J. Cryptology (1992) 5: 153–166

Journal of Cryptology
© 1992 International Association for
Cryptologic Research

Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes*

E. F. Brickell
Sandia National Laboratories, Albuquerque, NM 87185, U.S.A.

D. R. Stinson
Computer Science and Engineering, University of Nebraska,
Lincoln, NE 68588, U.S.A.

Communicated by Gustavus J. Simmons

Received 1 May 1990 and revised 24 May 1991

Abstract. In this paper we study secret sharing schemes for access structures based on graphs. A secret sharing scheme enables a secret key to be shared among a set of participants by distributing partial information called shares. Suppose we desire that some specified pairs of participants be able to compute the key. This gives rise in a natural way to a graph G which contains these specified pairs as its edges. The secret sharing scheme is called *perfect* if a pair of participants corresponding to a nonedge of G can obtain no information regarding the key. Such a perfect secret sharing scheme can be constructed for any graph. In this paper we study the information rate of these schemes, which measures how much information is being distributed as shares compared with the size of the secret key. We give several constructions for secret sharing schemes that have a higher information rate than previously known schemes. We prove the general result that, for any graph G having maximum degree d, there is a perfect secret sharing scheme realizing G in which the information rate is at least $2/(d + 3)$. This improves the best previous general bound by a factor of almost two.

Key words. Secret sharing, Ideal secret sharing, Perfect secret sharing, Information rate.

1. Introduction and Definitions

Informally, a *secret sharing scheme* is a method of sharing a secret key K among a finite set of participants in such a way that certain specified subsets of participants

* The work of E. F. Brickell was performed at the Sandia National Laboratories and was supported by the U.S. Department of Energy under Contract Number DE-AC04-76DP00789. The research of D. R. Stinson was supported by NSERC Operating Grant A9287 and by the Center for Communication and Information Science, University of Nebraska.

can compute a key. Suppose that $\mathbf{P}$ is the set of participants. Denote by Γ the set of subsets of participants which we desire to be able to determine the key; hence $\Gamma \subseteq 2^{\mathbf{P}}$. Γ is called the *access structure* of the secret sharing scheme. It seems reasonable to require that Γ be *monotone*, i.e.,

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

For any $\Gamma_0 \subseteq 2^{\mathbf{P}}$, define the *closure* of Γ_0 to be

$$\mathrm{cl}(\Gamma_0) = \{C\colon B \in \Gamma_0 \text{ and } B \subseteq C \subseteq \mathbf{P}\}.$$

Note that the closure of any set of subsets is monotone.

Let $\mathbf{K}$ be a set of q elements called *keys*, and let $\mathbf{S}$ be a set of s elements called *shares*. Suppose a dealer D wants to a share the secret key $K \in \mathbf{K}$ among the participants in $\mathbf{P}$ (we assume that $D \notin \mathbf{P}$). He does this by giving each participant a share. We say that the scheme is a *perfect* scheme with access structure Γ if the following two properties are satisfied:

(1) If a subset B of participants pool their shares, where $B \in \Gamma$, then they can determine the value of K.
(2) If a subset B of participants pool their shares, where $B \notin \Gamma$, then they can determine nothing about the value of K (in an information-theoretic sense), even with infinite computational resources.

We depict a secret sharing scheme as a matrix M, as was done in [5]. This matrix is not secret, but is known by all the participants. There are $|\mathbf{P}| + 1$ columns in M. The first column of M is indexed by D, and the remaining columns are indexed by the members of $\mathbf{P}$. In any row of M, we place the key K in the column D, and a possible list of shares corresponding to K in the remaining columns. When D wants to distribute shares corresponding to a key K, he will choose uniformly at random a row of M having K in column D, and distribute the shares in that row to the participants.

With this matrix representation, we can give a mathematically precise definition for conditions (1) and (2) above. Condition (1) becomes

(1′) If $B \in \Gamma$ and $M(r, b) = M(r', b)$ for all $b \in B$, then $M(r, D) = M(r', D)$.

Realizing condition (2) is more complicated, and there are at least two reasonable ways to proceed. For reasons that will become evident, we refer to the first formulation as *weakly perfect*. The condition is as follows:

(2′) If $B \notin \Gamma$, r_0 is any row and K is any key, then

$$|\{r\colon M(r, b) = M(r_0, b) \text{ for all } b \in B,\ M(r, D) = K\}| > 0.$$

The second formulation was termed "having no probabilistic information regarding the key" by Brickell and Davenport [5]. Here, we call it *strongly perfect*, or, more briefly, *perfect*. This condition is the following:

(2″) If $B \notin \Gamma$ and $f\colon B \to \mathbf{S}$ is any function, then there exists a nonnegative integer

$\lambda(f, B)$ such that

$$|\{r: \{(b, M(r, b)): b \in B\} = \{(b, f(b)): b \in B\} \text{ and } M(r, D) = K\}| = \lambda(f, B),$$

independent of the value of K.

Some explanation and discussion is certainly in order. First, it is obvious that perfect implies weakly perfect. However, we need to explain how these definitions relate to the security of the secret sharing scheme. The notion of security is made rigorous in terms of probability distributions as follows. We assume that there is a fixed *a priori* probability distribution on the set of keys $\mathbf{K}$, that is known to all the participants. Suppose a subset B of participants pool their shares. They can then compute a conditional probability distribution on the set of keys, given the information that they hold as shares. We illustrate this in the following example.

Example 1.1. Let $\mathbf{P} = \{a, b\}$ and let $\Gamma = \{\{a, b\}\}$. $\mathbf{K} = \{0, 1\}$ and $\mathbf{S} = \{0, 1, 2\}$. Let M be the following matrix:

D	a	b
0	0	1
0	0	2
0	1	1
0	2	0
1	0	0
1	1	0
1	2	2
1	2	1

This secret sharing scheme is weakly perfect but not perfect. We compute the conditional probability distribution on $\mathbf{K}$, given a value for s_a or s_b. Suppose that the two keys are equiprobable, i.e., $p(K = 0) = p(K = 1) = 1/2$. These conditional probability distributions are as follows:

$$\begin{array}{ll}
p(K = 0|s_a = 0) = 2/3, & p(K = 1|s_a = 0) = 1/3, \\
p(K = 0|s_a = 1) = 1/2, & p(K = 1|s_a = 1) = 1/2, \\
p(K = 0|s_a = 2) = 1/3, & p(K = 1|s_a = 2) = 2/3, \\
p(K = 0|s_b = 0) = 1/3, & p(K = 1|s_b = 0) = 2/3, \\
p(K = 0|s_b = 1) = 2/3, & p(K = 1|s_b = 1) = 1/3, \\
p(K = 0|s_b = 2) = 1/2, & p(K = 1|s_b = 2) = 1/2,
\end{array}$$

Let us consider what happens in general. First we consider the case of a weakly perfect scheme. Suppose $B \notin \Gamma$ and $S_B = (s_b: b \in B)$ is a possible distribution of shares to the participants in B (i.e., there is at least one row of M such that $M(r, b) = s_b$ for all $b \in B$). If K_0 is any key, then $p(K = K_0|S_B) > 0$. Hence, no key can be eliminated.

On the other hand, in a perfect scheme, we have the following stronger result.

Theorem 1.1. *Suppose M is a perfect secret sharing scheme for an access structure Γ. Suppose $B \notin \Gamma$ and $S_B = (s_b \colon b \in B)$ is a possible distribution of shares to the participants in B. If K_0 is any key, then the conditional probability $p(K = K_0 | S_B)$ equals the* a priori *probability $p(K = K_0)$.*

Proof. First we observe that there are the same number of rows of M, say λ, corresponding to each key K. This can be seen from property (2″) with B the empty set.

Now let $B \notin \Gamma$ and let $S_B = (s_b \colon b \in B)$ be a possible distribution of shares to the participants in B. Define $f \colon B \to \mathbf{S}$ to be the function such that $f(b) = s_b$ for every $b \in B$. Let K_0 be any key. Then property (2″) implies that $p(S_B | K = K_0) = \lambda(f, B)/\lambda$.

Now, we can compute $p(K = K_0 | S_B)$ as follows:

$$\begin{aligned}
p(K = K_0 | S_B) &= \frac{p(K = K_0) p(S_B | K = K_0)}{p(S_B)} \\
&= \frac{p(K = K_0)(\lambda(f, B)/\lambda)}{p(S_B)} \\
&= \frac{p(K = K_0)(\lambda(f, B)/\lambda)}{\sum_{k \in \mathbf{K}} p(K = k) p(S_B | K = K_0)} \\
&= \frac{p(K = K_0)(\lambda(f, B)/\lambda)}{(\lambda(f, B)/\lambda) \sum_{k \in \mathbf{K}} p(K = k)} \\
&= \frac{p(K = K_0)}{\sum_{k \in \mathbf{K}} p(K = k)} \\
&= p(K = K_0)
\end{aligned}$$

as desired. □

The *information rate* of the secret sharing scheme is defined to be

$$\rho = \frac{\log_2 q}{\log_2 s}.$$

It is not difficult to see that $q \le s$ in a perfect scheme, so the information rate satisfies $\rho \le 1$. If a secret sharing scheme is to be practical, we do not want to have to distribute too much secret information as shares. Consequently, we want to make the information rate as close to 1 as possible. A perfect secret sharing scheme with information rate $\rho = 1$ is called *ideal.* In Example 1.2 we depict an ideal secret sharing scheme. It is interesting to note that, for connected ideal schemes, Brickell and Davenport proved in [5] that conditions (2′) and (2″) are equivalent.

We use the notation PS(Γ, ρ, q) to denote a perfect secret sharing scheme with access structure Γ and information rate ρ for a set of q keys.

In the special case where the access structure $\Gamma = \{B \subseteq \mathbf{P} \colon |B| \ge t\}$, then the secret sharing scheme is called a *(t, w)-threshold scheme,* where $w = |P|$. Threshold schemes have been extensively studied in the literature; see [11] for a comprehensive bibliography.

Secret sharing schemes for general access structures were first studied by Ito *et al.* in [8]. They proved that *any* monotone access structure can be realized by a perfect secret sharing scheme. A more efficient construction was given by Benaloh and Leichter in [1]. In both these constructions, however, the information rate is exponentially small as a function of $|\mathbf{P}|$.

Some constructions for ideal schemes were given by Brickell [4]. More recently, ideal schemes were characterized by Brickell and Davenport [5] in terms of matroids.

Example 1.2. Let $\mathbf{P} = \{a, b, c\}$ and let $\Gamma = \{\{a, b\}, \{b, c\}, \{a, b, c\}\}$. The following is a PS($\Gamma$, 1, 3):

D	a	b	c
1	1	2	1
1	2	0	2
1	0	1	0
2	1	0	1
2	2	1	2
2	0	2	0
0	1	1	1
0	2	2	2
0	0	0	0

Note that if a has share s_a and b has share s_b, then they can compute the key as $s_b - s_a$ (modulo 3). Similarly, b and c can compute the key as $s_b - s_c$ (modulo 3). However, a and c together have no information regarding the key, since $s_a = s_c$ in every row.

2. Ideal Secret Sharing Schemes

In this section we discuss ideal secret sharing schemes in the case where the access structure consists of the closure of a graph. In this paper graphs do not have loops or multiple edges; a graph with multiple edges is termed a *multigraph*. If G is a graph, we denote the vertex set of G by $V(G)$ and the edge set by $E(G)$. G is *connected* if any two vertices are joined by a path. The *complete graph* K_n is the graph on n vertices in which any two vertices are joined by an edge. The *complete multipartite graph* $K_{n_1, n_2, \ldots, n_t}$ is a graph on $\sum_{i=1}^{t} n_i$ vertices, in which the vertex set is partitioned into subsets of size n_i ($1 \leq i \leq t$), such that vw is an edge if and only if v and w are in different subsets of the partition. An alternative way to characterize a complete multipartite graph is to say that the complementary graph is a vertex-disjoint union of cliques.

For a graph G, define PS(G, p, q) to be PS(Γ, p, q), where $\Gamma = \mathrm{cl}(E(G))$. The following result characterizing which graphs admit ideal secret sharing schemes was proved in [5].

Theorem 2.1 [5, Theorems 4 and 5]. *Suppose G is a connected graph. Then there exists a* PS(G, 1, q) *for some q if and only if G is a complete multipartite graph.*

Theorem 2.1 requires that G be connected. The cases when G is not connected are easily handled by the following easy observation.

Theorem 2.2. *Suppose G is a graph having as its connected components G_i, $1 \leq i \leq t$. Suppose that there is a* PS(G_i, ρ, q), $1 \leq i \leq t$. *Then there is a PS(G, ρ, q).*

We can easily prove the constructive half of Theorem 2.1 by using a couple of simple constructions. Suppose G is a graph and $v \in V(G)$. We define a graph $G(v)$ by replacing v by two nonadjacent vertices v_1 and v_2, such that $v_i w$ is an edge of $G(v)$ if and only if vw is an edge of G $(i = 1, 2)$. We say that $G(v)$ is constructed from G by *splitting v*.

Theorem 2.3. *Suppose G is a graph and there exists a* PS(G, ρ, q). *Then, for any vertex v of G, there exists a* PS$(G(v), \rho, q)$.

Proof. Replace column v of the matrix M by two identical columns v_1 and v_2. □

The next theorem generalizes the Shamir construction for a (2, 2)-threshold scheme [10]. It uses a structure from combinatorial design theory called an orthogonal array. An *orthogonal array* OA(k, n) is an $n^2 \times k$ array, with entries chosen from a symbol set of n elements, such that any pair of columns contains every ordered pair of symbols exactly once. It is well known that an OA(k, n) is equivalent to $k - 2$ mutually orthogonal Latin squares of order n.

Theorem 2.4. *Suppose t is a positive integer, and there exists an orthogonal array* OA$(t + 1, q)$. *Then there is a* PS$(K_t, 1, q)$.

Proof. We use the OA$(t + 1, q)$ as the matrix M representing the secret sharing scheme. The first column is indexed by D, and the remaining t columns are indexed by the participants. Let P_i and P_j be two participants. In the two corresponding columns, every ordered pair of shares occurs exactly once. Hence, property (1′) is satisfied. If we consider any one participant P_i, any share $s = f(P_i)$, and any key K, there is a unique row of M such that s occurs in column P_i and K occurs in column D. Hence, property (2″) is satisfied with $\lambda(f, P_i) = 1$. □

Corollary 2.5. *Suppose t is a positive integer, q is a prime power, and $q \geq t$. Then there is a* PS$(K_t, 1, q)$.

Proof. It is well known that an OA$(t + 1, q)$ exists if q is a prime power and $q \geq t$ (e.g., see [2]). □

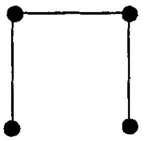
We can now prove the constructive half of Theorem 2.1 as a corollary of these constructions.

Corollary 2.6 [5, Theorem 5]. *Suppose q is a prime power and $q \geq t$. Then there is a* PS$(K_{n_1, n_2, \ldots, n_t}, 1, q)$.

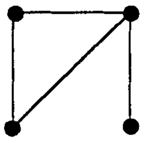
Proof. Start with a PS(K_t, 1, q) and split vertices until $K_{n_1,n_2,\ldots,n_t}$ is obtained. □

If we consider the possible graphs on at most four vertices, we find that all of them admit ideal secret sharing schemes, with two exceptions. We have the following consequence of the Theorems 2.1 and 2.2.

Theorem 2.7. *If G is a graph and $|V(G)| \leq 4$, then there exists a* PS(G, 1, q) *for some q, unless G is isomorphic to one of the following two graphs*:



P_3



H

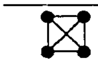
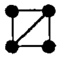
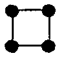
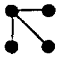
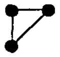
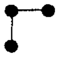
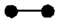
Remark. It was first shown by Benaloh and Leichter [1] that there does not exist a PS(P_3, 1, q), where P_3 is the path of length 3, for any q.

In fact, we can be more precise about the values of q admitted in Theorem 2.7.

Theorem 2.8. *If G is a connected graph, $|V(G)| \leq 4$, and G is not isomorphic to P_3 or H, then there exists a* PS(G, 1, q) *for all integers $q \in Q(G)$, where $Q(G)$ is defined in Table* 1.

Proof. It is known that there exists an OA(5, q) if $q \geq 4$, $q \neq 6$, 10; there exists an OA(4, q) if $q \geq 3$, $q \neq 6$; and there exists an OA(3, q) if $q \geq 2$ (see [2] for proofs). □

Table 1

G	$\|V(G)\|$	G^c	$Q(G)$
	4		$\{q: q \geq 4, q \neq 6, 10\}$
	4	K_2	$\{q: q \geq 3, q \neq 6\}$
	4	$K_2 \cup K_2$	$\{q: q \geq 2\}$
	4	K_3	$\{q: q \geq 2\}$
	3		$\{q: q \geq 3, q \neq 6\}$
	3	K_2	$\{q: q \geq 2\}$
	2		$\{q: q \geq 2\}$

3. Improved Lower Bounds on the Information Rate

We now turn to the construction of perfect secret sharing schemes in the cases where ideal schemes do not exist. First we give a construction that shows that the existence of a secret sharing scheme PS(Γ, ρ, q) for a single value of q implies the existence of an infinite class of schemes with the same information rate.

Theorem 3.1. *Suppose there is a* PS(Γ, ρ, q_1) *and a* PS(Γ, ρ, q_2). *Then there is a* PS(Γ, ρ, $q_1 q_2$).

Proof. Suppose M_i is the matrix representing PS(Γ, ρ, q_i), $i = 1, 2$. Let $\mathbf{K}_i$ denote the set of keys, and let $\mathbf{S}_i$ denote the set of possible shares, $i = 1, 2$. Define $\mathbf{K} = \mathbf{K}_1 \times \mathbf{K}_2$ and $\mathbf{S} = \mathbf{S}_1 \times \mathbf{S}_2$. Define a matrix M as follows: for every row r_1 of M_1 and for every row r_2 of M_2, define a row (r_1, r_2) of M by the rule

$$M((r_1, r_2), c) = (M_1(r_1, c), M_2(r_2, c)).$$

It is not difficult to see that M represents a PS(Γ, ρ', $q_1 q_2$) for some ρ', but

$$\rho' = \frac{\log_2 q_1 q_2}{\log_2 s_1 s_2},$$

where $s_1 = |\mathbf{S}_1|$ and $s_2 = |\mathbf{S}_2|$. Since

$$\rho = \frac{\log_2 q_1}{\log_2 s_1} = \frac{\log_2 q_2}{\log_2 s_2},$$

we see that

$$\begin{aligned}\rho' &= \frac{\log_2 q_1 q_2}{\log_2 s_1 s_2}\\ &= \frac{\log_2 q_1 + \log_2 q_2}{\log_2 s_1 + \log_2 s_2}\\ &= \frac{\rho \log_2 s_1 + \rho \log_2 s_2}{\log_2 s_1 + \log_2 s_2}\\ &= \rho.\end{aligned}$$

□

Corollary 3.2. *Suppose there is a* PS(Γ, ρ, q). *Then, for any positive integer n, there is a* PS(Γ, ρ, q^n).

If G is a graph, then G_1 is said to be a *subgraph* of G if $\mathrm{V}(G) \subseteq \mathrm{V}(G_1)$ and $\mathrm{E}(G) \subseteq \mathrm{E}(G_1)$. If $V_1 \subseteq \mathrm{V}(G)$, then we define the graph $G[V_1]$ to have vertex set V_1 and edge set $\{uv \in \mathrm{E}(G), u, v \in V_1\}$. We say that $G[V_1]$ is an *induced subgraph* of G. The following theorem is obvious.

Theorem 3.3. *Suppose G is a graph and G_1 is an induced subgraph of G. If there is a* PS(G, ρ, q), *then there exists a* PS(G_1, ρ, q).

Next, we prove some powerful "decomposition" constructions.

Theorem 3.4. *Suppose G is a graph, and G_1 and G_2 are connected subgraphs of G such that* $\mathrm{E}(G) = \mathrm{E}(G_1) \cup \mathrm{E}(G_2)$. *Suppose that there is a* $\mathrm{PS}(G_1, \rho_1, q)$ *and a* $\mathrm{PS}(G_2, \rho_2, q)$. *Then there is a* $\mathrm{PS}(G, \rho, q)$, *where*

$$\rho = \frac{\rho_1 \rho_2}{\rho_1 + \rho_2}.$$

Proof. Suppose M_i is the matrix representing $\mathrm{PS}(G_i, \rho_i, q)$, $i = 1, 2$. Let $\mathbf{K}$ denote the set of keys (which we can assume is the same for the two schemes), and let $\mathbf{S}_i$ denote the set of possible shares, $i = 1, 2$. For $i = 1, 2$, choose an arbitrary share $x_i \in \mathbf{S}_i$. Define $\mathbf{S} = \mathbf{S}_1 \times \mathbf{S}_2$. Define a matrix M as follows: for every row r_1 of M_1 and for every row r_2 of M_2 such that $M_1(r_1, D) = M_2(r_2, D)$, define a row (r_1, r_2) of M by the rule

$$\begin{aligned}
&M((r_1, r_2), c) = (M_1(r_1, c), M_2(r_2, c)) \quad \text{if} \quad c \in \mathrm{V}(G_1) \cap \mathrm{V}(G_2),\\
&M((r_1, r_2), c) = (M_1(r_1, c), x_2) \quad \text{if} \quad c \in \mathrm{V}(G_1) \backslash \mathrm{V}(G_2),\\
&M((r_1, r_2), c) = (x_1, M_2(r_2, c)) \quad \text{if} \quad c \in \mathrm{V}(G_2) \backslash \mathrm{V}(G_1),\\
&M((r_1, r_2), D) = M_1(r_1, D) \quad (= M_2(r_2, D)).
\end{aligned}$$

It is not difficult to see that M represents a $\mathrm{PS}(G, \rho', q)$ for some ρ', but

$$\rho' = \frac{\log_2 q}{\log_2 s_1 s_2},$$

where $s_1 = |\mathbf{S}_1|$ and $s_2 = |\mathbf{S}_2|$. Since

$$\rho_1 = \frac{\log_2 q}{\log_2 s_1}$$

and

$$\rho_2 = \frac{\log_2 q}{\log_2 s_2},$$

we see that

$$\begin{aligned}
\rho' &= \frac{\log_2 q}{\log_2 s_1 s_2}\\
&= \frac{\log_2 q}{\log_2 s_1 + \log_2 s_2}\\
&= \frac{\log_2 q}{(\log_2 q)/\rho_1 + (\log_2 q)/\rho_2}\\
&= \frac{\rho_1 \rho_2}{\rho_1 + \rho_2},
\end{aligned}$$

as desired. □

This theorem can be generalized as follows.

Theorem 3.5. *Suppose G is a graph and $G_1, \dots, G_t$ are connected subgraphs of G, such that each edge of G occurs in at least one of the G_i's. For $1 \le i \le t$, suppose that there is a* $\mathrm{PS}(G_i, \rho_i, q)$. *For every vertex v, define*

$$\rho(v) = \frac{1}{\sum_{\{i:\, v \in G_i\}} (1/\rho_i)}.$$

Then there is a $\mathrm{PS}(G, \rho, q)$, *where* $\rho = \min\{\rho(v) \colon v \in \mathrm{V}(G)\}$.

Proof. Suppose M_i is the matrix representing $\mathrm{PS}(G_i, \rho_i, q)$, $i = 1, 2, \dots, t$. Let $\mathbf{K}$ denote the set of keys (which we can assume is the same for all the schemes), and let S_i denote the set of possible shares, $i = 1, 2, \dots, t$. For each $v \in \mathrm{V}(G)$, define the Cartesian product

$$\mathrm{S}_v = \prod_{\{i:\, v \in G_i\}} \mathrm{S}_i.$$

Let S be a set of shares of size $\max\{|\mathrm{S}_v| \colon v \in \mathrm{V}(G)\}$, and for each $v \in \mathrm{V}(G)$, let $\phi_v \colon \mathrm{S}_v \to \mathrm{S}$ be any injective function. Then define a matrix M as follows: for every key K, and for every t-tuple of rows $(r_i \colon 1 \le i \le t)$ such that r_i is a row of M_i $(1 \le i \le t)$ and $M_i(r_i, D) = K$ $(1 \le i \le t)$, we define a row $(r_i : 1 \le i \le t)$ of M by the rule

$$M((r_1, r_2, \dots, r_t), c) = \phi_c(M_i(r_i, c) : c \in \mathrm{V}(G_i)),$$
$$M((r_1, r_2, \dots, r_t), D) = K.$$

The verifications are straightforward; we leave them to the reader. □

Corollary 3.6. *Suppose G is any graph with maximum degree d, and $q \ge 2$ is any integer. Then there is a* $\mathrm{PS}(G, 1/d, q)$.

Proof. Define each G_i to be an edge of G, and apply Theorem 3.5. □

Remark. Corollary 3.6 can also be proved by the "monotone circuit" construction of Benaloh and Leichter [1].

We can now obtain schemes for the two graphs P_3 and H from the previous constructions.

Corollary 3.7. *There exist schemes* $\mathrm{PS}(P_3, 0.5, q)$ *and* $\mathrm{PS}(H, 0.5, q)$ *for all* $q \ge 2$.

Proof. Existence of a scheme $\mathrm{PS}(P_3, 0.5, q)$ follows from Corollary 3.6. Existence of $\mathrm{PS}(H, 0.5, q)$ follows from decomposing H into two edge-disjoint paths of length 2, each of which admits an ideal secret sharing scheme, and applying Theorem 3.5. □

We now establish a general lower bound improving that of Corollary 3.6.

Theorem 3.8. *Suppose G is a graph of maximum degree d, and denote $e = \lceil d/2 \rceil$. Then there is a constant $\rho \geq 1/(e+1)$ such that there exists a* PS(G, ρ, q) *for all $q \geq 2$.*

Proof. Let x_i $(1 \leq i \leq 2t)$ be the vertices in V(G) having odd degree (any graph has an even number of vertices of odd degree). Construct G' from G by adding t new edges $x_{2i-1}x_{2i}$ $(1 \leq i \leq t)$. Observe that G' may contain edges of multiplicity two, in which case it is a multigraph. Every vertex of G' has even degree; hence G' is Eulerian. Let C be a (directed) Eulerian tour of G'. For every vertex $v \in$ V(G) define G_v to consist of the edges of $C \cap$ E(G) for which v is the head. Then the subgraphs G_v $(v \in$ V$(G))$ form an edge-decomposition of G. Also, each G_v is isomorphic to a complete bipartite graph K_{1,n_0}, where

$$n_0 = \frac{d_0}{2} \quad \text{if } v \text{ has degree } d_0 \text{ in } G \text{ and } d_0 \text{ is even,}$$

$$n_0 = \left\lceil \frac{d_0}{2} \right\rceil \quad \text{or} \quad \left\lfloor \frac{d_0}{2} \right\rfloor \quad \text{if } v \text{ has degree } d_0 \text{ in } G \text{ and } d_0 \text{ is odd.}$$

Hence, each G_v admits an ideal secret sharing scheme for any $q \geq 2$ (Corollary 2.6). Now apply Theorem 3.5. For every vertex $v \in$ V(G), we have

$$\rho(v) = \frac{1}{e_0 + 1} \quad \text{if } v \text{ has even degree } d_0 \text{ in } G \text{ and } e_0 = \frac{d_0}{2},$$

$$\rho(v) = \frac{1}{e_0} \quad \text{or} \quad \frac{1}{e_0 + 1} \quad \text{if } v \text{ has odd degree } d_0 \text{ in } G \text{ and } e_0 = \left\lceil \frac{d_0}{2} \right\rceil.$$

It follows that the resulting secret sharing scheme has rate $\rho = 1/e$ or $1/(e + 1)$, where G has maximum degree d and $e = \lceil d/2 \rceil$. Such a scheme can be constructed for any $q \geq 2$. □

We now show, for certain classes of graphs, that Theorem 3.8 is the best possible result that can be obtained by means of edge-decomposing a graph into complete multipartite graphs and then applying Theorems 2.1 and 3.5. For a graph G, let $\Pi = \{G_1, \ldots, G_t\}$ be a collection of subgraphs of G such that every edge of G is contained in at least one of the G_i's. Π is called a *complete multigraph covering* (or CMC) of G. For any vertex v of G, define $r_{v,\Pi}$ to be the number of G_i's in Π that contain vertex v. Let $r_\Pi = \max\{r_{v,\Pi} : v \in \text{V}(G)\}$ and let $r_G = \min\{r_\Pi : \Pi \text{ is a CMC of } G\}$. By Theorems 2.1 and 3.5, there exists a PS$(G, 1/r_G, q)$ for some q. In the case where G is a d-regular graph $(d \geq 2)$ of girth at least 5 (i.e., G contains no cycles of length 3 or 4) we can determine the value of r_G exactly.

Theorem 3.9. *If G is a d-regular graph $(d \geq 2)$ of girth at least 5, then $r_G = \lceil d/2 \rceil + 1$.*

Proof. In the special case of a d-regular graph, the proof of Theorem 3.8 always yields a CMC with $r_\Pi = \lceil d/2 \rceil + 1$; hence $r_G \leq \lceil d/2 \rceil + 1$. We show that if the girth of G is at least 5, then $r_G \geq \lceil d/2 \rceil + 1$. Let Π be a CMC of G. Since G contains no cycles of length 3 or 4, any G_i in Π must be a *star graph*, i.e., a complete bipartite graph $K_{1,m}$ for some $m \geq 1$. If any edge is in more than one of the G_i's, we can delete that edge from all but one of the G_i's containing it, and we will still have a CMC, say Π_0, in which every graph is a star graph. In Π_0, every edge occurs in exactly one of the G_i's; we call such a CMC a *complete multigraph partition*, or CMP. Also observe that $r_\Pi = r_{\Pi_0}$. Hence we can assume that there is a CMP, Π, such that $r_G = r_\Pi$.

Now every edge vw occurs in a unique G_i. If G_i is a $K_{1,m}$ with $m \geq 2$, then direct the edge $v \rightarrow w$ if w is the center of the star, and direct the edge $w \rightarrow v$ if v is the center of the star. If G_i is a $K_{1,1}$, then direct the edge $v \rightarrow w$ arbitrarily. Now every edge has a direction assigned to it.

Suppose there is a vertex v such that v is not the center of any G_i which is a $K_{1,m}$ with $m \geq 2$. Then $r_\Pi \geq d \geq \lceil d/2 \rceil + 1$, since $d \geq 2$, and we are done. Hence, we can assume, for every vertex v of G, that v is the center of at least one G_i which is a $K_{1,m}$ with $m \geq 2$. Hence, the number of directed edges $v \rightarrow w$ is at most $r_\Pi - 1$ since every such edge is in a different G_i. Then the number of directed edges $w \rightarrow v$ is at least $d - r_\Pi + 1$. If n is the number of vertices in G, then the total number of the edges in G is

$$\frac{dn}{2} = \sum_{v \in V(G)} |\{w\colon w \rightarrow v\}| \geq n(d - r_\Pi + 1).$$

Hence, $r_\Pi \geq d/2 + 1$. Since r_Π is an integer, $r_\Pi \geq \lceil d/2 \rceil + 1$ and we have the desired result. □

We now give a direct construction for a secret sharing scheme for C_6, the cycle of size 6.

Example 3.1. The following is a PS(C_6, $\log_3 2$, 2}, where V(C_6) = $\{a, b, c, d, e, f\}$ and E(C_6) = $\{\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{f, a\}\}$:

D	a	b	c	d	e	f
0	0	0	1	1	2	2
0	0	0	2	2	1	1
0	1	1	2	2	0	0
0	1	1	0	0	2	2
0	2	2	0	0	1	1
0	2	2	1	1	0	0
1	0	1	1	2	2	0
1	0	2	2	1	1	0
1	1	2	2	0	0	1
1	1	0	0	2	2	1
1	2	0	0	1	1	2
1	2	1	1	0	0	2

Note that if a has share s_a and b has share s_b, then they can compute the key to be 0 if $s_b = s_a$, and 1 otherwise. However, a and c together have no information regarding the key, since, for every ordered pair (s_b, s_c) that occurs, there is exactly one row where the key is 0 and one row where the key is 1. The analysis for other pairs of participants is similar to these arguments. The information rate $\rho = \log_2 2/\log_2 3 = \log_3 2 = 0.6309298$.

Remarks. By Theorem 2.1, there is no ideal scheme for C_6. By Theorem 3.9, the highest information rate that can be obtained from a CMC is $\rho = \frac{1}{2}$. Example 3.1 also provides us with a PS(P_3, $\log_3 2$, 2), since P_3 is an induced subgraph of C_6. We note that it is proved in [6] that no perfect secret sharing scheme for P_3 can have an information rate exceeding $\frac{2}{3} = 0.667$; and a construction is given in [6] for such a scheme with information rate $\frac{2}{3}$. The scheme constructed in [6] has $s = 8$ and $q = 4$.

4. Comments

First we observe that some of the constructions in this paper for threshold schemes based on graphs can be generalized to other access structures in a reasonably straightforward manner.

We also want to discuss briefly the difference between the model of secret sharing used in this paper (and in [4] and [5]) and the model for threshold schemes followed in [12], [9], and [7]. The two main differences are as follows:

1. In [12], [9], and [7] different participants must receive different shares.
2. In [12], [9], and [7] a key is determined as a function of the shares held by a subset of participants. Hence the key computation can be performed by a "black box" that does not know the identity of the people inputting the shares. In this paper the key is determined as a function of the shares *and* the participants holding them.

In the model of [12], [9], and [7] an ideal scheme cannot exist, since it was shown in [9] that $|\mathbf{S}| > |\mathbf{K}|$ in a perfect scheme in that setting.

Finally, we observe that a secret sharing scheme as described in this paper can be modified in a straightforward way to fit the model of [12], [9], and [7]. It suffices to define a new set of shares $\mathbf{T} = \mathbf{P} \times \mathbf{S}$, and give the share $(P_i, s) \in \mathbf{T}$ to P_i whenever the share $s \in \mathbf{S}$ would be given to P_i. With this modification, however, the information rate is lowered.

Acknowledgments

We would like to thank Richard Borie, Dean Hoffman, and Rolf Rees for helpful conversations which led to the proof of Theorem 3.8.

References

[1] J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, *Advances in Cryptology—Crypto '88 Proceedings*, Lecture Notes in Computer Science, Vol. 403, Springer-Verlag, Berlin, 1990, pp. 27–35.

[2] Th. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Bibliographisches Institut, Zurich, 1985.

[3] G. R. Blakley, Safeguarding cryptographic keys, *AFIPS Conference Proceedings*, Vol. 48, 1979, pp. 313–317.

[4] E. F. Brickell, Some ideal secret sharing schemes, *J. Combin. Math. Combin. Comput.*, **6** (1989), 105–113.

[5] E. F. Brickell and D. M. Davenport, On the classification of ideal secret sharing schemes, *Advances in Cryptology—Crypto '89 Proceedings*, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, Berlin, 1990, pp. 278–285 (also in *J. Cryptology*, **4** (1991), 123–134).

[6] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, On the sizes of shares for secret sharing schemes, presented at Crypto '91.

[7] D. Chen and D. R. Stinson, Recent results on combinatorial constructions for threshold schemes, *Australasian J. Combin.*, **1** (1990), 29–48.

[8] M. Ito, A. Saito, and T. Nishizeki, Secret sharing scheme realizing general access structure, *Proc. IEEE Globecom '87*, Tokyo, 1987, pp. 99–102.

[9] P. J. Schellenberg and D. R. Stinson, Threshold schemes from combinatorial designs, *J. Combin. Math. Combin. Comput.*, **5** (1989), 143–160.

[10] A. Shamir, How to share a secret, *Comm. ACM*, **22** (1979), 612–613.

[11] G. J. Simmons, Robust shared secret schemes or "how to be sure you have the right answer even though you don't know the question," *Congr. Numer.*, **68** (1989), 215–248.

[12] D. R. Stinson and S. A. Vanstone, A combinatorial approach to threshold schemes, *SIAM J. Discrete Math.*, **1** (1988), 230–236.