Ideal Multipartite Secret Sharing Schemes (New Results on an Old Problem)

Carles Padró

Universitat Politècnica de Catalunya

Contact Forum on Coding and Cryptography, 2007, Brussels

How to Share a Secret

A simple and brilliant idea by Shamir, 1979

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

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)

General Secret Sharing

A secret sharing scheme on the set $P = \{p_1, \ldots, p_n\}$ of participants is a mapping

$$\begin{aligned} \Pi \colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x) | \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E

- $\pi_0(x)$ is the secret value
- $\pi_i(x)$ is the share for the participant p_i

A secret sharing scheme on the set $P = \{p_1, \ldots, p_n\}$ of participants is a mapping

$$\begin{aligned} \Pi\colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x) | \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E such that

- If $A \subseteq P$ is qualified, $H(E_0|A) = H(E_0|(E_i)_{p_i \in A}) = 0$
- Otherwise, $H(E_0|A) = H(E_0)$

General Secret Sharing

A secret sharing scheme on the set $P = \{p_1, \ldots, p_n\}$ of participants is a mapping

$$\begin{aligned} \Pi \colon E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x) | \pi_1(x), \ldots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E such that

- If $A \subseteq P$ is qualified, $H(E_0|A) = H(E_0|(E_i)_{p_i \in A}) = 0$
- Otherwise, $H(E_0|A) = H(E_0)$

The qualified subsets form the access structure Γ of the scheme

If the access structure is connected, then $H(E_i) \geq H(E_0)$

General Secret Sharing

A secret sharing scheme on the set $P = \{p_1, \dots, p_n\}$ of participants is a mapping

$$\begin{aligned} \Pi\colon\ E &\to E_0 \times E_1 \times \cdots \times E_n \\ x &\mapsto (\pi_0(x) | \pi_1(x), \dots, \pi_n(x)) \end{aligned}$$

together with a probability distribution on E such that

- If $A \subseteq P$ is qualified, $H(E_0|A) = H(E_0|(E_i)_{p_i \in A}) = 0$
- Otherwise, $H(E_0|A) = H(E_0)$

The qualified subsets form the access structure Γ of the scheme

If the access structure is connected, then $H(E_i) \geq H(E_0)$

There exists a secret sharing scheme for every access structure, but in general the shares are much larger than the secret

The Old Problem

Problem

Find the best secret sharing scheme for every access structure

$\max H(E_i)$, $\sum H(E_i)$, and $H(E)$, compared to $H(E_0)$,
are used to measure the complexity of a secret sharing scheme

Definition (optimal complexity of an access structure)

Given an access structure Γ and $q = |E_0|$,

$$\sigma(\Gamma) = \inf\{\max H(E_i)/H(E_0)\} \geq 1$$

over all SSS for Γ with $q = |E_0| \geq 2$. Observe $\rho(\Gamma) = 1/\sigma(\Gamma)$
We consider as well $\sigma_q(\Gamma)$

Problem

Determine $\sigma(\Gamma)$, $\sigma_q(\Gamma)$

Ideal Secret Sharing Schemes

Definition (ideal secret sharing scheme)

A secret sharing scheme is ideal if
$H(E_i) = H(E_0)$ for every $i \in P$

Definition (ideal secret sharing scheme)

An access structure Γ is ideal if it admits an ideal scheme.
In particular, $\sigma_q(\Gamma) = 1$ for some $q \geq 2$

Problem

Characterize the ideal access structures

Linear Constructions: Ideal 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

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

$A \in \Gamma$ if and only if
$\mathrm{rank}(\pi_0, (\pi_i)_{i \in A}) = \mathrm{rank}((\pi_i)_{i \in A})$ or $r(A \cup \{p_0\}) = r(A)$

That is, $\Gamma = \Gamma_{p_0}(\mathcal{M})$ where $\mathcal{M} = (Q, r)$
is the representable matroid associated to the code

Linear Constructions: Non-Ideal Schemes

From the geometrical construction by
Simmons, Jackson, and Martin, 1991

A linear secret sharing scheme is a linear mapping

$$\begin{array}{rccl} \Pi \colon & E & \rightarrow & E_0 \times E_1 \times \cdots \times E_n \\ & x & \mapsto & (\pi_0(x) | \pi_1(x), \ldots, \pi_n(x)) \end{array}$$

with the uniform probability distribution on E, such that

- If $A \in \Gamma$, then $\bigcap_{i \in A} \ker \pi_i \subset \ker \pi_0$
- If $A \notin \Gamma$, then $\ker \pi_0 + \bigcap_{i \in A} \ker \pi_i = E$

Definition

$\lambda(\Gamma)$ is the optimal efficiency of the LSSS for Γ
We write $\lambda_{q,r}(\Gamma)$ if the set of secrets $E_0 = (\mathbb{F}_q)^r$ is fixed

Clearly, $\sigma(\Gamma) \leq \lambda(\Gamma)$ and $\sigma_{q^r}(\Gamma) \leq \lambda_{q,r}(\Gamma)$

For an arbitrary secret sharing scheme consider, for every $A \subseteq Q = P \cup \{p_0\}$

$$h(A) = \frac{H(A)}{H(E_0)}$$

Combinatorial Techniques: SSS and Polymatroids

For an arbitrary secret sharing scheme consider, for every $A \subseteq Q = P \cup \{p_0\}$

$$h(A) = \frac{H(A)}{H(E_0)}$$

Then

1. $h(\emptyset) = 0$
2. $X \subseteq Y \Rightarrow h(X) \leq h(Y)$
3. $h(X \cup Y) + h(X \cap Y) \leq h(X) + h(Y)$
4. $h(A \cup \{p_0\}) \in \{h(A), h(A) + 1\}$

$\mathcal{S} = (Q, h)$ is a p_0-ss-polymatroid, $\sigma = \max h(\{p_i\})$

From Information Theory to Combinatorics

Every p_0-ss-polymatroid defines an access structure

$$\Gamma = \Gamma_{p_0}(\mathcal{S}) = \{A \subseteq P \, : \, h(A \cup \{p_0\}) = h(A)\}$$

$\omega(\mathcal{S}) = \max h(\{p_i\})$, $\kappa(\Gamma) = \inf\{\omega(\mathcal{S}) \, : \, \Gamma_{p_0}(\mathcal{S}) = \Gamma\}$

Theorem

$$\sigma(\Gamma) \geq \kappa(\Gamma)$$

From Information Theory to Combinatorics

Every p_0-ss-polymatroid defines an access structure

$$\Gamma = \Gamma_{p_0}(\mathcal{S}) = \{A \subseteq P \,:\, h(A \cup \{p_0\}) = h(A)\}$$

$\omega(\mathcal{S}) = \max h(\{p_i\})$, $\kappa(\Gamma) = \inf\{\omega(\mathcal{S}) \,:\, \Gamma_{p_0}(\mathcal{S}) = \Gamma\}$

Theorem

$$\sigma(\Gamma) \geq \kappa(\Gamma)$$

Theorem (Csirmaz 1997)

For every access structure Γ on n players, $\kappa(\Gamma) \leq n$.

This seems to imply $\sigma(\Gamma) > \kappa(\Gamma)$ in general
The best bound by this technique: $\sigma(\Gamma_n) \geq \kappa(\Gamma_n) \geq n/\log n$

Every Ideal SSS Defines a Matroid

For every ideal secret sharing scheme, the mapping

$$h(A) = \frac{H(A)}{H(E_0)}$$

is such that $h(A \cup \{x\}) \in \{h(A), h(A) + 1\}$

That is, the polymatroid $\mathcal{M} = (Q, h)$ is a matroid with

$$\Gamma = \Gamma_{p_0}(\mathcal{M}) = \{A \subseteq P \,:\, h(A \cup \{p_0\}) = h(A)\}$$

or, equivalently

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

Γ is matroid-related, or $\min \Gamma$ is a matroid-port

In this situation we say that $\mathcal{M}$ is ss-representable or entropic

More about Matroids

Theorem (Brickell and Davenport 1991)

Every ideal access structure is matroid-related

Theorem (Seymour 1992)

The Vamos matroid is not ss-representable
There exist non-ideal matroid-related access structures

Theorem (Martí-Farré and P. 2007)

If Γ is not matroid-related, then $\kappa(\Gamma) \geq 3/2$
In particular, there is no access structure with $1 < \kappa(\Gamma) < 3/2$

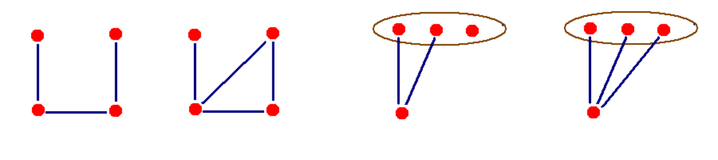
Are there other gaps in the values of $\kappa(\Gamma)$?

Is there an access structure with $1 < \sigma(\Gamma) < 3/2$?

An Old but Unknown Result

Theorem (Seymour, 1976)

An access structure is matroid-related if and only if it has no minor isomorphic to Φ, $\widehat{\Phi}$, $\widehat{\Phi}^*$ or Ψ_s with $s \geq 3$.



How Good are Linear Schemes?

$$\kappa(\Gamma) \leq \sigma(\Gamma) \leq \lambda(\Gamma), \qquad \kappa(\Gamma) \leq \sigma_{q^r}(\Gamma) \leq \lambda_{q,r}(\Gamma)$$

In general, there is a wide gap between lower and upper bounds
Many open questions about the functions κ and λ
In addition, they are not enough to get the values of σ

Non-linear schemes can be more efficient than the linear ones

Theorem (Beimel and Weinreb 2003)

There exist a family of access structures such that $\mu(\Gamma)$ is linear on n while $\lambda(\Gamma)$ is superpolynomial

The non-linear schemes for this result are quasi-linear
Very few non-linear constructions are known

How Good Are Combinatorial Bounds?

$$\kappa(\Gamma) \le \sigma(\Gamma) \le \lambda(\Gamma), \qquad \kappa(\Gamma) \le \sigma_{q^r}(\Gamma) \le \lambda_{q,r}(\Gamma)$$

What about the separation between κ and σ?

A polymatroid $\mathcal{S} = (Q, h)$ is entropic if there exist random variables such that $h(A) = H(A)$ for every $A \subseteq Q$

There exist non-entropic polymatroids
Non-Shannon inequalities

Nevertheless, no example with $\kappa(\Gamma) < \mu(\Gamma)$ was known

Duality

The dual of an access structure

$$\Gamma^* = \{A \subseteq P : P - A \notin \Gamma\}$$

- $\lambda_{q,r}(\Gamma) = \lambda_{q,r}(\Gamma^*)$ (dual code)
- $\kappa(\Gamma) = \kappa(\Gamma^*)$ (dual polymatroid)
- Γ matroid-related $\Longleftrightarrow$ Γ^* matroid-related (dual matroid)

Problem

- *Is there any relation between $\mu(\Gamma)$ and $\mu(\Gamma^*)$?*
- *Is the dual of an ideal access structure ideal?*

Non-Ideal Matroid-Related Access Structures

Problem

Characterize the ss-representable (or entropic) matroids

Problem

Characterize the asymptotically entropic matroids

If $\sigma(\Gamma) = 1$ but there is no ideal scheme for Γ, then $\Gamma = \Gamma_{p_0}(\mathcal{M})$, where $\mathcal{M}$ is asymptotically entropic but non-entropic

Problem

Determine $\sigma(\Gamma)$ for the matroid-related access structures
In particular, is there a matroid-related structure with $\sigma(\Gamma) > 1$?

Vamos and Non-Desargues Matroids

If there exists and access structure with $1 < \sigma(\Gamma) < 3/2$, it must be matroid-related

Theorem (Beimel and Livne, 2006)

In every SSS for the access structures related to the Vamos matroid, the size of the shares is at least $k + \Omega(\sqrt{k})$

This does not imply $\sigma(\Gamma) > 1$

Theorem

For every access structure related to the Vamos or the non-Desargues matroids, $\sigma(\Gamma) \leq \lambda(\Gamma) \leq 4/3$

Non-Shannon Inequalities

Theorem (Zhang-Yeung,1998)

For every four discrete random variables $A, B, C,$

$$3[H(CD) + H(BD) + H(BC)] + H(AC) + H(AB)$$
$$\geq H(D) + 2[H(C) + H(B)] + H(AD) + 4H(BCD) + H(ABC)$$

Theorem (Ingleton, 1971)

For every four linear discrete random variables $A, B, C,$ and D,

$$H(CD) + H(BD) + H(BC) + H(AC) + H(AB)$$
$$\geq H(C) + H(B) + H(AD) + H(BCD) + H(ABC)$$

Lower Bounds beyond Combinatorics

By combining non-Shannon inequalities with combinatorial results by Beimel and Livne (TCC 2006)

Theorem

Let Γ be the access structure induced by the Vamos matroid.

$$\kappa(\Gamma) = 1 < 10/9 \leq \sigma(\Gamma) \leq \lambda(\Gamma) \leq 4/3 < 3/2$$

$$\kappa(\Gamma) = 1 < 10/9 < 6/5 \leq \lambda(\Gamma) \leq 4/3 < 3/2$$

The first example of $\kappa(\Gamma) < \sigma(\Gamma)$

The first example of $1 < \sigma(\Gamma) < 3/2$

Studying the Problems for Particular Families

For instance, constructing ideal schemes for nice 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

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

Other authors have proposed ideal schemes for other
Multipartite 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

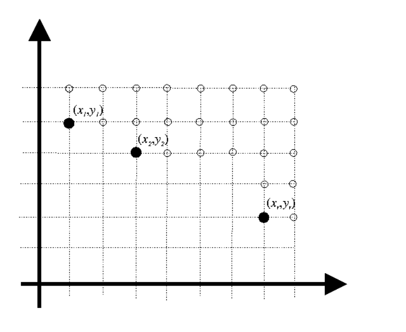
Representing Multipartite Objects

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

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



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)

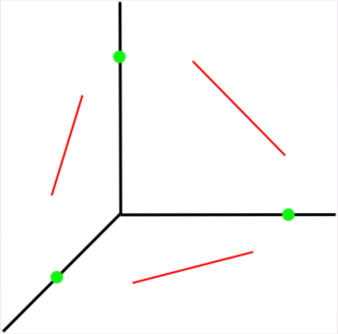
A matroid $\mathcal{M} = (Q, \mathcal{I})$ is Π-partite
if the family of the independent sets $\mathcal{I} \subseteq 2^Q$ is Π-partite

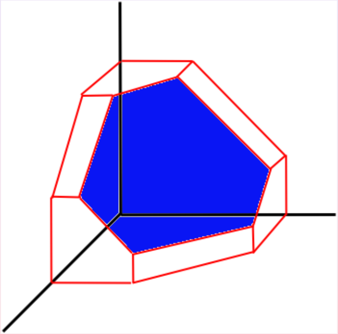
Lemma

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

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



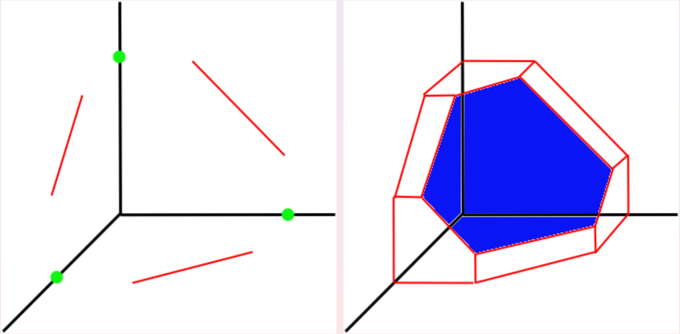


Necessary Conditions

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

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)