x = 0$ into the Lagrange interpolation formula:

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

Suppose we define

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

$1 \le j \le t$. (Note that these values b_j can be precomputed, if desired, and their values are not secret.) Then we have

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

Hence, the key is a linear combination of the t shares.

To illustrate this approach, let's recompute the key from Example 11.1.

Example 11.1 (Cont.)
The participants $\{P_1, P_3, P_5\}$ can compute b_1, b_2, and b_3 according to the formula given above. For example, they would obtain

$$\begin{aligned} b_1 &= \frac{x_3 x_5}{(x_1 - x_3)(x_1 - x_5)} \bmod 17 \\ &= 3 \times 5 \times (-2)^{-1} \times (-4)^{-1} \bmod 17 \\ &= 4. \end{aligned}$$

Similarly, $b_2 = 3$ and $b_3 = 11$. Then, given shares 8, 10, and 11 (respectively), they would obtain

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

FIGURE 11.2
A (t, t)-threshold scheme in $\mathbb{Z}_m$

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

as before. □

The last topic of this section is a simplified construction for threshold schemes in the special case $w = t$. This construction will work for any key set $\mathcal{K} = \mathbb{Z}_m$ with $\mathcal{S} = \mathbb{Z}_m$. (For this scheme, it is not required that m be prime, and it is not necessary that $m \geq w + 1$.) If D wants to share the key $K \in \mathbb{Z}_m$, he carries out the protocol of Figure 11.2.

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 do so, 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

$$K - \sum_{i=1}^{t-1} y_i.$$

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.

11.2 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 key. A more general situation is to specify exactly which subsets of participants should be able to determine the key and which should not. Let Γ be a set of subsets of $\mathcal{P}$; the subsets in Γ are those subsets of participants that should be able to compute the key. 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 key $K \in \mathcal{K}$, 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.

DEFINITION 11.2 *A **perfect secret sharing scheme realizing** the access structure Γ is a method of sharing a key K among a set of w participants (denoted by $\mathcal{P}$), in such a way that 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.*

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

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

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.

We study the unconditional security of secret sharing scheme schemes. That is, we do not place any limit on the amount of computation that can be performed by an unauthorized subset of participants.

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:

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

In the remainder of this chapter, we will assume that all access structures are monotone.

If Γ is an access structure, then $B \in \Gamma$ is a *minimal* authorized subset if $A \notin \Gamma$ 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

$$\Gamma = cl(\Gamma_0).$$

Example 11.2
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

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

Conversely, given this access structure Γ, it is easy to see that Γ_0 consists of the minimal subsets in Γ. □

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

11.3 The Monotone Circuit Construction

In this section, we will give a conceptually simple and elegant construction due to Benaloh and Leichter that shows that any (monotone) access structure can be realized by a perfect secret sharing scheme. 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 **C**, with w boolean inputs, $x_1, \ldots, x_w$ (corresponding to the w participants $P_1, \ldots, P_w$), 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 $\mathbf{C}$ is a monotone circuit, and define

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

where $\mathbf{C}(x_1, \ldots, x_w)$ denotes the output of $\mathbf{C}$, given inputs $x_1, \ldots, x_w$. Since the circuit $\mathbf{C}$ is monotone, it follows that $\Gamma(\mathbf{C})$ 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") and $\vee$ ("or"), but do not contain any negations.

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

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

In Example 11.2, 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

$$(P_1 \wedge P_2 \wedge P_4) \vee (P_1 \wedge P_3 \wedge P_4) \vee (P_2 \wedge P_3). \tag{11.1}$$

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 $\mathbf{C}$ is any monotone circuit that recognizes Γ (note that $\mathbf{C}$ need not be the circuit described above.) We describe an algorithm which enables D, the dealer, to construct a perfect secret sharing scheme that realizes Γ. This scheme will use as a building block the (t, t)-schemes constructed in Figure 11.2. Hence, we take the key set to be $\mathcal{K} = \mathbb{Z}_m$ for some integer m.

The algorithm proceeds by assigning a value $f(W) \in \mathcal{K}$ to every wire W in the circuit $\mathbf{C}$. Initially, the output wire W_{out} of the circuit is assigned the value K, the key. 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.

A description of the construction is given in Figure 11.3. Note that, whenever a gate G is an "and" gate having (say) t input wires, we share the "key" $f(W_G)$ among the input wires using a (t, t)-threshold scheme.

Let's carry out this procedure for the access structure of Example 11.2, using the circuit corresponding to the boolean formula (11.1).

FIGURE 11.3
The monotone circuit construction

1. $f(W_{out}) = K$
2. **while** there exists a wire W such that $f(W)$ is not defined **do**
3. find a gate G of **C** such that $f(W_G)$ is defined, where W_G is the output wire of G, but $f(W)$ is not defined for any of the input wires of G
4. **if** G is an "or" gate **then**
5. $f(W) = f(W_G)$ for every input wire W of G
6. **else** (G is an "and" gate)
7. let the input wires of G be $W_1, \ldots, W_t$
8. choose (independently at random) $t - 1$ elements of $\mathbb{Z}_m$, denoted by $y_{G,1}, \ldots, y_{G,t-1}$
9. compute

$$y_{G,t} = f(W_G) - \sum_{i=1}^{t-1} y_{G,i} \bmod m$$

10. **for** $1 \leq i \leq t$ **do**
11. $f(W_i) = y_{G,i}$

Example 11.3
We illustrate the construction in Figure 11.4. Suppose K is the key. 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 $\mathbb{Z}_m$. 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 independent random values in $\mathbb{Z}_m$. If we look at the shares that the four participants receive, we have the following:

1. P_1 receives a_1, b_1.
2. P_2 receives a_2, c_1.
3. P_3 receives $b_2, K - c_1$.
4. P_4 receives $K - a_1 - a_2, K - b_1 - b_2$.

Thus, every participant receives two elements of $\mathbb{Z}_m$ as his or her share.

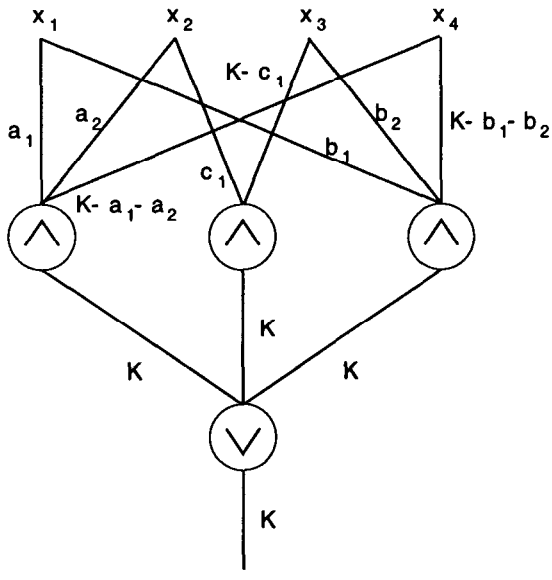

FIGURE 11.4
A monotone circuit

Let's prove that the scheme is perfect. First, we verify that each basis subset can compute K. The authorized subset $\{P_1, P_2, P_4\}$ can compute

$$K = a_1 + a_2 + (K - a_1 - a_2) \bmod m.$$

The subset $\{P_1, P_3, P_4\}$ can compute

$$K = b_1 + b_2 + (K - b_1 - b_2) \bmod m.$$

Finally, the subset $\{P_2, P_3\}$ can compute

$$K = c_1 + (K - c_1) \bmod m.$$

Thus any authorized subset can compute K, so we turn our attention to the unauthorized subsets. Note that we do not need to look at all the unauthorized subsets. For, if B_1 and B_2 are both unauthorized subsets, $B_1 \subseteq B_2$, and B_2 cannot compute K, then neither can B_1 compute K. Define a subset $B \subseteq \mathcal{P}$ to be a *maximal* unauthorized subset if $B_1 \in \Gamma$ for all $B_1 \supseteq B$, $B_1 \neq B$. It follows that it suffices to verify that none of the maximal unauthorized subsets can determine

any information about K. Here, the maximal unauthorized subsets are

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

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. As another example, 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. In each possible case, an unauthorized subset has no information about the value of K. □

We can obtain a different scheme realizing the same access structure by using a different circuit. We illustrate by returning again to the access structure of Example 11.2.

Example 11.4
Suppose we convert the formula (11.1) to the so-called conjunctive normal form:

$$(P_1 \vee P_2) \wedge (P_1 \vee P_3) \wedge (P_2 \vee P_3) \wedge (P_2 \vee P_4) \wedge (P_3 \vee P_4). \qquad (11.2)$$

(The reader can verify that this formula is equivalent to the formula (11.1).) If we implement the scheme using the circuit corresponding to formula (11.2), then we obtain the following:

1. P_1 receives a_1, a_2.
2. P_2 receives a_1, a_3, a_4.
3. P_3 receives $a_2, a_3, K - a_1 - a_2 - a_3 - a_4$.
4. P_4 receives $a_4, K - a_1 - a_2 - a_3 - a_4$.

We leave the details for the reader to check. □

We now prove that the monotone circuit construction always produces a perfect secret sharing scheme.

THEOREM 11.1
Let **C** *be any monotone boolean circuit. Then the monotone circuit construction yields a perfect secret sharing scheme realizing the access structure* $\Gamma(\mathbf{C})$.

PROOF We 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 key. This scheme realizes the access structure consisting of all non-empty subsets of participants. If **C** consists of a

single "and" gate with t inputs, then the scheme is the (t, t)-threshold scheme presented in Figure 11.2.

Now, as an induction assumption, suppose that there is an integer $j > 1$ such that, for all circuits $\mathbf{C}$ with fewer than j gates, the construction produces a scheme that realizes $\Gamma(\mathbf{C})$. Let $\mathbf{C}$ 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 outputs of t sub-circuits of $\mathbf{C}$, which we denote $\mathbf{C}_i$, $1 \leq i \leq t$. Corresponding to each $\mathbf{C}_i$, we have a (sub-)scheme that realizes the access structure $\Gamma_{\mathbf{C}_i}$, by induction. Now, it is easy to see that

$$\Gamma(\mathbf{C}) = \bigcup_{i=1}^{t} \Gamma_{\mathbf{C}_i}.$$

Since every W_i is assigned the key K, it follows that the scheme realizes $\Gamma(\mathbf{C})$, as desired.

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

$$\Gamma(\mathbf{C}) = \bigcap_{i=1}^{t} \Gamma_{\mathbf{C}_i}.$$

Since the key K is shared among the t wires W_i using a (t, t)-threshold scheme, it follows again that the scheme realizes $\Gamma(\mathbf{C})$. This completes the proof. ∎

Of course, when an authorized subset, B, wants to compute the key, 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 key involves combining shares according to the circuit, with the stipulation that an "and" gate corresponds to summing the values on the input wires modulo 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).

11.4 Formal Definitions

In this section, we will give formal mathematical definitions of a (perfect) secret sharing scheme. We represent a secret sharing scheme by a set of distribution rules. A *distribution rule* is a function

$$f : \mathcal{P} \rightarrow \mathcal{S}.$$

A distribution rule represents a possible distribution of shares to the participants, where $f(P_i)$ is the share given to P_i, $1 \leq i \leq w$.

Now, for each $K \in \mathcal{K}$, let $\mathcal{F}_K$ be a set of distribution rules. $\mathcal{F}_K$ will be distribution rules corresponding to the key having the value K. The sets of distribution rules $\mathcal{F}_K$ are public knowledge.

Next, define

$$\mathcal{F} = \bigcup_{K \in \mathcal{K}} \mathcal{F}_K.$$

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

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.

It is useful to develop conditions which ensure that a set of distribution rules for a scheme realizes a specified access structure. This will involve looking at certain probability distributions, as we did previously when studying the concept of perfect secrecy. To begin with, we suppose that there is a probability distribution $p_{\mathcal{K}}$ on $\mathcal{K}$. Further, for every $K \in \mathcal{K}$, D will choose a distribution rule in $\mathcal{F}_K$ according to a probability distribution $p_{\mathcal{F}_K}$.

Given these probability distributions, it is straightforward to compute the probability distribution on the list of shares given to any subset of participants, B (authorized or unauthorized). This is done as follows. Suppose $B \subseteq \mathcal{P}$. Define

$$\mathcal{S}(B) = \{f|_B : f \in \mathcal{F}\},$$

where the function $f|_B$ denotes the restriction of the distribution rule f to B. That is, $f|_B : B \rightarrow \mathcal{S}$ is defined by

$$f|_B(P_i) = f(P_i)$$

for all $P_i \in B$. Thus, $\mathcal{S}(B)$ is the set of possible distributions of shares to the participants in B.

The probability distribution on $\mathcal{S}(B)$, denoted $p_{\mathcal{S}(B)}$, is computed as follows: Let $f_B \in \mathcal{S}(B)$. Then

$$p_{\mathcal{S}(B)}(f_B) = \sum_{K \in \mathcal{K}} p_{\mathcal{K}}(K) \sum_{\{f \in \mathcal{F}_K : f|_B = f_B\}} p_{\mathcal{F}_K}(f).$$

Also,

$$p_{\mathcal{S}(B)}(f_B|K) = \sum_{\{f \in \mathcal{F}_K : f|_B = f_B\}} p_{\mathcal{F}_K}(f),$$

for all $f_B \in \mathcal{S}(B)$ and $K \in \mathcal{K}$.

Here now is a formal definition of a perfect secret sharing scheme.

DEFINITION 11.3 *Suppose Γ is an access structure and $\mathcal{F} = \cup_{K \in \mathcal{K}} \mathcal{F}_K$ is a set of distribution rules. Then $\mathcal{F}$ is a* ***perfect secret sharing scheme*** *realizing the access structure Γ provided that the following two properties are satisfied:*

1. *For any authorized subset of participants $B \subseteq \mathcal{P}$, there do not exist two distribution rules $f \in \mathcal{F}_K$ and $f' \in \mathcal{F}_{K'}$ with $K \neq K'$, such that $f|_B = f'|_B$. (That is, any distribution of shares to the participants in an authorized subset B determines the value of the key.)*
2. *For any unauthorized subset of participants $B \subseteq \mathcal{P}$ and for any distribution of shares $f_B \in \mathcal{S}_B$, $p_{\mathcal{K}}(K|f_B) = p_{\mathcal{K}}(K)$ for every $K \in \mathcal{K}$. (That is, the conditional probability distribution on $\mathcal{K}$, given a distribution of shares f_B to an unauthorized subset B, is the same as the a priori probability distribution on $\mathcal{K}$. In other words, the distribution of shares to B provides no information as to the value of the key.)*

Observe that the second property in Definition 11.3 is very similar to the concept of perfect secrecy; this similarity is why the resulting secret sharing scheme is termed "perfect."

Note that the probability $p_{\mathcal{K}}(K|f_B)$ can be computed from probability distributions exhibited above using Bayes' theorem:

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

Let us now illustrate these definitions by looking at a small example.

Example 11.5

We will present the distribution rules for the scheme constructed in Example 11.4 when it is implemented in $\mathbb{Z}_2$. Each of $\mathcal{F}_0$ and $\mathcal{F}_1$ contains 16 equiprobable distribution rules. For conciseness, we replace a binary k-tuple by an integer between 0 and $2^k - 1$. If this is done, then $\mathcal{F}_0$ and $\mathcal{F}_1$ are as depicted in Figure 11.5, where each row represents a distribution rule.

This yields a perfect scheme for any probability distribution $p_{\mathcal{K}}$ on the keys. We will not perform all the verifications here, but we will look at a couple of typcial cases to illustrate the use of the two properties in Definition 11.3.

The subset $\{P_2, P_3\}$ is an authorized subset. Thus the shares that P_2 and P_3 receive should (together) determine a unique key. It can easily be checked that any distribution of shares to these two participants occurs in a distribution rule in at most one of the sets $\mathcal{F}_0$ and $\mathcal{F}_1$. For example, if P_2 has the share 3 and P_3 has the share 6, then the distribution rule must be the eighth rule in $\mathcal{F}_0$ and thus the key is 0.

$\mathcal{F}_0$

P_1	P_2	P_3	P_4
0	0	0	0
0	1	1	3
0	2	3	1
0	3	2	2
1	0	4	0
1	1	5	3
1	2	7	1
1	3	6	2
2	4	0	0
2	5	1	3
2	6	3	1
2	7	2	2
3	4	4	0
3	5	5	3
3	6	7	1
3	7	6	2

$\mathcal{F}_1$

P_1	P_2	P_3	P_4
0	0	1	1
0	1	0	2
0	2	2	0
0	3	3	3
1	0	5	1
1	1	4	2
1	2	6	0
1	3	7	3
2	4	1	1
2	5	0	0
2	6	2	2
2	7	3	3
3	4	5	1
3	5	4	2
3	6	6	0
3	7	7	3

FIGURE 11.5
Distribution rules for a secret sharing scheme

On the other hand, $B = \{P_1, P_2\}$ is an unauthorized subset. It is not too hard to see that any distribution of shares to these two participants occurs in exactly one distribution rule in $\mathcal{F}_0$ and in exactly one distribution rule in $\mathcal{F}_1$. That is,

$$p_{\mathcal{S}(B)}(f_B|K) = \frac{1}{16}$$

for any $f_B \in \mathcal{S}(B)$ and for $K = 0, 1$. Next, we compute

$$\begin{aligned} p_{\mathcal{S}(B)}(f_B) &= \sum_{K \in \mathcal{K}} p_{\mathcal{K}}(K) \sum_{\{f \in \mathcal{F}_K : f|_B = f_B\}} p_{\mathcal{F}_K}(f) \\ &= \sum_{K=0}^{1} p_{\mathcal{K}}(K) \times \frac{1}{16} \\ &= \frac{1}{16}. \end{aligned}$$

Now, we use Bayes' theorem to compute $p_{\mathcal{K}}(K|f_B)$:

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

$$= \frac{\frac{1}{16} \times p_{\mathcal{K}}(K)}{\frac{1}{16}}$$
$$= p_{\mathcal{K}}(K),$$

so the second property is satisfied for this subset B.

Similar computations can be performed for other authorized and unauthorized sets, and in each case the appropriate property is satisfied. Hence we have a perfect secret sharing scheme. □

11.5 Information Rate

The results of Section 11.3 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 $1 + \binom{w}{t}$ gates. Each participant will receive $\binom{w-1}{t-1}$ elements of $\mathbb{Z}_m$ as his or her share. This seems very inefficient, since a Shamir (t, w)-threshold scheme enables a key 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, which we define now.

DEFINITION 11.4 *Suppose we have a perfect secret sharing scheme realizing an access structure Γ. The **information rate** for P_i is the ratio*

$$\rho_i = \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}(P_i)|}.$$

*(Note that $\mathcal{S}(P_i)$ denotes the set of possible shares that P_i might receive; of course $\mathcal{S}(P_i) \subseteq \mathcal{S}$.) The **information rate** of the scheme is denoted by ρ and is defined as*

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

The motivation for this definition is as follows. Since the 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 $\log_2 |\mathcal{S}(P_i)|$. Intuitively, P_i receives $\log_2 |\mathcal{S}(P_i)|$ bits of information (in his or her share), but the information content of the key is $\log_2 |\mathcal{K}|$ bits. Thus ρ_i is the ratio of the number of bits in a share to the number of bits in the key.

Example 11.6
Let's look at the two schemes from Section 11.2. The scheme produced in Example 11.3 has

$$\rho = \frac{\log_2 m}{\log_2 m^2} = \frac{1}{2}.$$

However, in Example 11.4, we get a scheme with

$$\rho = \frac{\log_2 m}{\log_2 m^3} = \frac{1}{3}.$$

Hence, the first implementation is preferable. □

In general, if we construct a scheme from a circuit **C** using the monotone circuit construction, then the information rate can be computed as indicated in the following theorem.

THEOREM 11.2
Let **C** *be any monotone boolean circuit. Then there is a perfect secret sharing scheme realizing the access structure* $\Gamma(\mathbf{C})$ *having information rate*

$$\rho = \max\{1/r_i : 1 \leq i \leq w\},$$

where r_i *denotes the number of input wires to* **C** *carrying the input* x_i.

With respect to threshold access structures, we observe that the Shamir scheme will have information rate 1, which we show below is the optimal value. In contrast, an implementation of a (t, w)-threshold scheme using a disjunctive normal form boolean circuit will have information rate $1/\binom{w-1}{t-1}$, which is much lower (and therefore inferior) if $1 < t < w$.

Obviously, a high information rate is desirable. The first general result we prove is that $\rho \leq 1$ in any scheme.

THEOREM 11.3
In any perfect secret sharing scheme realizing an access structure Γ, $\rho \leq 1$.

PROOF Suppose we have a a perfect secret sharing scheme that realizes the access structure Γ. Let $B \in \Gamma_0$ and choose any participant $P_j \in B$. Define $B' = B \backslash \{P_j\}$. Let $g \in \mathcal{S}(B)$. Now, $B' \notin \Gamma$, so the distribution of shares $g|_{B'}$ provides no information about the key. Hence, for each $K \in \mathcal{K}$, there is a distribution rule $g^K \in \mathcal{F}_K$ such that $g^K|_{B'} = g|_{B'}$. Since $B \in \Gamma$, it must be the case that $g^K(P_j) \neq g^{K'}(P_j)$ if $K \neq K'$. Hence, $|\mathcal{S}(P_j)| \geq |\mathcal{K}|$, and thus $\rho \leq 1$. ∎

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

11.6 The Brickell Vector Space Construction

In this section, we present a construction for certain ideal schemes known as the *Brickell vector space construction.*

Suppose Γ is an access structure, and let $(\mathbb{Z}_p)^d$ denote the vector space of all d-tuples over $\mathbb{Z}_p$, where p is prime and $d \geq 2$. Suppose there exists a function

$$\phi : \mathcal{P} \rightarrow (\mathbb{Z}_p)^d$$

which satisfies the property

$$(1, 0, \ldots, 0) \in \langle \phi(P_i) : P_i \in B \rangle \Leftrightarrow B \in \Gamma. \tag{11.3}$$

In other words, the vector $(1, 0, \ldots, 0)$ 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 Property (11.3). (In general, finding such a function is often a matter of trial and error, though we will see some explicit constructions of suitable functions ϕ for certain access structures a bit later.) We are going to construct an ideal secret sharing scheme with $\mathcal{K} = \mathcal{S}(P_i) = \mathbb{Z}_p$, $1 \leq i \leq w$. The distribution rules of the scheme are as follows: for every vector $\overline{a} = (a_1, \ldots, a_d) \in {\mathbb{Z}_p}^d$, define a distribution rule $f_{\overline{a}} \in \mathcal{F}_{a_1}$, where

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

for every $x \in \mathcal{P}$, and the operation "$\cdot$" is the inner product modulo p.

Note that each $\mathcal{F}_K$ contains p^{d-1} distribution rules. We will suppose that each probability distribution $p_{\mathcal{F}_K}$ is equiprobable: $p_{\mathcal{F}_K}(f) = 1/p^{d-1}$ for every $f \in \mathcal{F}_K$. The Brickell scheme is presented in Figure 11.6.

We have the following result.

THEOREM 11.4

Suppose ϕ satisfies Property (11.3). Then the sets of distribution rules $\mathcal{F}_K$, $K \in \mathcal{K}$, comprise 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

$$(1, 0, \ldots, 0) \in \langle \phi(P_i) : P_i \in B \rangle,$$

FIGURE 11.6
The Brickell scheme

Initialization Phase

1. For $1 \leq i \leq w$, D gives the vector $\phi(P_i) \in (\mathbb{Z}_p)^d$ to P_i. These vectors are public.

Share Distribution

2. Suppose D wants to share a key $K \in \mathbb{Z}_p$. D secretly chooses (independently at random) $d-1$ elements of $\mathbb{Z}_p$, $a_2, \ldots, a_d$.
3. For $1 \leq i \leq w$, D computes $y_i = \overline{a} \cdot \phi(P_i)$, where
$$\overline{a} = (K, a_2, \ldots, a_d).$$
4. For $1 \leq i \leq w$, D gives the share y_i to P_i.

we can write

$$(1, 0, \ldots, 0) = \sum_{\{i:P_i \in B\}} c_i \phi(P_i),$$

where each $c_i \in \mathbb{Z}_p$. Denote by s_i the share given to P_i. Then

$$s_i = \overline{a} \cdot \phi(P_i),$$

where $\overline{a}$ is an unknown vector chosen by D and

$$K = a_1 = \overline{a} \cdot (1, 0, \ldots, 0).$$

By the linearity of the inner product operation,

$$K = \sum_{\{i:P_i \in B\}} c_i \overline{a} \cdot \phi(P_i).$$

Thus, it is a simple matter for the participants in B to compute

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

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

$$\phi(P_i) \cdot \overline{a} = s_i, \forall P_i \in B$$
$$(1, 0, \ldots, 0) \cdot \overline{a} = K.$$

This is a system of linear equations in the d unknowns $a_1, \ldots, a_d$. The coefficient matrix has rank $e + 1$, since

$$(1, 0, \ldots, 0) \notin \langle \phi(P_i) : P_i \in B \rangle.$$

Provided the system of equations is consistent, the solution space has dimension $d - e - 1$ (independent of the value of K). It will then follow that there are precisely p^{d-e-1} distribution rules in each $\mathcal{F}_K$ that are consistent with any possible distribution of shares to B. By a similar computation as was performed in Example 11.5, we see that $p_{\mathcal{K}}(K|f_B) = p_{\mathcal{K}}(K)$ for every $K \in \mathcal{K}$, where $f_B(P_i) = s_i$ for all $P_i \in B$.

Why is the system consistent? The first $|B|$ equations are consistent, since the vector $\overline{a}$ chosen by D is a solution. Since

$$(1, 0, \ldots, 0) \notin \langle \phi(P_i) : P_i \in B \rangle$$

(as mentioned above), the last equation is consistent with the first $|B|$ equations. This completes the proof. ∎

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

Here is another general result that is easy to prove. It concerns access structures that have as a basis a collection of pairs of participants that forms a complete multipartite graph. A graph $G = (V, E)$ with vertex set V and edge set E 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 11.5

Suppose $G = (V, E)$ is a complete multipartite graph. Then there is an ideal scheme realizing the access structure $cl(E)$ on participant set V.

PROOF Let $V_1, \ldots, V_\ell$ be the parts of G. Let $x_1, \ldots, x_\ell$ be distinct elements of $\mathbb{Z}_p$, where $p \geq \ell$. Let $d = 2$. For every participant $v \in V_i$, define $\phi(v) = (x_i, 1)$. It is straightforward to verify Property (11.3). By Theorem 11.4, we have an ideal scheme. ∎

TABLE 11.1
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	
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	
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	
12.	4	$P_1P_3P_4, P_1P_2, P_2P_3$	2/3	
13.	4	$P_1P_3P_4, P_1P_2, P_2P_3, P_2P_4$	2/3	
14.	4	$P_1P_2P_3, P_1P_2P_4$	1	
15.	4	$P_1P_2P_3, P_1P_2P_4, P_3P_4$	1	
16.	4	$P_1P_2P_3, P_1P_2P_4, P_1P_3P_4$	1	
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

To illustrate the 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 non-empty subsets on disjoint participant sets. (For example, $\Gamma_0 = \{\{P_1, P_2\}, \{P_3, P_4\}\}$ can be partitioned as $\{\{P_1, P_2\}\} \cup \{\{P_3, P_4\}\}$ so we do not consider it.) We list the non-isomorphic access structures of this type on two, three, and four participants in Table 11.1 (the quantities ρ^* are defined in Section 11.7).

Of these 18 access structures, we can already obtain ideal schemes for ten of them using the constructions we have at our disposal now. These ten access structures are either threshold access structures or have a basis which is a complete multipartite graph, so Theorem 11.5 can be applied. One such access structure is # 9, whose basis is the complete multipartite graph $K_{1,1,2}$. We illustrate in the following example.

Example 11.7
For access structure # 9, take $d = 2$, $p \geq 3$, and define ϕ as follows:

$$\phi(P_1) = (0, 1)$$
$$\phi(P_2) = (0, 1)$$
$$\phi(P_3) = (1, 1)$$

$$\phi(P_4) = (1, 2).$$

Applying Theorem 11.5, an ideal scheme results. □

Eight access structures remain to be considered. It is possible to use *ad hoc* applications of the vector space construction to construct ideal schemes for four of these: # 11, # 14, # 15 and # 16. We present the constructions for # 11 and # 14 here.

Example 11.8
For access structure # 11, take $d = 3$, $p \geq 3$, and define ϕ as follows:

$$\phi(P_1) = (0, 1, 0)$$
$$\phi(P_2) = (1, 0, 1)$$
$$\phi(P_3) = (0, 1, -1)$$
$$\phi(P_4) = (1, 1, 0).$$

First, we have

$$\begin{aligned}\phi(P_4) - \phi(P_1) &= (1, 1, 0) - (0, 1, 0)\\ &= (1, 0, 0).\end{aligned}$$

Also,

$$\begin{aligned}\phi(P_2) + \phi(P_3) - \phi(P_1) &= (1, 0, 1) + (0, 1, -1) - (0, 1, 0)\\ &= (1, 0, 0).\end{aligned}$$

Hence,

$$(1, 0, 0) \in \langle \phi(P_1), \phi(P_2), \phi(P_3) \rangle$$

and

$$(1, 0, 0) \in \langle \phi(P_1), \phi(P_4) \rangle.$$

Now, it suffices to show that

$$(1, 0, 0) \notin \langle \phi(P_i) : P_i \in B \rangle$$

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 $\{P_2, P_3, P_4\}$. In each case, we need to establish that a system of linear equations has no solution. For example, suppose that

$$(1, 0, 0) = a_2\phi(P_2) + a_3\phi(P_3) + a_4\phi(P_4),$$

where $a_2, a_3, a_4 \in \mathbb{Z}_p$. 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 other two subsets B for the reader to consider. □

Example 11.9
For access structure # 14, take $d = 3, p \geq 2$ and define ϕ as follows:

$$\phi(P_1) = (0, 1, 0)$$
$$\phi(P_2) = (1, 0, 1)$$
$$\phi(P_3) = (0, 1, 1)$$
$$\phi(P_4) = (0, 1, 1).$$

Again, Property (11.3) is satisfied and hence an ideal scheme results. □

Constructions of ideal schemes for the access structures # 15 and # 16 are left as exercises. In the next section, we will show that the remaining four access structures cannot be realized by ideal schemes.

11.7 An Upper Bound on the Information Rate

Four access structures remain to be considered: # 5, # 8, # 12, and # 13. We will see in this section that in each case, there does not exist a scheme having information rate $\rho > 2/3$.

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 present is an entropy bound that will lead to an upper bound on ρ^* for certain access structures. We have defined a probability distribution $p_{\mathcal{K}}$ on $\mathcal{K}$; the entropy of this probability distribution is denoted $H(\mathbf{K})$. We have also denoted by $p_{\mathcal{S}(B)}$ the probability distribution on the shares given to a subset $B \subseteq \mathcal{P}$. We will denote the entropy of this probability distribution by $H(\mathbf{B})$.

We begin by giving yet another definition of perfect secret sharing schemes, this time using the language of entropy. This definition is equivalent to Definition 11.3.

DEFINITION 11.5 *Suppose Γ is an access structure and $\mathcal{F}$ is a set of distribution rules. Then $\mathcal{F}$ is a* ***perfect secret sharing scheme*** *realizing the access structure Γ provided that the following two properties are satisfied:*

1. *For any authorized subset of participants $B \subseteq \mathcal{P}$, $H(\mathbf{K}|\mathbf{B}) = 0$.*
2. *For any unauthorized subset of participants $B \subseteq \mathcal{P}$, $H(\mathbf{K}|\mathbf{B}) = H(\mathbf{K})$.*

We will require several entropy identities and inequalities. Some of these results were given in Section 2.3 and the rest are proved similarly, so we state them without proof in the following Lemma.

LEMMA 11.6
Let $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ be random variables. Then the following hold:

$$H(\mathbf{XY}) = H(\mathbf{X}|\mathbf{Y}) + H(\mathbf{Y}) \tag{11.4}$$

$$H(\mathbf{XY}|\mathbf{Z}) = H(\mathbf{X}|\mathbf{YZ}) + H(\mathbf{Y}|\mathbf{Z}) \tag{11.5}$$

$$H(\mathbf{XY}|\mathbf{Z}) = H(\mathbf{Y}|\mathbf{XZ}) + H(\mathbf{X}|\mathbf{Z}) \tag{11.6}$$

$$H(\mathbf{X}|\mathbf{Y}) \geq 0 \tag{11.7}$$

$$H(\mathbf{X}|\mathbf{Z}) \geq H(\mathbf{X}|\mathbf{YZ}) \tag{11.8}$$

$$H(\mathbf{XY}|\mathbf{Z}) \geq H(\mathbf{Y}|\mathbf{Z}) \tag{11.9}$$

We next prove two preliminary entropy lemmas for secret sharing schemes.

LEMMA 11.7
Suppose Γ is an access structure and $\mathcal{F}$ is a set of distribution rules realizing Γ. Suppose $B \notin \Gamma$ and $A \cup B \in \Gamma$, where $A, B \subseteq \mathcal{P}$. Then

$$H(\mathbf{A}|\mathbf{B}) = H(\mathbf{K}) + H(\mathbf{A}|\mathbf{BK}).$$

PROOF From Equations 11.5 and 11.6, we have that

$$H(\mathbf{AK}|\mathbf{B}) = H(\mathbf{A}|\mathbf{BK}) + H(\mathbf{K}|\mathbf{B})$$

and

$$H(\mathbf{AK}|\mathbf{B}) = H(\mathbf{K}|\mathbf{AB}) + H(\mathbf{A}|\mathbf{B}),$$

so

$$H(\mathbf{A}|\mathbf{BK}) + H(\mathbf{K}|\mathbf{B}) = H(\mathbf{K}|\mathbf{AB}) + H(\mathbf{A}|\mathbf{B}).$$

Since, by Property 2 of Definition 11.5, we have

$$H(\mathbf{K}|\mathbf{B}) = H(\mathbf{K}),$$

and, by Property 1 of Definition 11.5, we have

$$H(\mathbf{K}|\mathbf{AB}) = 0,$$

the result follows. ∎

LEMMA 11.8

Suppose Γ *is an access structure and* $\mathcal{F}$ *is a set of distribution rules realizing* Γ. *Suppose* $A \cup B \notin \Gamma$, *where* $A, B \subseteq \mathcal{P}$. *Then* $H(\mathbf{A}|\mathbf{B}) = H(\mathbf{A}|\mathbf{BK})$.

PROOF As in Lemma 11.7, we have that

$$H(\mathbf{A}|\mathbf{BK}) + H(\mathbf{K}|\mathbf{B}) = H(\mathbf{K}|\mathbf{AB}) + H(\mathbf{A}|\mathbf{B}).$$

Since

$$H(\mathbf{K}|\mathbf{B}) = H(\mathbf{K})$$

and

$$H(\mathbf{K}|\mathbf{AB}) = H(\mathbf{K}),$$

the result follows. ∎

We now prove the following important theorem.

THEOREM 11.9

Suppose Γ *is an access structure such that*

$$\{W, X\}, \{X, Y\}, \{W, Y, Z\} \in \Gamma$$

and

$$\{W, Y\}, \{X\}, \{W, Z\} \notin \Gamma.$$

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

PROOF We establish a sequence of inequalities:

$$\begin{aligned}
H(\mathbf{K}) &= H(\mathbf{Y}|\mathbf{WZ}) - H(\mathbf{Y}|\mathbf{WZK}) && \text{by Lemma 11.7}\\
&\leq H(\mathbf{Y}|\mathbf{WZ}) && \text{by (11.7)}\\
&\leq H(\mathbf{Y}|\mathbf{W}) && \text{by (11.8)}\\
&= H(\mathbf{Y}|\mathbf{WK}) && \text{by Lemma 11.8}\\
&\leq H(\mathbf{XY}|\mathbf{WK}) && \text{by (11.9)}\\
&= H(\mathbf{X}|\mathbf{WK}) + H(\mathbf{Y}|\mathbf{WXK}) && \text{by (11.5)}\\
&\leq H(\mathbf{X}|\mathbf{WK}) + H(\mathbf{Y}|\mathbf{XK}) && \text{by (11.8)}\\
&= H(\mathbf{X}|\mathbf{W}) - H(\mathbf{K}) + H(\mathbf{Y}|\mathbf{X}) - H(\mathbf{K}) && \text{by Lemma 11.7}\\
&\leq H(\mathbf{X}) - H(\mathbf{K}) + H(\mathbf{Y}|\mathbf{X}) - H(\mathbf{K}) && \text{by (11.7)}\\
&= H(\mathbf{XY}) - 2H(\mathbf{K}) && \text{by (11.4).}
\end{aligned}$$

Hence, the result follows. ∎

COROLLARY 11.10
Suppose that Γ is an access structure that satisfies the hypotheses of Theorem 11.9. Suppose the $|\mathcal{K}|$ keys are equally probable. Then $\rho \leq 2/3$.

PROOF Since the keys are equiprobable, we have

$$H(\mathbf{K}) = \log_2 |\mathcal{K}|.$$

Also, we have that

$$\begin{aligned}
H(\mathbf{XY}) &\leq H(\mathbf{X}) + H(\mathbf{Y})\\
&\leq \log_2 |\mathcal{S}(X)| + \log_2 |\mathcal{S}(Y)|.
\end{aligned}$$

By Theorem 11.9, we have that

$$H(\mathbf{XY}) \geq 3H(\mathbf{K}).$$

Hence it follows that

$$\log_2 |\mathcal{S}(X)| + \log_2 |\mathcal{S}(Y)| \geq 3 \log_2 |\mathcal{K}|.$$

Now, by the definition of information rate, we have

$$\rho \leq \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}(X)|}$$

and

$$\rho \leq \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}(Y)|}.$$

It follows that

$$\begin{aligned} 3\log_2|\mathcal{K}| &\leq \log_2|\mathcal{S}(X)| + \log_2|\mathcal{S}(Y)| \\ &\leq \frac{\log_2|\mathcal{K}|}{\rho} + \frac{\log_2|\mathcal{K}|}{\rho} \\ &= 2\frac{\log_2|\mathcal{K}|}{\rho}. \end{aligned}$$

Hence, $\rho \leq 2/3$. ∎

For the access structures # 5, # 8, # 12, and # 13, the hypotheses of Theorem 11.9 are satisfied. Hence, $\rho^* \leq 2/3$ for these four access structures.

We also have the following result concerning ρ^* in the case where the access structure has a basis Γ_0 which is a graph. The proof 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. If $G = (V, E)$ is a graph with vertex set V and edge set E, and $V_1 \subseteq V$, then the *induced subgraph* $G[V_1]$ is defined to be the graph (V_1, E_1), where

$$E_1 = \{uv \in E, u, v \in V_1\}.$$

THEOREM 11.11

Suppose G is a connected graph that is not a complete multipartite graph. Let $\Gamma(G)$ be the access structure that is the closure of E, where E is the edge set of G. Then $\rho^*(\Gamma(G)) \leq 2/3$.

PROOF We will first prove that any connected graph that is not a complete multipartite graph must contain four vertices w, x, y, z such that the induced subgraph $G[w, x, y, z]$ is isomorphic to either the basis of access structure # 5 or # 8.

Let G^C denote the complement of G. Since G is not a complete multipartite graph, there must exist three vertices x, y, z such that $xy, yz \in E(G^C)$ and $xz \in E(G)$. Define

$$d = \min\{d_G(y, x), d_G(y, z)\},$$

where d_G denotes the length of a shortest path (in G) between two vertices. Then $d \geq 2$. Without loss of generality, we can assume that $d = d_G(y, x)$ by symmetry. Let

$$y_0, y_1, \ldots, y_{d-1}, x$$

be a path in G, where $y_0 = y$. We have that

$$y_{d-2}z, y_{d-2}x \in E(G^C)$$

and

$$y_{d-2}y_{d-1}, y_{d-1}x, xz \in E(G).$$

It follows that $G[y_{d-2}, y_{d-1}, x, z]$ is isomorphic to the basis of access structure # 5 or # 8, as desired.

So, we can assume that we have found four vertices w, x, y, z such that the induced subgraph $G[w, x, y, z]$ is isomorphic to either the basis of access structure # 5 or # 8. Now, let $\mathcal{F}$ be any scheme realizing the access structure $\Gamma(G)$. If we restrict the domain of the distribution rules to $\{w, x, y, z\}$, then we obtain a scheme $\mathcal{F}'$ realizing access structure # 5 or # 8. It is also obvious that $\rho(\mathcal{F}') \geq \rho(\mathcal{F})$. Since $\rho(\mathcal{F}') \leq 2/3$, it follows that $\rho(\mathcal{F}) \leq 2/3$. This completes the proof. ∎

Since $\rho^* = 1$ for complete multipartite graphs, Theorem 11.11 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.

11.8 The Decomposition Construction

We still have four access structures in Table 11.1 to consider. Of course, we can use the monotone circuit construction to produce schemes for these access structures. 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 cases # 8 and # 13, a disjunctive normal form boolean circuit will yield $\rho = 1/3$, but other monotone circuits exist which allow us to attain $\rho = 1/2$. But in fact, it is possible to construct schemes with $\rho = 2/3$ for each of these four access structures, by employing constructions that use ideal schemes as building blocks in the construction of larger schemes.

We present a construction of this type called the "decomposition construction." First, we need to define an important concept.

DEFINITION 11.6 *Suppose Γ is an access structure having basis Γ_0. Let $\mathcal{K}$ be a specified key set. An **ideal $\mathcal{K}$-decomposition** of Γ_0 consists of a set $\{\Gamma_1, \ldots \Gamma_n\}$ such that the following 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.

Given an ideal $\mathcal{K}$-decomposition of an access structure Γ, we can easily construct a perfect secret sharing scheme, as described in the following theorem.

THEOREM 11.12
Suppose Γ *is an access structure having basis* Γ_0. *Let* $\mathcal{K}$ *be a specified key set, and suppose* $\{\Gamma_1, \ldots \Gamma_n\}$ *is an ideal* $\mathcal{K}$*-decomposition of* Γ. *For every participant* P_i, *define*

$$R_i = |\{k : P_i \in \mathcal{P}_k\}|.$$

Then there exists a perfect secret sharing scheme realizing Γ, *having information rate* $\rho = 1/R$, *where*

$$R = \max\{R_i : 1 \leq i \leq w\}.$$

PROOF For $1 \leq k \leq n$, we have an ideal scheme realizing the access structure with basis Γ_k, with key set $\mathcal{K}$, having $\mathcal{F}^k$ as its set of distribution rules. We will construct a scheme realizing Γ, with key set $\mathcal{K}$. The set of distribution rules $\mathcal{F}$ is constructed according to the following recipe. Suppose D wants to share a key K. Then, for $1 \leq k \leq n$, he chooses a random distribution rule $f^k \in \mathcal{F}^k_K$ and distributes the resulting shares to the participants in $\mathcal{P}_k$.

We omit the proof that the scheme is perfect. However, it is easy to compute the information rate of the resulting scheme. Since each of the component schemes is ideal, it follows that

$$|\mathcal{S}(P_i)| = |\mathcal{K}|^{R_i},$$

for $1 \leq i \leq w$. So

$$\rho_i = \frac{1}{R_i},$$

and

$$\rho = \frac{1}{\max\{R_i : 1 \leq i \leq w\}},$$

which is what we were required to prove. ∎

Although Theorem 11.12 is useful, it is often much more useful to employ a generalization in which we have ℓ ideal $\mathcal{K}$-decompositions of Γ_0 instead of just one. Each of the ℓ decompositions is used to share a key chosen from $\mathcal{K}$. Thus, we build a scheme with key set $\mathcal{K}^\ell$. The construction of the scheme and its information rate are as stated in the following theorem.

THEOREM 11.13 (Decomposition Construction)
Suppose Γ is an access structure having basis Γ_0, and $\ell \geq 1$ is an integer. Let $\mathcal{K}$ be a specified key set, and for $1 \leq j \leq \ell$, suppose that $\mathcal{D}_j = \{\Gamma_{j,1}, \ldots \Gamma_{j,n_j}\}$ is an ideal decomposition of Γ_0. Let $\mathcal{P}_{j,k}$ denote the participant set for the access structure $\Gamma_{j,k}$. For every participant P_i, define

$$R_i = \sum_{j=1}^{\ell} |\{k : P_i \in \mathcal{P}_{j,k}\}|.$$

Then there exists a perfect secret sharing scheme realizing Γ, having information rate $\rho = \ell/R$, where

$$R = \max\{R_i : 1 \leq i \leq w\}.$$

PROOF For $1 \leq j \leq \ell$ and $1 \leq k \leq n$, we have an ideal scheme realizing the access structure with basis $\Gamma_{j,k}$, with key set $\mathcal{K}$, having $\mathcal{F}^{j,k}$ as its set of distribution rules. We construct a scheme realizing Γ, 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 key $K = (K_1, \ldots, K_\ell)$. Then for $1 \leq j \leq \ell$ and $1 \leq k \leq n$, he chooses a random distribution rule $f^{j,k} \in \mathcal{F}^{j,k}_{K_j}$ and distributes the resulting shares to the participants in $\mathcal{P}_{j,k}$.

The information rate can be computed in a manner similar to that of Theorem 11.12. ∎

Let's look at a couple of examples.

Example 11.10
Consider access structure # 5. The basis is a graph that is not a complete multipartite graph. Therefore we know from Theorem 11.11 that $\rho^* \leq 2/3$.

Let p be prime, and consider the following two ideal $\mathbb{Z}_p$-decompositions:

$$\mathcal{D}_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\},$$

where

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

and

$$\mathcal{D}_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\},$$

where

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

Each decomposition consists of a K_2 and a $K_{1,2}$, so they are indeed ideal $\mathbb{Z}_p$-decompositions. Either of them yields a scheme with $\rho = 1/2$. However, if we "combine" them by applying Theorem 11.13 with $\ell = 2$, then we get a scheme with $\rho = 2/3$, which is optimal.

One implementation of the scheme, using Theorem 11.5, is as follows. D will choose four random elements (independently) from $\mathbb{Z}_p$, say b_{11}, b_{12}, b_{21}, and b_{22}. Given a key $(K_1, K_2) \in (\mathbb{Z}_p)^2$, D distributes shares as follows:

1. P_1 receives b_{11}, b_{21}.
2. P_2 receives $b_{11} + K_1, b_{12}, b_{21} + K_2$.
3. P_3 receives $b_{12} + K_1, b_{21}, b_{22}$.
4. P_4 receives $b_{12}, b_{22} + K_2$.

(All arithmetic is performed in $\mathbb{Z}_p$.) □

Example 11.11

Consider access structure # 8. Again, $\rho^* \leq 2/3$ by Theorem 11.11, and two suitable ideal compositions will yield an (optimal) scheme with $\rho = 2/3$.

Take $\mathcal{K} = \mathbb{Z}_p$ for any prime $p \geq 3$, and define two ideal $\mathcal{K}$-decompositions to be:

$$\mathcal{D}_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\},$$

where

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

and

$$\mathcal{D}_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\},$$

where

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

$\mathcal{D}_1$ consists of a K_2 and a K_3, and $\mathcal{D}_1$ consists of a K_2 and a $K_{1,3}$, so both are ideal $\mathcal{K}$-decompositions. Applying Theorem 11.13 with $\ell = 2$, we get a scheme with $\rho = 2/3$.

One implementation, using Theorem 11.5, is as follows. D will choose four random elements (independently) from $\mathbb{Z}_p$, say b_{11}, b_{12}, b_{21}, and b_{22}. Given a key $(K_1, K_2) \in (\mathbb{Z}_p)^2$, D distributes shares as follows:

1. P_1 receives $b_{11} + K_1, b_{21} + K_2$.
2. P_2 receives b_{11}, b_{12}, b_{21}.

3. P_3 receives $b_{12} + K_1, b_{21} + K_2, b_{22}$.
4. P_4 receives $b_{12} + 2K_1, b_{21} + K_2, b_{22} + K_2$.

(All arithmetic is performed in $\mathbb{Z}_p$.) □

To this point, we have explained all the information in Table 11.1 except for the values of ρ^* for access structures # 12 and # 13. These values arise from a more general version of the decomposition construction which we do not describe here; see the notes below.

11.9 Notes and References

Threshold schemes were invented independently by Blakley [BL79] and Shamir [SH79]. Secret sharing for general access structures was first studied in Ito, Saito, and Nishizeki [ISN87]; we based Section 11.2 on the approach of Benaloh and Leichter [BL90]. The vector space construction is due to Brickell [BR89A]. The entropy bound of Section 11.7 is proved in Capocelli *et al.* [CDGV93], and some of the other material from this section is found in Blundo *et al.* [BDSV93].

In this chapter, we have emphasized a linear-algebraic and combinatorial approach to secret sharing. Some interesting connections with matroid theory can be found in Brickell and Davenport [BD91]. Secret sharing schemes can also be constructed using geometric techniques. Simmons has done considerable research in this direction; we refer to [SI92A] for an overview of geometric techniques in secret sharing. Further discussion of these topics, as well as constructions for schemes having information rate $2/3$ for access structures # 12 and # 13, can be found in the expository paper by Stinson [ST92A].

Exercises

11.1 Write a computer program to compute the key for a Shamir (t, w)-threshold scheme implemented in $\mathbb{Z}_p$. That is, given t public x-coordinates, $x_1, x_2, \ldots, x_t$, and t y-coordinates $y_1, \ldots, y_t$, compute the resulting key. Use the Lagrange interpolation method, as it is easier to program.

(a) Test your program if $p = 31847$, $t = 5$ and $w = 10$, with the following

shares:

x_1	=	413	y_1	=	25439
x_2	=	432	y_2	=	14847
x_3	=	451	y_3	=	24780
x_4	=	470	y_4	=	5910
x_5	=	489	y_5	=	12734
x_6	=	508	y_1	=	12492
x_7	=	527	y_2	=	12555
x_8	=	546	y_3	=	28578
x_9	=	565	y_4	=	20806
x_{10}	=	584	y_5	=	21462

Verify that the same key is computed by using several different subsets of five shares.

(b) Having determined the key, compute the share that would be given to a participant with x-coordinate 10000. (Note that this can be done without computing the whole secret polynomial $a(x)$.)

11.2 A dishonest dealer might distribute "bad" shares for a Shamir threshold scheme, i.e., shares for which different t-subsets determine different keys. Given all w shares, we could test the consistency of the shares by computing the key for every one of the $\binom{w}{t}$ t-subsets of participants, and verifying that the same key is computed in each case. Can you describe a more efficient method of testing the consistency of the shares?

11.3 For access structures having the following bases, use the monotone circuit construction to construct a secret sharing scheme with information rate $\rho = 1/2$.

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

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

(c) $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3, P_4\}, \{P_2, P_4, P_5\}, \{P_3, P_4, P_5\}\}$.

11.4 Use the vector space construction to obtain ideal schemes for access structures having the following bases:

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

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

(c) $\Gamma_0 = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2, P_3\}, \{P_1, P_4, P_5\}, \{P_2, P_4, P_5\}\}$.

11.5 Use the decomposition construction to obtain schemes with specified information rates for access structures having the following bases:

(a) $\Gamma_0 = \{\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}\}$, $\rho = 3/5$.

(b) $\Gamma_0 = \{\{P_1, P_3, P_4\}, \{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_4\}\}$, $\rho = 4/7$.