A Note on Ideal Tripartite Access Structures

Michael J. Collins
Sandia National Laboratories* and Univ. of New Mexico
mjcolli@sandia.gov, mcollins@cs.unm.edu

2 December 2002

Abstract

Padró and Sáez [PS] introduced the concept of a k-partite access structure for secret sharing and gave a complete characterization of ideal bipartite structures. We derive a necessary condition for ideal tripartite structures, which we conjecture is necessary for all k.

1 Introduction

A *secret sharing scheme* is a method for distributing *shares* of a secret value s among a set of participants P in such a way that only certain "authorized" subsets of P can reconstruct s by pooling their shares. The collection of authorized subsets $\Gamma \subset 2^P$ is called an *access structure*. Naturally $S \in \Gamma$ and $S \subset T$ implies $T \in \Gamma$. It is clear that the structure is determined completely by Γ_0, the set of minimal elements of Γ. For example, a t-threshold access structure consists of all $S \subset P$ with $|S| \geq t$; then Γ_0 consists of all subsets with $|S| = t$.

More formally, the secret s and the shares x_p given to each $p \in P$ are random variables, such that for any set $S \subset P$, $H(s|\{x_p|p \in S\}) = 0$ if and only if $S \in \Gamma$. The scheme is called *perfect* if $S \notin \Gamma$ implies $H(s|\{x_p, p \in S\}) =$

*Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin company, for the U.S. Department of Energy under contract DE-AC04-94AL85000

$H(s)$; this means that non-authorized sets do not obtain any new information about s by pooling their shares. We write $H(s|S)$ for $H(s|\{x_p|p \in S\})$.

Other things being equal, the security of a system degrades as the amount of information to be kept secret increases. Thus the study of secret sharing schemes has focused on the *information rate*, which is a measure of the size of the shares relative to the size of s. Let Σ be a joint probability distribution on s and the x_p which gives a secret sharing scheme as defined above. Then the information rate is defined as

$$\rho(\Sigma, \Gamma) = \frac{H(s)}{\max_{p \in P} H(x_p)}$$

When $\rho(\Sigma, \Gamma) = 1$ then the scheme is called *ideal*. We define $\rho^*(\Gamma)$ as the maximum information rate of all perfect schemes for Γ. It is well-known that perfect schemes exist for all Γ, that $\rho^*(\Gamma) \leq 1$ for all Γ, and that for most structures, ideal schemes do not exist [St]. When $\rho^*(\Gamma) = 1$ we say that Γ is ideal.

Let Γ be an access structure on $P = \cup_{1 \leq i \leq k} Y_i$ (all Y_i disjoint). Γ is a *k-partite* access structure if, for any permutation σ of P satisfying $\sigma(Y_i) = Y_i$ for all i, we have $\sigma(S) \in \Gamma$ if and only if $S \in \Gamma$. The sets Y_i are called the *classes* of Γ. Intuitively, all members of a given class play identical roles in the structure; thus to determine whether a set is authorized, we need only know how many members it has from each Y_i. For example, in a weighted threshold scheme, all participants with the same weight are in the same class. The hierarchical and compartmented structures introduced in [Sim] are k-partite structures where k is the number of levels or compartments. Of course, every access structure is k-partite for some k (in the extreme case taking each Y_i to consist of a single participant, so $k = |P|$); but it is natural to consider families of structures in which the number of types of participants is fixed and small, while the number of participants of each type can grow large. We define $N_i = |Y_i|$.

In a k-partite scheme, a subset $S \subseteq P$ can be specified by a vector of integers $y = (y_1, \ldots, y_k)$ where $y_i = |S \cap Y_i|$. Then Γ can be thought of as a set of points in $[0, N_1] \times \cdots \times [0, N_k]$. Of course $(y_1, \ldots, y_k) \in \Gamma$ implies $(z_1, \ldots, z_k) \in \Gamma$ for all vectors z with $z_i \geq y_i$. This permits a convenient graphical representation of Γ when k is 2 or 3.

2 Previous Work

In studying the information rate of k-partite structures, our fundamental tool is the following result from [BDDV] (as generalized in [PS]), which contains most earlier bounds on information rates as special cases:

Theorem 1 *Let Γ be an access structure, let*

$$\emptyset = B_0 \subset B_i \subset \cdots \subset B_m \notin \Gamma$$

and suppose that for each $i = 1, \ldots, m$ there exists $X_i \subset P$ such that

$$B_i \cup X_i \in \Gamma \text{ but } B_{i-1} \cup X_i \notin \Gamma$$

Then

$$\rho^*(\Gamma) \leq \frac{|\cup X_i|}{m + (\cup X_i \in \Gamma)}$$

(Using the notation of [GKP] whereby, for a statement S, $(S) = 1$ if S is true and 0 if S is false).

Padró and Sáez [PS] give an explicit description of the class of ideal bipartite access structures; it is precisely the class of *quasi-threshold* structures. A quasi-threshold access structure Γ is of the form $\Gamma = T \cup A \cup B$, where for some integers $n \leq N_1 + N_2, n_1 \leq N_1, n_2 \leq N_2$, T consists of all (x, y) with $x + y \geq n, x \geq n - n_2$, and $y \geq n - n_1$; A is either empty or consists of all (x, y) with $x \geq n_1$, and B similarly is either empty or consists of all (x, y) with $y \geq n_2$. The various cases are illustrated in Figure 1.

3 A Necessary Condition for Ideal Tripartite Structures

Given a tripartite structure Γ, we can consider two-dimensional "slices" of Γ which have one coordinate fixed. Such a slice is denoted $\Gamma_{y_i=k}$. Such a slice is of course a bipartite structure. It is easy to see that $\rho^*(\Gamma_{y_i=k}) \geq \rho^*(\Gamma)$. Given a share-distribution scheme for Γ realizing information rate r, we obtain a scheme for $\Gamma_{y_i=k}$ with information rate at least r by generating shares exactly as we would for Γ, making public the shares that would have been given to

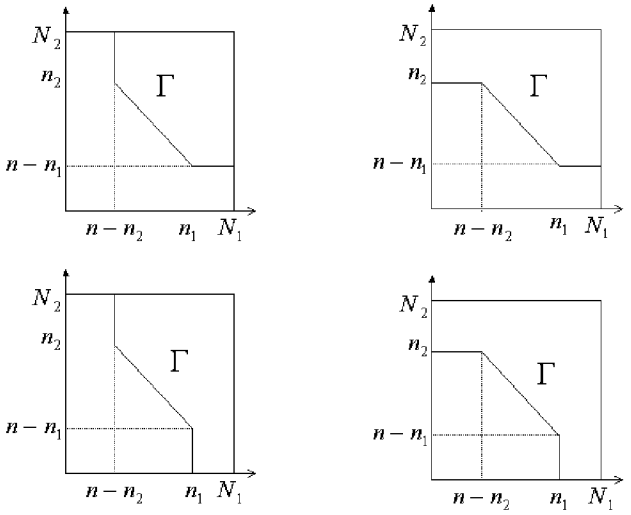

Figure 1: Ideal bipartite access structures

k members of Y_i, and removing all of Y_i from the set of participants. In particular, if Γ is ideal, then every slice $\Gamma_{x_i=k}$ must be a quasi-threshold structure.

But the converse is not true; in Figure 2 we see an illustration of a tripartite access structure which is not ideal (filled circles represent authorized sets, open circles unauthorized sets): Using theorem 1 with B_i as indicated and $X_1 = (1,0,1), X_2 = (1,0,0), X_3 = (0,0,1)$, we obtain $\rho^*(\Gamma) \leq 2/3$, even though each bipartite slice is ideal . We call this the "forbidden configuration" for tripartite access structures.

Thus we are led to seek other necessary conditions on ideal k-partite access structures which involve all k coordinates at once. Note that in a bipartite quasi-threshold structure, there is a constant c such that all $(x,y) \in \Gamma_0$ with $\min(x,y) > 0$ satisfy $x + y = c$: we will prove that the same thing happens in three dimensions. We define

$$\tilde{\Gamma} = \{(x_1, \ldots, x_k) \in \Gamma_0 | min_i(x_i) > 0\}$$

We make use of a technical lemma, which follows easily from the definition of quasi-threshold structures: We omit the rather tedious formal proof, appealing instead to the geometry of Figure 1.

Lemma 2 *Let Γ be an ideal bipartite access structure, and let $(x,y) \in \tilde{\Gamma}$. If there exists any $(x',y') \in \Gamma$ with $x' < x$, then $(x-1, y+1) \in \Gamma$. Furthermore, if $(x-1, y+1) \notin \Gamma_0$, then $(0, y+1) \in \Gamma_0$.*

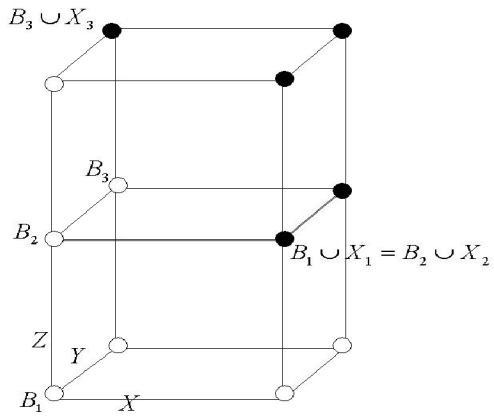

Figure 2: A non-ideal access structure

Theorem 3 *Let Γ be an ideal tripartite access structure. Then all sets in $\tilde{\Gamma}$ are the same size.*

Proof: Let (x, y, z) and $(x+\delta_X, y+\delta_Y, z-k)$ be elements of $\tilde{\Gamma}$ with $\delta_X+\delta_Y \neq k$ We will show that Γ cannot be ideal; in fact we will show that $\rho^*(\Gamma) \leq 2/3$.

There is no loss of generality in assuming that δ_X, δ_Y, and k are non-negative. In fact we must have $\delta_X > 0$; for if $\delta_X = 0$, then $\tilde{\Gamma}_{(X=x)}$ would contain two points $(y, z), (y+\delta_Y, z-k)$ whose coordinates had different sums. Similarly $\delta_Y > 0$ and $k > 0$.

Now note that if $k = 1$, we have the forbidden configuration, and can apply theorem 1 with

$$B_1 = (x-1, y, z-1), B_2 = (x, y, z-1), B_3 = (x+\delta_X-1, y+\delta_Y, z-1)$$

and

$$X_1 = (1, 0, 1), X_2 = (0, 0, 1), X_3 = (1, 0, 0)$$

So we have $k \geq 2$. The proof now proceeds by induction on k, showing that if this structure cannot be ideal when $k = k'$ then it cannot be ideal when $k = k' + 1$. We require $A = (x + \delta_X - 1, y + \delta_Y - 1, z - k + 1) \notin \Gamma$ (see Figure 3), otherwise we have the forbidden configuration as before. Also note that, in order for the slice $\Gamma_{(X=x+\delta_X)}$ to be ideal, we require $T = (x + \delta_X, y + \delta_Y - 1, z - k + 1) \in \Gamma$ by lemma 2. Now if T is minimal in the slice

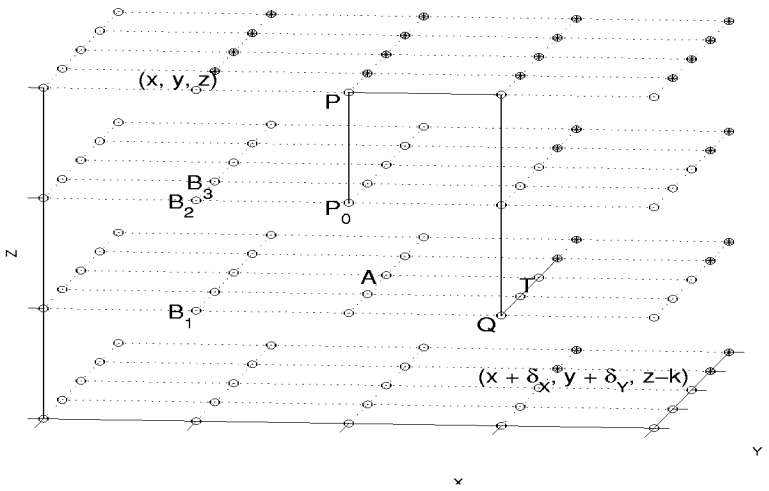

Figure 3: Proof of theorem 3

$\Gamma_{(X=x+\delta_X)}$, it is minimal in Γ (because $A \notin \Gamma$), and by induction Γ is not ideal. The only other possibility is that $(x+\delta_X, 0, z-k+1) \in \Gamma$.

Now we know that $(x+\delta_X, y-1, z) \in \Gamma$ because it dominates $(x+\delta_X, 0, z-k+1)$. Then by lemma 2, in order for the slice $\Gamma_{(Z=z)}$ to be ideal we require $P = (x+1, y-1, z) \in \Gamma$.

Now consider the slice $(Y = y)$. Since (x, z) and $(x+\delta_X, z-k+1)$ are both minimal in this slice (the latter must be minimal since $A \notin \Gamma$), we have

$$x + z = x + \delta_X + z - k + 1$$

thus

$$\delta_X = k - 1$$

But now consider the slice $\Gamma_{(Y=y-1)}$. We have that $Q = (x+\delta_X, y-1, z-k+1)$ is a minimal point in this slice (since $A \notin \Gamma$). Thus P is not minimal in this slice (since $\delta_X - k + 1 \neq 1$). So we have $P_0 = (x+1, y-1, z-1) \in \Gamma$. But $(x+1, y-1, z-2) \notin \Gamma$ (else $\Gamma_{(Y=y-1)}$ is not ideal). And now we get the forbidden configuration (see Figure 3), with

$$B_1 = (x, y-1, z-2), B_2 = (x, y-1, z-1), B_3 = (x, y, z-1)$$

and

$$X_1 = (1, 0, 1), X_2 = (1, 0, 0), X_3 = (0, 0, 1)$$

So we conclude that Γ is not ideal; indeed if the conditions of the theorem do not hold, then $\rho^*(\Gamma) \leq 2/3$. ∎

Intuitively, theorem 3 suggests that a tripartite access structure cannot be ideal unless it "sufficiently close" to being a simple threshold structure. It is natural to ask if this result generalizes to an arbitrary number of dimensions. We know of no counterexamples. Consider, for example, the hierarchical structures introduced in [Sim]. The participants are divided into k mutually disjoint levels: $P = \cup_{i=1}^{k} P_i$, with P_1 being the "highest" level and P_k the lowest. For each level i there is a threshold t_i such that $t_1 < t_2 < \cdots < t_k$. The access structure is defined as

$$\Gamma = \{S \subset P : \sum_{j=1}^{i} |S \cap P_j| \geq t_i \text{ for some } \ 1 \leq i \leq k\}$$

A standard example to illustrate this is the case of a bank vault which can be opened with the cooperation of three managers *or* two vice-presidents; then two managers and one vice-president should also suffice, since one vice-president can "stand in" for a manager. Clearly the sets P_i form a k-partite access structure. Such a structure is known to be ideal for any values of the parameters; an ideal sharing scheme is given in [GPSN]. If $S \in \Gamma$ and each coordinate is nonzero, then in particular $|S \cap P_k| > 0$; but if S is minimal, so $S - P_k \notin \Gamma$, then S must satisfy the definition with $i = k$ and $|S| = t_k$; thus every such S (if there are any) must be the same size.

References

[BDDV] C. Blundo, A. De Santis, R. De Simone, and U. Vaccaro, "Tight Bounds on the Information Rate of Secret Sharing Schemes", *Designs, Codes, and Cryptography*, v. 11 (1997) pp. 107-122

[GKP] R. Graham, D. Knuth, and O. Patashnik, "Concrete Mathematics: A Foundation for Computer Science", Addsion-Wesley, 1989

[GPSN] H. Ghodosi, J. Pieprzyk, and R. Sefavi-Naini "Cryptosystems for Hierarchical Groups", Lecture Notes in Computer Science v. 1172 pp. 275-286, Springer-Verlag 1996

[PS] C. Padró and G. Sáez, "Secret Sharing Schemes with Bipartite Access Structure" *IEEE Trans. Info. Th.*, v. 46 no. 7 (Nov. 2000) pp. 2596-2604 (earlier version in EUROCRYPT '98)

[Sim] G. Simmons, "How to (Really) Share a Secret" *CRYPTO '88*, Lecture Notes in Computer Science v. 403, pp. 390-488, Springer-Verlag, 1990

[St] D. Stinson *Cryptography: Theory and Practice*, Boca Raton: CRC, 1995