New General Lower Bounds on the Information Rate of Secret Sharing Schemes

D. R. Stinson

Computer Science and Engineering Department
and Center for Communication and Information Science
University of Nebraska
Lincoln, NE 68588-0115, U.S.A.
stinson@bibd.unl.edu

Abstract. We use two combinatorial techniques to apply a decomposition construction in obtaining general lower bounds on information rate and average information rate of certain general classes of access structures. The first technique uses combinatorial designs (in particular, Steiner systems $S(t, k, v)$). The second technique uses equitable edge-colourings of bipartite graphs. For uniform access structures of rank t, this second technique improves the best previous general bounds by a factor of t (asymptotically).

1 Introduction and Terminology

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 can compute the secret key K. The value K is chosen by a special participant called the *dealer*.

We will use the following notation. Let $\mathcal{P} = \{P_i : 1 \leq i \leq w\}$ be the set of participants. The dealer is denoted by D and we assume $D \notin \mathcal{P}$. $\mathcal{K}$ is *key set* (i.e. the set of all possible keys) and $\mathcal{S}$ is the *share set* (i.e. the set of all possible shares). Let Γ be a set of subsets of $\mathcal{P}$; this is denoted mathematically by the notation $\Gamma \subseteq 2^{\mathcal{P}}$. The subsets in Γ are those subsets of participants that should be able to compute the secret. Γ is called an *access structure* and the subsets in Γ are called *authorized subsets*.

When a dealer D wants to share a secret $K \in \mathcal{K}$, he will give each participant a share from $\mathcal{S}$. The shares should be distributed secretly, so no participant knows the share given to another participant. At a later time, a subset of participants will attempt to determine K from the shares they collectively hold. We will say that a scheme is a *perfect secret sharing scheme realizing* the access structure Γ provided the following two properties are satisfied:

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

E.F. Brickell (Ed.): Advances in Cryptology - CRYPTO '92, LNCS 740, pp. 168-182, 1993.

The security of such a scheme is unconditional, since we do not place any limit on the amount of computation that can be performed by a subset of participants.

Suppose that $B \in \Gamma$, $B \subseteq C \subseteq \mathcal{P}$ and 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:

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

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 $\Gamma = cl(\Gamma_0)$.

We define the *rank* of an access structure Γ to be the maximum cardinality of a minimal authorized subset. An access structure is *uniform* if every minimal authorized subset has the same cardinality. Observe that the rank of Γ is two if and only if $\Gamma = cl(E(G))$, where $E(G)$ denotes the edge set of a graph G.

We now briefly describe a general mathematical model for secret sharing and discuss the concept of security. In this model, we represent a secret sharing scheme by a set $\mathcal{F}$ of *distribution rules*. A distribution rule is a function

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

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

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

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

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

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

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

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

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

Then $\mathcal{F}$ is a perfect secret sharing scheme that realizes the access structure Γ. The property (*) is relatively straightforward: it says that the shares given to an authorized subset uniquely determine the value of the secret. The property (**) guarantees that the shares given to an unauthorized subset give no information as to the value of the secret. The list of shares $(f(P_i) : P_i \in B)$ given to an unauthorized subset B will restrict the possible distribution rules to some subset of $\mathcal{F}$. However, the remaining possible rules will be equally divided among the possible keys. More precisely, for any assignment of shares f to B, there will remain $\lambda(f, B)$ possible rules corresponding to each value of the secret. The formal security proof uses probability distributions; it can be found in [9].

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

$$C_6 = \{\{A, B\}, \{B, C\}, \{C, D\}, \{D, E\}, \{E, F\}, \{F, A\}\}.$$

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

Fig. 1. A Secret Sharing Scheme For C_6

	D	A	B	C	D	E	F
f_1	0	0	0	1	1	2	2
f_2	0	0	0	2	2	1	1
f_3	0	1	1	2	2	0	0
f_4	0	1	1	0	0	2	2
f_5	0	2	2	0	0	1	1
f_6	0	2	2	1	1	0	0
f_7	1	0	1	1	2	2	0
f_8	1	0	2	2	1	1	0
f_9	1	1	2	2	0	0	1
f_{10}	1	1	0	0	2	2	1
f_{11}	1	2	0	0	1	1	2
f_{12}	1	2	1	1	0	0	2

The construction of secret sharing schemes for arbitrary access structures has been studied by several researchers. General construction methods are described in [14, 1, 21, 20].

2 Information Rate

We measure the efficiency of a secret sharing scheme by the information rate. Suppose $\mathcal{F}$ is a set of distribution rules for a secret sharing scheme. For $1 \leq i \leq w$, define

$$S_i = \{f(P_i) : f \in \mathcal{F}\}.$$

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

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

The *information rate* [9] of the scheme is denoted by ρ and is defined as

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

The *average information rate* [3, 17], denoted by $\widetilde{\rho}$, is the harmonic mean of the ρ_i's:

$$\widetilde{\rho} = \frac{w}{\sum_{i=1}^{w} \frac{1}{\rho_i}} = \frac{w \log_2 |\mathcal{K}|}{\sum_{i=1}^{w} \log_2 |\mathcal{S}_i|}.$$

The scheme of Figure 1 has $\rho = \widetilde{\rho} = \log_2 2 / \log_2 3 \approx .63$. (This is not optimal: the optimal scheme has rate 2/3 [4].)

It is easy to prove that $\rho \leq \widetilde{\rho} \leq 1$ in any scheme, and that $\rho = 1$ if and only if $\widetilde{\rho} = 1$. Since $\rho = \widetilde{\rho} = 1$ is the optimal situation, we refer to such a scheme an *ideal* scheme. Ideal schemes have been studied extensively; see for example [7, 8, 17, 15, 18]. In the cases where ideal schemes do not exist, the objective is to construct a scheme with (average) information rate as close to one as possible. Research in this direction can be found in [9, 10, 4, 22, 16].

3 A Decomposition Construction

Our main recursive construction uses small schemes as building blocks in the construction of larger schemes. We call this the decomposition construction. Note that various versions of this construction have been described in several papers, such as [9, 4, 22, 17, 16].

We will use the notation $PS(\Gamma, \rho, q)$ to denote a perfect secret sharing scheme with access structure $cl(\Gamma)$ and information rate at least ρ for a set of q keys. Analogously, a perfect secret sharing scheme with access structure $cl(\Gamma)$ and average information rate at least $\widetilde{\rho}$ for a set of q keys will be denoted by $\widetilde{PS}(\Gamma, \widetilde{\rho}, q)$.

Suppose Γ is an access structure having basis Γ_0. A *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. $\cup_{k=1}^{n} \Gamma_k = \Gamma_0$

Often, $\{\Gamma_1, \ldots, \Gamma_n\}$ will form a partition of Γ_0, but this is not a requirement. For $1 \leq k \leq n$, define $\mathcal{P}_k = \cup_{B \in \Gamma_k} B$; $\mathcal{P}_k$ denotes the set of participants in a scheme with access structure $cl(\Gamma_k)$.

We present the following two results, both of which use the same construction.

Theorem 1. *Let Γ be an access structure on w participants having basis Γ_0 and suppose that $\{\Gamma_1, \ldots, \Gamma_n\}$ is a decomposition of Γ_0. Let q be an integer and for $1 \leq k \leq n$, suppose there exists a $PS(\Gamma_k, \rho_k, q)$. For $1 \leq i \leq w$, let*

$$R_i = \frac{1}{\sum_{\{k: P_i \in \mathcal{P}_k\}} \frac{1}{\rho_k}}.$$

Then there exists a $PS(\Gamma, \rho, q)$, where

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

Theorem 2. *Let Γ be an access structure on w participants having basis Γ_0 and suppose that $\{\Gamma_1, \ldots, \Gamma_n\}$ is a decomposition of Γ_0. Let q be an integer and for $1 \leq k \leq n$, suppose there exists a $\widetilde{PS}(\Gamma_k, \widetilde{\rho}_k, q)$. Then there exists a $\widetilde{PS}(\Gamma, \widetilde{\rho}, q)$, where*

$$\widetilde{\rho} = \frac{w}{\sum_{k=1}^{n} \frac{|\mathcal{P}_k|}{\rho_k}}.$$

Remark. If we define

$$\widetilde{R}_i = \frac{1}{\sum_{\{k: P_i \in \mathcal{P}_k\}} \frac{1}{\rho_k}}$$

for $1 \leq i \leq w$, then

$$\widetilde{\rho} = \frac{w}{\sum_{i=1}^{w} \frac{1}{R_i}}.$$

Proof. Let $\mathcal{K}$ be a fixed set of q keys. For $1 \leq k \leq n$, let $\mathcal{F}^k$ denote the distribution rules in a $PS(\Gamma_k, \rho_k, q)$ with key set $\mathcal{K}$. For any $K \in \mathcal{K}$, and for $1 \leq k \leq n$, we have

$$\mathcal{F}^k = \bigcup_{K \in \mathcal{K}} \mathcal{F}_K^k,$$

where $\mathcal{F}_K^k$ consists of the distribution rules in $\mathcal{F}^k$ for which the key value is K. For $1 \leq k \leq n$, suppose $f_K^k \in \mathcal{F}_K^k$. Define a distribution function $f_K^1 \times f_K^2 \times \ldots \times f_K^n$ which gives to each participant P_j the list of shares

$$(f_K^k(P_j) : P_j \in \mathcal{P}_k).$$

We construct a $PS(\Gamma, \rho, q)$ in which $\mathcal{F} = \cup_{K \in \mathcal{K}} \mathcal{F}_K$, where

$$\mathcal{F}_K = \{f_K^1 \times f_K^2 \times \ldots \times f_K^n : f_K^k \in \mathcal{F}_K^k, 1 \leq k \leq n\}.$$

The verifications and the computation of the information rate are straightforward. □

Let us look at an example to illustrate these constructions. Consider the access structure having basis

$$\Gamma_0 = \{\{A,B\},\{A,C\},\{B,C\},\{C,D\},\{C,E\},\{D,E\},\{E,F\},\{E,A\},\{F,A\}\}.$$

Consider the decomposition

$$\Gamma_1 = \{\{A,B\},\{B,C\},\{C,D\},\{D,E\},\{E,F\},\{F,A\}\}$$
$$\Gamma_2 = \{\{A,C\},\{C,E\},\{E,A\}\}.$$

We have already seen in Fig. 1 that there is a $PS(\Gamma_1, 2, \log 2/\log 3)$. For all $q \geq 3$, a $PS(\Gamma_2, q, 1)$ exists from [9]. However, in order to apply the decomposition construction, we need schemes with the same number of keys. This creates no problem, as it follows from [9] that a $PS(\Gamma_1, 2, \log 2/\log 3)$ implies the existence of a $PS(\Gamma_1, 2^j, \log 2/\log 3)$ for all $j \geq 1$. So we can take $q = 2^j$, $j \geq 2$. From Theorem 1 we get a $PS(\Gamma, 2, \rho)$ where $\rho = \log 2/\log 6 \approx .38$, and Theorem 2 yields a $\widetilde{PS}(\Gamma, 2, \widetilde{\rho})$ where $\widetilde{\rho} = \log 4/\log 18 \approx .47$.

However, if we use a different decomposition, we can do better. Define

$$\Gamma_3 = \{\{A,B\},\{B,C\},\{A,C\}\}$$
$$\Gamma_4 = \{\{C,D\},\{D,E\},\{C,E\}\}$$
$$\Gamma_5 = \{\{E,F\},\{F,A\},\{E,A\}\}.$$

For any $q \geq 3$, there exists a $PS(\Gamma_i, q, 1)$ for $i = 3, 4, 5$, and we obtain a $PS(\Gamma, q, 1/2)$ and a $\widetilde{PS}(\Gamma, q, 2/3)$.

This scheme could be implemented as follows: Suppose $q \geq 3$ is prime and let $\mathcal{K} = GF(q)$. Then $\mathcal{F}_K = \{f_{r_1,r_2,r_3,K} : r_1, r_2, r_3 \in GF(q)\}$, where

$$f_{r_1,r_2,r_3,K}(A) = (r_3, 2K + r_5)$$
$$f_{r_1,r_2,r_3,K}(B) = K + r_3$$
$$f_{r_1,r_2,r_3,K}(C) = (r_4, 2K + r_3)$$
$$f_{r_1,r_2,r_3,K}(D) = K + r_4$$
$$f_{r_1,r_2,r_3,K}(E) = (r_5, 2K + r_4)$$
$$f_{r_1,r_2,r_3,K}(F) = K + r_5.$$

In the remaining sections of this paper, we use two combinatorial techniques to apply the decomposition construction in obtaining general lower bounds on information rate and average information rate of certain general classes of access structures. The first technique uses combinatorial designs (in particular, Steiner systems $S(t, k, v)$). (Due to a lack of knowledge of infinite classes of Steiner systems for $t > 3$, this technique is applicable primarily to access structures of ranks two and three.) The second technique uses equitable edge-colourings of bipartite graphs. We first give a new proof of a result proved by Brickell and Stinson [9] which applies to access structures of rank two. Then we describe some generalizations to access structures of higher rank which improve the best previous general bounds by a factor of t (asymptotically).

4 Applications Using Steiner Systems

4.1 Two Corollaries of the Decomposition Construction

In this section we discuss applications of the decomposition construction using combinatorial designs. A *Steiner system* $S(t,k,w)$ is a pair $(X,\mathcal{A})$, where X is a set of w elements (called *points*) and $\mathcal{A}$ is a set of k–subsets of X (called *blocks*), such that every t–subset of points occurs in exactly one block. An $S(t,k,w)$ is said to be *non-trivial* if $t < k < w$. We note that no non-trivial Steiner systems are known to exist for $t > 5$, and very few are known to exist for $t > 3$. For general information on the existence of Steiner systems, we refer to [2].

Suppose Γ is an access structure of rank t on w participants, having basis Γ_0. Suppose also that $(X,\mathcal{A})$ is an $S(t,k,w)$. We can use $(X,\mathcal{A})$ to construct a decomposition of Γ_0, as follows: For every block $A \in \mathcal{A}$, define

$$\Gamma_A = \{B \in \Gamma_0 : B \subseteq A\}.$$

Then $\{\Gamma_A : A \in \mathcal{A}\}$ is a decomposition of Γ_0 (observe that it is a partition if and only if Γ is uniform).

Now suppose that we compute values $\pi_{k,t}$ and $q_{k,t}$ such that there exists a $PS(\Gamma', \pi_{k,t}, q_{k,t})$ for *any* access structure Γ' of rank $\leq t$ on k participants. Now, in the Steiner system, elementary counting shows that each point occurs in exactly $\binom{w-1}{t-1}/\binom{k-1}{t-1}$ blocks. Hence, when we apply Theorem 1, we get

$$R_i = \frac{\pi_{k,t}\binom{k-1}{t-1}}{\binom{w-1}{t-1}}$$

for every point i. The resulting scheme is a $PS(\Gamma, \rho, q_{k,t})$ for $\rho = \pi_{k,t}\binom{k-1}{t-1}/\binom{w-1}{t-1}$.

Summarizing, we have the following result.

Theorem 3. *Suppose Γ is an access structure of rank t on w participants, and suppose that an $S(t,k,w)$ exists. Suppose there exists a $PS(\Gamma', \pi_{k,t}, q_{k,t})$ for any access structure Γ' of rank $\leq t$ on k participants. Then there exists a $PS(\Gamma, \rho, q_{k,t})$ for $\rho = \pi_{k,t}\binom{k-1}{t-1}/\binom{w-1}{t-1}$.*

For average information rate, we get the following similar result by applying Theorem 2.

Theorem 4. *Suppose Γ is an access structure of rank t on w participants, and suppose that an $S(t,k,w)$ exists. Suppose there exists a $PS(\Gamma', \widetilde{\pi}_{k,t}, \widetilde{q}_{k,t})$ for any access structure Γ' of rank $\leq t$ on k participants. Then there exists a $PS(\Gamma, \widetilde{\rho}, \widetilde{q}_{k,t})$ for $\widetilde{\rho} = \widetilde{\pi}_{k,t}\binom{k-1}{t-1}/\binom{w-1}{t-1}$.*

4.2 Graph Access Structures

The situation that has been studied the most is when the basis consists of the edges of a graph (i.e. the access structure has rank two); see [9, 4, 10], for example. If G is a graph, then we will denote the vertex set of G by $V(G)$, the edge set by $E(G)$, and a $PS(cl(E(G)), \rho, q)$ by $PS(G, \rho, q)$.

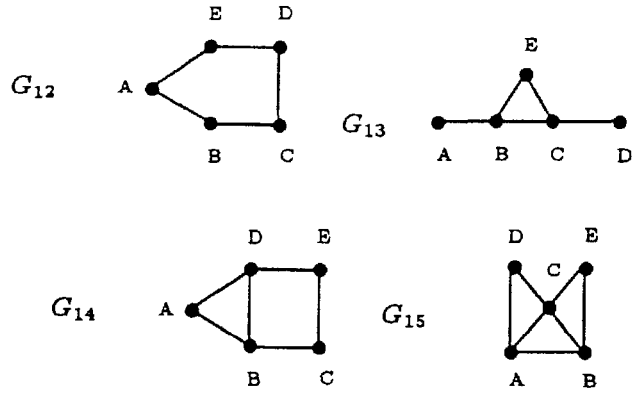
Considerable attention has been paid to the graphs on at most five vertices. Lower bounds on the (average) information rate have been obtained in [4] by applying various versions of the decomposition construction. The following result updates the bounds of [4]:

Theorem 5. *1. If G is a graph with $|V(G)| \leq 3$, then there is a $PS(G, 1, q)$ for any prime power $q \geq 3$.*

2. If G is a graph with $|V(G)| = 4$, then there is a $PS(G, 2/3, q^2)$ and a $\widetilde{PS}(G, 4/5, q)$ for any prime power $q \geq 4$.

3. If G is a graph with $|V(G)| = 5$, then there is a $PS(G, 2/3, q^2)$ and a $\widetilde{PS}(G, 5/7, q)$ for any prime power $q \geq 5$.

Proof. The only cases left unresolved in [4] concern the following four graphs on five vertices:



For G_{12}, we produce a scheme which is simultaneously a $PS(G_{12}, 2/3, q^2)$ and a $\widetilde{PS}(G_{12}, 2/3), q^2)$, where $q \geq 5$ is a prime and $\mathcal{K} = (GF(q))^2$. For each $K = (K_1, K_2) \in \mathcal{K}$, $\mathcal{F}_K = \{f_{r_1,r_2,r_3,r_4,r_5,K} : r_1, r_2, r_3, r_4, r_5 \in GF(q)\}$, where

$$f_{r_1,r_2,r_3,r_4,r_5,K}(A) = (r_1, r_4, r_5 + K_1 + 3K_2)$$
$$f_{r_1,r_2,r_3,r_4,r_5,K}(B) = (r_2, r_5, r_1 + K_1)$$
$$f_{r_1,r_2,r_3,r_4,r_5,K}(C) = (r_3, r_1, r_2 + K_2)$$
$$f_{r_1,r_2,r_3,r_4,r_5,K}(D) = (r_4, r_2, r_3 + K_1 + K_2)$$
$$f_{r_1,r_2,r_3,r_4,r_5,K}(E) = (r_5, r_3, r_4 + K_1 + 2K_2).$$

For G_{13}, we exhibit a scheme (constructed by Dean Hoffman) which is simultaneously a $PS(G_{13}, 2/3, q^2)$ and a $\widetilde{PS}(G_{12}, 10/13), q^2)$, where $q \geq 3$ is a

prime and $\mathcal{K} = (GF(q))^2$. For each $K = (K_1, K_2) \in \mathcal{K}$, $\mathcal{F}_K = \{f_{r_1,r_2,r_3,r_4,K} : r_1, r_2, r_3, r_4 \in GF(q)\}$, where

$$
\begin{aligned}
f_{r_1,r_2,r_3,r_4,K}(A) &= (r_1 + K_1, r_2) \\
f_{r_1,r_2,r_3,r_4,K}(B) &= (r_1, r_2 + K_2, r_3) \\
f_{r_1,r_2,r_3,r_4,K}(C) &= (r_2, r_3 + K_1, r_4) \\
f_{r_1,r_2,r_3,r_4,K}(D) &= (r_3, r_4 + K_2) \\
f_{r_1,r_2,r_3,r_4,K}(E) &= (r_1 + r_4 + K_1 + K_2, r_4 + K_2, r_2 - r_3).
\end{aligned}
$$

For G_{14}, we produce a scheme which is a $PS(G_{12}, 2/3, q^2)$, where $q \geq 5$ is a prime and $\mathcal{K} = (GF(q))^2$. Ror each $K = (K_1, K_2) \in \mathcal{K}$, $\mathcal{F}_K = \{f_{r_1,r_2,r_3,r_4,r_5,K} : r_1, r_2, r_3, r_4, r_5 \in GF(q)\}$, where

$$
\begin{aligned}
f_{r_1,r_2,r_3,r_4,r_5,K}(A) &= (r_1 + K_1, r_2 + K_2, r_4) \\
f_{r_1,r_2,r_3,r_4,r_5,K}(B) &= (r_1, r_4 + K_1 + 2K_2, r_5) \\
f_{r_1,r_2,r_3,r_4,r_5,K}(C) &= (r_1 + K_1, r_3 + K_1 + K_2, r_5 + 2K_1 + K_2) \\
f_{r_1,r_2,r_3,r_4,r_5,K}(D) &= (r_2, r_4 + 2K_1 + 4K_2, r_5 + 2K_1 + K_2) \\
f_{r_1,r_2,r_3,r_4,r_5,K}(E) &= (r_2 + K_2, r_3, r_5).
\end{aligned}
$$

Finally, for G_{15}, we produce a scheme which is a $PS(G_{12}, 2/3, q^2)$, where $q \geq 5$ is a prime and $\mathcal{K} = (GF(q))^2$. For each $K = (K_1, K_2) \in \mathcal{K}$, $\mathcal{F}_K = \{f_{r_1,r_2,r_3,r_4,r_5,K} : r_1, r_2, r_3, r_4, r_5 \in GF(q)\}$, where

$$
\begin{aligned}
f_{r_1,r_2,r_3,r_4,r_5,K}(A) &= (r_1 + K_1, r_4, r_5 + K_1 + 2K_2) \\
f_{r_1,r_2,r_3,r_4,r_5,K}(B) &= (r_2 + K_2, r_4 + 2K_1 + K_2, r_5) \\
f_{r_1,r_2,r_3,r_4,r_5,K}(C) &= (r_3, r_4 + 4K_1 + 2K_2, r_5 + 2K_1 + 4K_2) \\
f_{r_1,r_2,r_3,r_4,r_5,K}(D) &= (r_1, r_3 + K_1 + K_2, r_4 + 2K_1 + K_2) \\
f_{r_1,r_2,r_3,r_4,r_5,K}(E) &= (r_2, r_3 + K_1 + K_2, r_5 + K_1 + 2K_2).
\end{aligned}
$$

□

Remark. With the schemes presented above, the optimal value of the information rate and average information rate is now determined for all graph access structures on at most five vertices. In each case, the upper bound presented in [4] turns out to be the correct value. Also, the constructions for G_{12}, G_{14} and G_{15} are based on a new generalization of the decomposition that we will present in a forthcoming paper. Finally, we remark that minor modifications of the above constructions will produce schemes where the number of keys is a prime power.

Using the notation of Section 4.1, we can take $\pi_{3,2} = 1$, $\pi_{4,2} = 2/3$, and $\pi_{5,2} = 2/3$; $\widetilde{\pi}_{3,2} = 1$, $\widetilde{\pi}_{4,2} = 4/5$, and $\widetilde{\pi}_{5,2} = 5/7$.

In order to apply Theorems 3 and 4, we need information about Steiner systems $S(2, k, w)$ for $k = 3, 4, 5$. This information is summarized in the following theorem:

Theorem 6. *[13] Suppose $3 \leq k \leq 5$. Then there exists an $S(2, k, w)$ if and only if $w \equiv 1, k \pmod{k(k-1)}$.*

We obtain lower bounds on the (average) information rate of any graph on w vertices that are presented in Table 1. For example, we see that there is a $PS(G, 1/3, q)$ for any graph G having seven vertices, where $q \geq 3$ is a prime power.

Table 1. Bounds on the Information Rate for Access Structures of Rank Two

k	w	lower bound on ρ or $\widetilde{\rho}$	number of keys
3	$w \equiv 1, 3 \pmod 6$	$\rho \geq \frac{2}{w-1}$	q, where $q \geq 3$ is a prime power
4	$w \equiv 1, 4 \pmod{12}$	$\rho \geq \frac{2}{w-1}$	q^2, where $q \geq 3$ is a prime power
4	$w \equiv 1, 4 \pmod{12}$	$\widetilde{\rho} \geq \frac{12}{5(w-1)}$	q, where $q \geq 4$ is a prime power
5	$w \equiv 1, 5 \pmod{20}$	$\rho \geq \frac{8}{3(w-1)}$	q^2, where $q \geq 5$ is a prime power
5	$w \equiv 1, 5 \pmod{20}$	$\widetilde{\rho} \geq \frac{20}{7(w-1)}$	q, where $q \geq 5$ is a prime power

It is interesting to observe how the bounds improve as we use designs with larger block size. Also, note that if there does not exist an $S(2, k, w)$, then we can take the smallest integer $w_0 > w$ such that there does exist an $S(2, k, w_0)$, and delete $w_0 - w$ points from the Steiner system, thereby constructing a pairwise balanced design [2]. Then apply Theorem 1 or 2 to obtain a scheme where the information rate is computed by replacing w by w_0 in Table 1.

4.3 Rank Three Access Structures

We can apply the same techniques to access structures of rank three, using the following results concerning access structures on four participants, proved in [22, 17].

Theorem 7. *1. If Γ is a rank three access structure on four participants, then there is a $PS(\Gamma, 2/3, q^2)$ and a $\widetilde{PS}(\Gamma, 4/5, q)$ for any prime power $q \geq 4$.*

2. If Γ is a uniform rank three access structure on four participants, then there is a $PS(\Gamma, 1, q)$ for any prime power $q \geq 4$.

Using the notation of Section 4.1, we can let $\pi_{4,3} = 2/3$ and $\widetilde{\pi}_{4,3} = 4/5$. The relevant Steiner systems $S(3, 4, w)$ exist as follows:

Theorem 8. *[12] There exists an $S(3,4,w)$ if and only if $w \equiv 2,4 \pmod 6$.*

Application of Theorems 3 and 4 yield the bounds for access structures of rank three presented in Table 2.

Table 2. Bounds on the Information Rate for Access Structures of Rank Three

w	lower bound on ρ or $\overline{\rho}$	number of keys
$w \equiv 2,4 \pmod 6$	$\rho \geq \frac{4}{(w-1)(w-2)}$	q^2, where $q \geq 4$ is a prime power
$w \equiv 2,4 \pmod 6$	$\overline{\rho} \geq \frac{24}{5(w-1)(w-2)}$	q, where $q \geq 4$ is a prime power
$w \equiv 2,4 \pmod 6$	$\rho \geq \frac{6}{(w-1)(w-2)}$ if Γ is uniform	q, where $q \geq 4$ is a prime power

5 Applications Using Edge-colourings of Bipartite Graphs

The following result was proved in [9].

Theorem 9. *Suppose G is a graph in which the maximum vertex degree is d. Then there exists a $PS(G, 1/(\lceil \frac{d}{2} \rceil + 1), q)$ for any prime power $q \geq 2$.*

Remark. For the case of odd d, an improved bound is given in [5].

Theorem 9 is proved by decomposing G into complete bipartite graphs $K_{1,m}$ (called *stars*) in such a way that any vertex of G is in at most $\lceil \frac{d}{2} \rceil + 1$ of the stars. It has been shown in [8] that there is a $PS(K_{1,m}, 1, q)$ for any prime power $q \geq 2$. Hence, the result follows from Theorem 1.

The star decomposition was obtained in [9] by first constructing an eulerian tour in a multigraph related to G. We will present an alternative proof of Theorem 9 which appears to be more easily generalizable. This proof makes use of a result concerning edge-colourings of bipartite graphs.

For a graph G, denote the degree of a vertex x by $d_G(x)$. Suppose ℓ is an integer. An *ℓ–edge colouring* of G is a function $f : E(G) \rightarrow \{1, \ldots, \ell\}$. f induces a partition $E(G) = \cup_{i=1}^{\ell} E_i(G)$, where $E_i(G) = f^{-1}(i)$, $1 \leq i \leq \ell$ (that is, $E_i(G)$ consists of the edges of G receiving colour i). An ℓ–edge colouring is said to be *equitable* if, for every vertex $x \in V(G)$ and for every colour i ($1 \leq i \leq \ell$), the number of edges in $E_i(G)$ incident with vertex x is either $\lfloor d(x)/\ell \rfloor$ or $\lceil d(x)/\ell \rceil$.

The following theorem of de Werra [11] (see also [6, pp. 62-63]) is of use to us:

Theorem 10. *If G is a bipartite graph, then there exists an equitable ℓ−edge colouring of G for any positive integer ℓ.*

Here now is an alternate proof of Theorem 9:

Proof of Theorem 9. Construct a bipartite graph H with bipartition $(V(G), E(G))$ having edge set

$$E(H) = \{xe : x \in V(G), e \in E(G), x \in e\}.$$

By Theorem 10, there is an equitable 2−edge colouring of H. Each vertex $x \in V(G)$ has degree $d_G(x)$ in H and each vertex $e \in E(G)$ has degree 2 in H. Hence, every vertex $e \in E(G)$ is incident with one edge of $E_1(H)$ and every vertex $x \in V(G)$ is incident with $\lfloor d(x)/2 \rfloor$ or $\lceil d(x)/2 \rceil$ edges of $E_1(H)$.

For every vertex $x \in V(G)$, define a subgraph $G_x = \{e \in E(G) : xe \in E_1(H)\}$. It is not difficult to see that $\{G_x : x \in V(G)\}$ forms the desired star decomposition. □

Let's consider how to generalize this result to uniform access structures of higher rank. As our "building blocks" we use a class of access structures that we call *generalized stars*. Let $t \geq 2$ and $m \geq t-1$. Define a basis on $m+t-1$ participants as follows:

$$\Gamma_0^*(t,m) = \{\{P_1, \ldots, P_{t-1}, P_j\} : t \leq j \leq m+t-1\}.$$

(In the case $t = 2$, $\Gamma_0^*(t,m)$ consists of the edges of a star graph $K_{1,m}$.) Define the *centre* of a generalized star to be the intersection of the basis subsets (i.e. $\{P_1, \ldots, P_{t-1}\}$ in the above example). Any access structure $\Gamma^*(t,m)$ is easily seen to be ideal. In fact, there exists a $PS(\Gamma^*(t,m), 1, q)$ for any prime power $q \geq t$ by a simple modification of a Shamir (t,t)−threshold scheme [19].

Now, suppose Γ_0 is the basis of a uniform access structure of rank t. Construct a bipartite graph H as follows: The bipartition is (X, Y), where $Y = \Gamma_0$ and

$$X = \{A : A \subseteq B \in \Gamma_0, |A| = t-1\};$$

and the edges in H are

$$E(H) = \{AB : A \in X, B \in Y, A \subseteq B\}.$$

(In the case $t = 2$, the graph H is the same as the one constructed earlier.)

Note that every vertex $A \in X$ has degree t in H. Now, apply Theorem 10 to obtain an equitable t−edge colouring of H. For every vertex $A \in X$, define

$$\Gamma_A = \{B \in Y : AB \in E_1(H)\}.$$

Then each Γ_A is a $\Gamma_0^*(t,m)$ where $m = \lceil d_H(A)/t \rceil$ or $m = \lfloor d_H(A)/t \rfloor$. $\{\Gamma_A : A \in X\}$ is a decomposition of Γ_0, and for every $A \in X$, there is a $PS(\Gamma_A, 1, q)$ for any prime power $q \geq t$.

It remains to compute bounds on the R_i's. Define d_i (the *degree* of P_i) to be the number of $t-$subsets in Γ_0 which contain P_i. Then

$$d_i = \frac{1}{t-1} \sum_{\{A:P_i \in A \in X\}} d_H(A).$$

Now, P_i is in the centre of $|\{A \in X : P_i \in A\}|$ of the Γ_A's. Since we used an equitable colouring to construct the Γ_A's, this accounts for at least

$$\sum_{\{A:P_i \in A \in X\}} \left\lfloor \frac{d_H(A)}{t} \right\rfloor$$

of the d_i $t-$subsets in Γ_0 that contain P_i. Hence, the number of Γ_A's that contain P_i is at most

$$\begin{aligned}
&|\{A \in X : P_i \in A\}| + \sum_{\{A:P_i \in A \in X\}} \left(\frac{d_H(A)}{t-1} - \left\lfloor \frac{d_H(A)}{t} \right\rfloor \right) \\
&\leq |\{A \in X : P_i \in A\}| + \sum_{\{A:P_i \in A \in X\}} \left(\frac{d_H(A)}{t-1} - \frac{d_H(A)-t+1}{t} \right) \\
&= \frac{d_i}{t} + \frac{2t-1}{t} |\{A \in X : P_i \in A\}|
\end{aligned}$$

It is easy to see that

$$|\{A \in X : P_i \in A\}| \leq \binom{w-1}{t-2};$$

hence,

$$R_i \geq \frac{t}{(2t-1)\binom{w-1}{t-2} + d_i}$$

for $1 \leq i \leq w$.

Now ρ is just the minimum of the R_i's. To compute a bound on $\bar{\rho}$, we use the remark following Theorem 2. We calculate:

$$\begin{aligned}
\bar{\rho} &= \frac{w}{\sum_{i=1}^{w} \frac{1}{R_i}} \\
&\geq \frac{wt}{\sum_{i=1}^{w} \left((2t-1)\binom{w-1}{t-2} + d_i \right)} \\
&= \frac{wt}{w(2t-1)\binom{w-1}{t-2} + t|\Gamma_0|}.
\end{aligned}$$

Summarizing, we have the following generalization of Theorem 9:

Theorem 11. *Let Γ be a uniform access structure of rank t on w participants, and denote by d the maximum degree of any participant. Then there exists a $PS(\Gamma, \frac{t}{(2t-1)\binom{w-1}{t-2}+d}, q)$ and a $\widetilde{PS}(\Gamma, \frac{wt}{w(2t-1)\binom{w-1}{t-2}+t|\Gamma_0|}, q)$ for any prime power $q \geq t$.*

Asymptotically, the bound on ρ represents an improvement by a factor of t to the rate that would be obtained from the Benaloh-Leichter construction [1] using a disjunctive normal form boolean circuit.

Finally, note that if Γ is a non-uniform access structure of rank t, we can first partition the basis as $\Gamma_0 = \cup_{i=1}^{t} \Gamma_i$, where each Γ_i is uniform of rank i, and then apply the techniques of this section to each Γ_i.

References

1. J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. Lecture Notes in Computer Science **403** (1990) 27–35.
2. T. Beth, D. Jungnickel, and H. Lenz. Design Theory. Bibliographisches Institut, Zurich, 1985.
3. C. Blundo. Secret Sharing Schemes for Access Structures based on Graphs. Tesi di Laurea, University of Salerno, 1991.
4. C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. Presented at EUROCRYPT '92, submitted to Journal of Cryptology.
5. C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the information rate of secret sharing schemes. Presented at CRYPTO '92.
6. B. Bollobás. Graph Theory – An Introductory Course. Springer-Verlag, 1979.
7. E. F. Brickell. Some ideal secret sharing schemes. J. Combin. Math. and Combin. Comput. 9 (1989) 105–113.
8. E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. J. Cryptology 4 (1991), 123–134.
9. E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. J. Cryptology (to appear), preliminary version appeared in Lecture Notes in Computer Science **537** (1991) 242–252.
10. R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. Submitted to Journal of Cryptology, preliminary version appeared in Lecture Notes in Computer Science **576** (1992) 101–113.
11. D. de Werra. Equitable colorations of graphs. Rev. Franc. Automat. Informat. Rech. Operat. Sér. Rouge **3** (1971) 3–8.
12. H. Hanani. On quadruple systems. Canad. J. Math. **12** (1960) 145–157
13. H. Hanani. Balanced incomplete block designs and related designs. Discrete Math. **11** (1975) 255–369.
14. M. Ito, A. Saito, and T. Nishizeki. Secret sharing scheme realizing general access structure. Proc. IEEE Globecom '87 (1987) 99–102.
15. W.-A. Jackson and K. M. Martin. On ideal secret sharing schemes. Submitted to J. Cryptology.
16. K. M. Martin. New secret sharing schemes from old. Submitted to J. Comb. Math. Comb. Comp.

17. K. M. Martin. Discrete Structures in the Theory of Secret Sharing. PhD thesis, University of London, 1991.
18. P. D. Seymour. On secret-sharing matroids. Journal of Combin. Theory B (to appear).
19. A. Shamir. How to share a secret. Commun. of the ACM 22 (1979) 612–613.
20. G. J. Simmons. An introduction to shared secret and/or shared control schemes and their application. In G. J. Simmons, editor, Contemporary Cryptology, The Science of Information Integrity, IEEE Press, 1991, pp. 441–447.
21. G. J. Simmons, W. Jackson, and K. Martin. The geometry of shared secret schemes. Bulletin of the ICA 1 (1991) 71–88.
22. D. R. Stinson. An explication of secret sharing schemes. Designs, Codes and Cryptography (to appear).