Ideal Multipartite Secret Sharing Schemes

Oriol Farràs, Jaume Martí-Farré, Carles Padró

Universitat Politècnica de Catalunya

Eurocrypt 2007, Barcelona

Plan of the Talk

How to Share a Secret

To share a secret value $k \in \mathbb{K}$, take a random polynomial

$$f(x) = k + a_1 x + \cdots + a_{d-1} x^{d-1} \in \mathbb{K}[x]$$

and distribute the shares

$$f(x_1),\ f(x_2),\ \ldots,\ f(x_n)$$

where $x_i \in \mathbb{K} - \{0\}$ is a public value associated to player p_i

Shamir 1979

Unconditional Security

Every set of d players can reconstruct the secret value from their shares by using Lagrange interpolation

$$H(K|S_1 \dots S_d) = 0$$

The shares of any $d-1$ players contain no information about the value of the secret

$$H(K|S_1 \dots S_{d-1}) = H(K)$$

Perfect (d, n)-threshold secret sharing scheme

Access structure: $\Gamma = \{A \subseteq P : |A| \geq d\}$

Shamir's scheme is ideal
(Every share has the same length as the secret)

A Generalization

What if all players are not equally important?

We can consider a Weighted threshold access structure

Every player can have a different weight $w_i \in \mathbb{Z}$

A subset $A \subseteq P$ is qualified if and only if $\sum_{i \in A} w_i \geq d$

One can take a (d, n)-threshold scheme with $n = \sum_{i \in P} w_i$
Every player receives as many shares as its weight

But this scheme is not ideal

Shamir 1979

Ideal Linear Secret Sharing Schemes

Can we construct ideal secret sharing schemes for non-threshold access structures?

The geometric schemes by Blakley (1979) were transformed by Brickell (1989) into a linear construction

Every linear code defines an ideal linear secret sharing scheme

$$(x_1, \dots, x_d) \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ \pi_0 & \pi_1 & \cdots & \pi_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} = (k, s_1, \dots, s_n)$$

$A \in \Gamma$ if and only if $\mathrm{rank}(\pi_0, (\pi_i)_{i \in A}) = \mathrm{rank}((\pi_i)_{i \in A})$

Multilevel and Compartmented Access Structures

Brickell (1989) proved that there exist
ideal linear secret sharing schemes for

Multilevel access structures
For instance, participants are divided in 3 levels
A subset is qualified if and only if it contains

- at least 5 participants in the first level, or
- at least 8 participants in the first two levels, or
- at least 15 participants in the first three levels

Multilevel and Compartmented Access Structures

Brickell (1989) proved that there exist
ideal linear secret sharing schemes for

Compartmented access structures
For instance, participants are divided in 3 classes
A subset is qualified if and only if it contains

- at least 5 participants in each class, and
- at least 20 participants in total

Multilevel and Compartmented Access Structures

Brickell (1989) proved that there exist ideal linear secret sharing schemes for

Multilevel access structures
Compartmented access structures

Other authors have proposed ideal schemes for other Multipartite access structures

Problems

Theorem (Ito, Saito, Nishizeki 1987)

There exists a secret sharing scheme for every access structure

Theorem (Benaloh, Leichter 1988)

There exist access structures that cannot be realized by any ideal secret sharing scheme

Problem

Characterize the access structures of ideal secret sharing schemes.

And, more generally,

Problem

Find the most efficient scheme for every access structure.

Ideal LSSS and Matroids

Let $Q = \{0, 1, \ldots, n\}$ and $P = Q - \{0\}$
For an ideal linear secret sharing scheme

$$(x_1, \ldots, x_d) \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ \pi_0 & \pi_1 & \cdots & \pi_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} = (k, s_1, \ldots, s_n)$$

This collection of vectors defines a representable matroid (Q, r)
For instance, from the rank function $r \colon \mathcal{P}(Q) \to \mathbb{Z}$

The access structure of the corresponding ideal linear SSS is

$$\Gamma = \Gamma_0(\mathcal{M}) = \{A \subset P : r(A \cup \{0\}) = r(A)\}$$

$$\min \Gamma = \{A \subset P : A \cup \{0\} \text{ is a circuit of } \mathcal{M}\}$$

A Sufficient Condition

Definition (matroid-related access structure)

An access structure Γ on P is matroid-related if there is a matroid $\mathcal{M}$ on $Q = P \cup \{p_0\}$ such that

$$\min \Gamma = \{A \subset P \,:\, A \cup \{p_0\} \text{ is a circuit of } \mathcal{M}\}$$

In this case, we write $\Gamma = \Gamma_{p_0}(\mathcal{M})$

Theorem (Brickell, 1989)

If $\Gamma = \Gamma_{p_0}(\mathcal{M})$ for some representable matroid $\mathcal{M}$, then Γ admits an ideal linear secret sharing scheme

A Necessary Condition

Definition (matroid-related access structure)

An access structure Γ on P is matroid-related if there is a matroid $\mathcal{M}$ on $Q = P \cup \{p_0\}$ such that

$$\min \Gamma = \{A \subset P \ : \ A \cup \{p_0\} \text{ is a circuit of } \mathcal{M}\}$$

In this case, we write $\Gamma = \Gamma_{p_0}(\mathcal{M})$

Theorem (Brickell, Davenport, 1991)

The access structure of every ideal secret sharing scheme (linear or not) is matroid-related

Characterizing Ideal Access Structures

- To characterize the matroid-related access structures
- To characterize the matroids that are represented by an ideal secret sharing scheme

It is also interesting

- To study particular families of access structures
- To find interesting families of ideal access structures

Characterizing Ideal Access Structures

- To characterize the matroid-related access structures
- To characterize the matroids that are represented by an ideal secret sharing scheme

It is also interesting

- To study particular families of access structures
- To find interesting families of ideal access structures

Problem (our goal)

Characterize the ideal multipartite access structures

What Is a Multipartite Access Structure?

Definition (multipartite access structure)

Let $\Pi = (P_1, \ldots, P_m)$ be a partition of the set P
A family of subsets $\Lambda \subseteq 2^P$ is Π-partite if, for every permutation,

$$\sigma(P_i) = P_i \; \forall i = 1, \ldots, m \Longrightarrow \sigma(\Lambda) = \Lambda$$

For instance, a Π-partite access structure

Examples:
Weighted threshold access structures
Multilevel and compartmented access structures

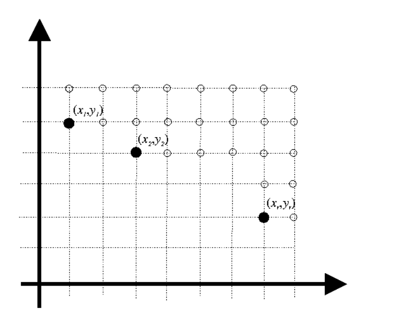
Representing Multipartite Objects

For a partition $\Pi = (P_1, \ldots, P_m)$ of P and a subset $A \subseteq P$, we define

$$\Pi(A) = (|A \cap P_1|, \ldots, |A \cap P_m|) \in \mathbb{Z}^m$$

A Π-partite family of subsets $\Lambda \subseteq 2^P$ is determined by the points

$$\Pi(\Lambda) = \{\Pi(A) \,:\, A \in \Lambda\} \subset \mathbb{Z}^m$$



Related Work (1)

- Weighted threshold access structures were introduced by Shamir (1979)
- Multilevel and compartmented access structures were proposed by Simmons (1988)
  They were proved to be ideal by Brickell (1989)
- New methods to find ideal schemes for these and other similar multipartite structures have been given by
  Tassa (2004); Tassa, Dyn (2006); Ng (2006)

Related Work (2)

- Ideal bipartite access structures
  were characterized by Padró, Sáez (1998)
- Tripartite access structures have been studied by Collins (2002)
- Ideal weighted threshold access structures
  have been characterized by Beimel, Tassa, Weinreb (2005)
  In particular, ideal schemes for some
  tripartite structures are constructed
- The first attempt to solve the general problem
  has been done by Herranz, Sáez (2006)
  They present some new results for the tripartite case

Strategy

Problem (our goal)

Characterize the ideal multipartite access structures

1. Characterize the matroid-related multipartite access structures and the corresponding matroids (necessary conditions)
2. Determine which of those matroids are representable (sufficient conditions)

Strategy

Problem (our goal)

Characterize the ideal multipartite access structures

1. Characterize the matroid-related multipartite access structures and the corresponding matroids (necessary conditions)
2. Determine which of those matroids are representable (sufficient conditions)

But... Every access structure is multipartite

So... We study the characterization of ideal access structures under a different point of view

Strategy

Problem (our goal)

Characterize the ideal multipartite access structures

1. Characterize the matroid-related multipartite access structures and the corresponding matroids (necessary conditions)
2. Determine which of those matroids are representable (sufficient conditions)

But. . . Every access structure is multipartite

So. . . We study the characterization of ideal access structures under a different point of view

Nevertheless, the most interesting applications of our results are obtained when applied to

- solve the problem in particular families, and
- find new interesting examples of ideal access structures

Multipartite Matroids

Theorem (Brickell, Davenport, 1991)

The access structure of every ideal secret sharing scheme (linear or not) is matroid-related

Problem (Goal 1)

To characterize matroid-related multipartite access structures

Definition (multipartite matroid)

A matroid $\mathcal{M} = (Q, \mathcal{I})$ is Π-partite
if the family of the independent sets $\mathcal{I} \subseteq 2^Q$ is Π-partite

Lemma

A matroid-related access structure $\Gamma = \Gamma_{p_0}(\mathcal{M})$ is Π-partite if and only if the matroid $\mathcal{M}$ is Π'-partite

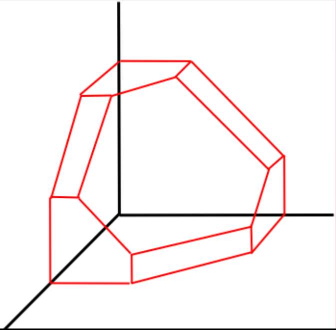
Multipartite Matroids and Discrete Polymatroids

A collection of vectors defines a matroid
A collection of subspaces defines a discrete polymatroid

A discrete polymatroid is a pair (J, h),
where $h\colon \mathcal{P}(J) \to \mathbb{Z}$ is a rank function

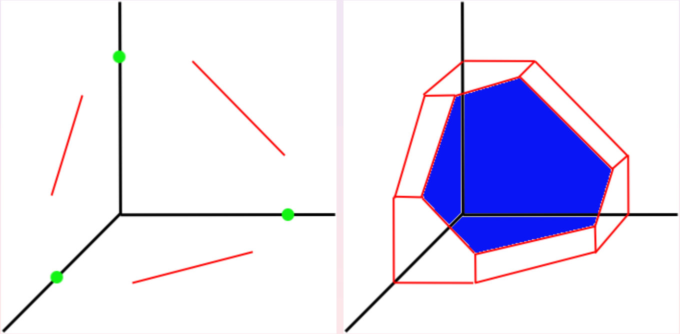
m-partite matroids $\longleftrightarrow$ discrete polymatroids on $J = \{1, \ldots, m\}$

Moreover, $\Pi(\mathcal{I})$ is a set of vectors of $\mathbb{Z}^m$ of the form



Matroid-Related Multipartite Access Structures

By using recent results by Herzog, Hibi (2002) on discrete polymatroids, we obtained a characterization of matroid-related multipartite access structures

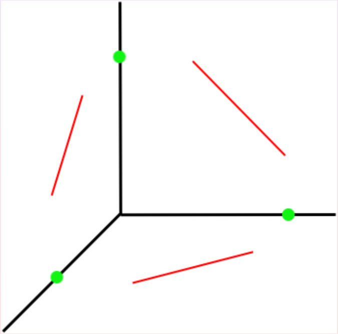


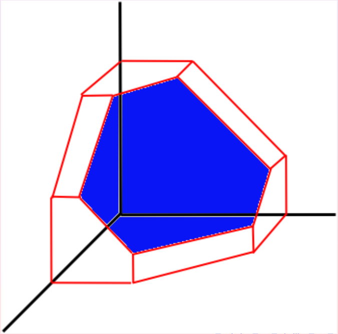
Necessary Conditions

Corollary

All minimal qualified subsets with the same support

- *have the same cardinality, and*
- *form a convex set*





Representable Multipartite Matroids

Theorem (Brickell, 1989)

If $\Gamma = \Gamma_{p_0}(\mathcal{M})$ for some representable matroid $\mathcal{M}$, then Γ admits an ideal linear secret sharing scheme

Representable Multipartite Matroids

Theorem (Brickell, 1989)

If $\Gamma = \Gamma_{p_0}(\mathcal{M})$ for some representable matroid $\mathcal{M}$, then Γ admits an ideal linear secret sharing scheme

Matroids are represented by collections of vectors
Discrete polymatroids are represented by collections of subspaces

Representable Multipartite Matroids

Theorem (Brickell, 1989)

If $\Gamma = \Gamma_{p_0}(\mathcal{M})$ for some representable matroid $\mathcal{M}$, then Γ admits an ideal linear secret sharing scheme

Matroids are represented by collections of vectors
Discrete polymatroids are represented by collections of subspaces

Theorem

A Π-partite matroid is representable if and only if the discrete polymatroid $\Pi(\mathcal{I})$ is representable

Bipartite and Tripartite Access Structures

A full characterization of ideal bipartite access structures was given by Padró and Sáez (1998)

As a consequence of our results, an easier proof of this result is obtained

Only partial results were known about the characterization of ideal tripartite access structures

With the previously known techniques, it seemed a difficult problem
From our results, a complete characterization is obtained

Theorem

Every matroid-related bipartite or tripartite access structure is ideal

This is not the case for $m = 4$ (Vamos matroid)

Nevertheless, there are nice applications of our results for $m \geq 4$.

Conclusion

- New results on the characterization of
  ideal multipartite access structures
- They are contributions to the general open problem of the
  characterization of ideal access structures
- But they are interesting mainly for
  solving the problem for particular families
  and the construction of useful ideal secret sharing schemes
- The results have been obtained by taking the adequate tool from
  Combinatorics: discrete polymatroids
  As it happened before with
  matroids (Brickell, Davenport 1991),
  polymatroids (Csirmaz 1997), and
  matroid ports (Martí-Farré, Padró 2007)