On the Optimization of Bipartite Secret Sharing Schemes

Oriol Farràs, Jessica Ruth Metcalf-Burton,
Carles Padró, Leonor Vázquez

Seminar MAS-SPMS-NTU, Singapore, January 2010

How to Share a Secret

How to share a secret in such a way that $t \leq n$ players can reconstruct it but $t - 1$ players get no information?

How to Share a Secret

How to share a secret in such a way that $t \leq n$ players can reconstruct it but $t-1$ players get no information?

A simple and brilliant idea by Shamir, 1979

Let $\mathbb{K}$ be a finite field with $|\mathbb{K}| \geq n+1$

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

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

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

Independently, Blakley proposed in 1979
a geometric secret sharing scheme

Properties of Shamir's Secret Sharing Scheme

1. It is a threshold scheme
2. It is perfect
3. It is ideal
4. It is linear
5. It is multiplicative

Properties of Shamir's Secret Sharing Scheme

1. It is a threshold scheme
   Every set of t players can reconstruct the secret value $k = f(0)$
   from their shares $f(x_1), \ldots, f(x_t)$
   by using Lagrange interpolation
2. It is perfect
3. It is ideal
4. It is linear
5. It is multiplicative

Properties of Shamir's Secret Sharing Scheme

1. It is a threshold scheme
   Every set of t players can reconstruct the secret value $k = f(0)$
   from their shares $f(x_1), \ldots, f(x_t)$
   by using Lagrange interpolation
2. It is perfect
   The shares of any $t - 1$ players contain no information
   about the value of the secret
3. It is ideal
4. It is linear
5. It is multiplicative

Properties of Shamir's Secret Sharing Scheme

1. It is a threshold scheme
2. It is perfect
3. It is ideal
   Every share has the same length as the secret:
   all are elements in a finite field
   This is the best possible situation
4. It is linear
5. It is multiplicative

Properties of Shamir's Secret Sharing Scheme

1. It is a threshold scheme
2. It is perfect
3. It is ideal
4. It is linear
   Shares are a linear function of the secret and random values.
   The secret can be recovered by a linear function of the shares.
   Shares for a linear combination of two secrets
   can be obtained from the linear combination of the shares

   $$\lambda_1 k_1 + \lambda_2 k_2 = (\lambda_1 f_1 + \lambda_2 f_2)(0) \qquad \lambda_1 s_{1i} + \lambda_2 s_{2i} = (\lambda_1 f_1 + \lambda_2 f_2)(x_i)$$

5. It is multiplicative

Properties of Shamir's Secret Sharing Scheme

1. It is a threshold scheme
2. It is perfect
3. It is ideal
4. It is linear
5. It is multiplicative
   If $n \geq 2t - 1$, shares for the product of two secrets can be obtained from the products of the shares

$$k_1 k_2 = f_1 f_2(0) \qquad s_{1i} s_{2i} = f_1 f_2(x_i)$$

Properties of Shamir's Secret Sharing Scheme

1. It is a threshold scheme
2. It is perfect
3. It is ideal
4. It is linear
5. It is multiplicative

To which extent these properties can be generalized to secret sharing schemes with other access structures?

The access structure Γ is the family of qualified subsets

Existential Questions & Optimization Problems

Does there exist a perfect SSS for every access structure?

Existential Questions & Optimization Problems

Does there exist a perfect SSS for every access structure? YES

Existential Questions & Optimization Problems

Does there exist a perfect SSS for every access structure? YES

- From now on, we deal only with perfect schemes

Existential Questions & Optimization Problems

Does there exist a perfect SSS for every access structure? YES

- From now on, we deal only with perfect schemes

Does there exist a linear SSS for every access structure?

Existential Questions & Optimization Problems

Does there exist a perfect SSS for every access structure? YES

- From now on, we deal only with perfect schemes

Does there exist a linear SSS for every access structure? YES

Existential Questions & Optimization Problems

Does there exist a perfect SSS for every access structure? YES

- From now on, we deal only with perfect schemes

Does there exist a linear SSS for every access structure? YES

Does there exist an ideal SSS for every access structure?

Existential Questions & Optimization Problems

Does there exist a perfect SSS for every access structure? YES

- From now on, we deal only with perfect schemes

Does there exist a linear SSS for every access structure? YES

Does there exist an ideal SSS for every access structure? NO

Existential Questions & Optimization Problems

Does there exist a perfect SSS for every access structure? YES

- From now on, we deal only with perfect schemes

Does there exist a linear SSS for every access structure? YES

Does there exist an ideal SSS for every access structure? NO

Problem

What access structures admit an ideal secret sharing scheme?

Existential Questions & Optimization Problems

Does there exist a perfect SSS for every access structure? YES

- From now on, we deal only with perfect schemes

Does there exist a linear SSS for every access structure? YES

Does there exist an ideal SSS for every access structure? NO

Problem

What access structures admit an ideal secret sharing scheme?

Problem

To find the most efficient (linear) secret sharing scheme for every access structure

Some Interesting Access Structures

Shamir (1979) introduced the weighted threshold access structures
Every participant has a weight
A subset is qualified if and only if
the weight sum attains certain threshold

These access structures are hierarchical
The scheme proposed by Shamir is not ideal

Simmons (1988) introduced the
multilevel and compartmented access structures

Brickell (1989) presented ideal secret sharing schemes for them

P. and Sáez (1998) studied those problems
for the bipartite access structures

Subsequently, many other works appeared on
multipartite secret sharing schemes
specially on the construction of ideal schemes and
the characterization of ideal access structures

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

A secret sharing scheme is a collection of random variables

- $\pi_0(x) \in E_0$ is the secret value
- $\pi_i(x) \in E_i$ is the share for the player p_i

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

A secret sharing scheme is a collection of random variables such that

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

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

A secret sharing scheme is a collection of random variables such that

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

The qualified subsets form the access structure Γ of the scheme

If p_i is a non-redundant player, then $H(E_i) \geq H(E_0)$

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

A secret sharing scheme is a collection of random variables such that

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

The qualified subsets form the access structure Γ of the scheme

If p_i is a non-redundant player, 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

Complexity of Secret Sharing Schemes

Problem

To find the most efficient 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 (complexity of a secret sharing scheme)

The complexity $\sigma(\Sigma)$ of a secret sharing scheme Σ is defined as

$$\sigma(\Sigma) = \max_{p_i \in P} \frac{H(E_i)}{H(E_0)} \geq 1$$

The Big Problem

Problem

To find the most efficient secret sharing scheme
for every access structure

Definition (optimal complexity of an access structure)

The optimal complexity $\sigma(\Gamma)$ of an access structure Γ is the infimum of the complexities of all secret sharing schemes for Γ

Problem

To determine $\sigma(\Gamma)$ for every Γ
At least, to determine the asymptotic behavior of this parameter

Very little is known about this problem

It has been studied for several
particular families of access structures

Bipartite Access Structures

In this paper, we consider this problem for
bipartite access structures

An access structure is bipartite if

$$P = P_1 \cup P_2$$

and participants in the same part play an equivalent role.

Ideal bipartite access structures
were characterized by Padró and Sáez, 1998
Some bounds on $\sigma(\Gamma)$ were given in that work

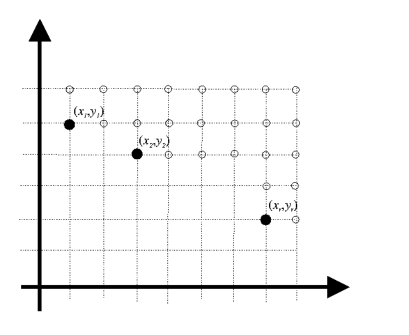
More general results about ideal multipartite access structures
by Farràs, Martí-Farré and P. 2007

Geometric Representation

Let Γ be a bipartite access structure on $P = P_1 \cup P_2$.
For every set $A \subseteq P$, consider

$$\Pi(A) = (|A \cap P_1|, |A \cap P_2|) \in \mathbb{Z}_+^2$$

The set of points $\Pi(\Gamma) = \{\Pi(A) \ : \ A \in \Gamma\} \subseteq \mathbb{Z}_+^2$ determine Γ



Actually, the minimal points in $\Pi(\min \Gamma)$ determine Γ

Upper Bounds from Constructions

Of course, every construction of a secret sharing scheme Σ for Γ provides an upper bound: $\sigma(\Gamma) \leq \sigma(\Sigma)$

Most of the good construction methods used until now provide linear secret sharing schemes

Upper Bounds from Constructions

Of course, every construction of a secret sharing scheme Σ for Γ provides an upper bound: $\sigma(\Gamma) \leq \sigma(\Sigma)$

Most of the good construction methods used until now provide linear secret sharing schemes

That is, the mapping $x \mapsto (\pi_0(x)|\pi_1(x), \ldots, \pi_n(x))$ is linear and $x \in E$ is chosen with uniform probability

Definition

For an access structure Γ, we define $\lambda(\Gamma)$ as the infimum of the complexities of all linear secret sharing schemes for Γ

Obviously, $\sigma(\Gamma) \leq \lambda(\Gamma)$

If Γ is bipartite,
$\sigma(\Gamma) \leq \lambda(\Gamma) \leq$ number of minimal points $\leq \min\{|P_1|, |P_2|\}$

How Good Are Linear Secret Sharing Schemes?

For some access structures, the optimal schemes must be non-linear

Beimel and Weinreb (2005) proved a strong separation result:
There exist a family of access structures such that
$\sigma(\Gamma_n)$ grows linearly while
$\lambda(\Gamma_n)$ grows superpolynomially

Problem

Is $\sigma(\Gamma) = \lambda(\Gamma)$ for every bipartite access structure?

Combinatorial Lower Bounds, Polymatroids

Consider $P = \{p_1, \ldots, p_n\}$ and $Q = P \cup \{p_0\}$

For an arbitrary secret sharing scheme consider, for every $A \subseteq Q$

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

Combinatorial Lower Bounds, Polymatroids

Consider $P = \{p_1, \ldots, p_n\}$ and $Q = P \cup \{p_0\}$

For an arbitrary secret sharing scheme consider, for every $A \subseteq Q$

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

Then

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

Combinatorial Lower Bounds, Polymatroids

Consider $P = \{p_1, \ldots, p_n\}$ and $Q = P \cup \{p_0\}$

For an arbitrary secret sharing scheme consider, for every $A \subseteq Q$

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

Then

1. $h(\emptyset) = 0$
2. $X \subseteq Y \subseteq Q \Rightarrow h(X) \leq h(Y)$
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 polymatroid
- p_0 is an atomic point of $\mathcal{S}$
- $\Gamma = \Gamma_{p_0}(\mathcal{S}) = \{A \subseteq P \,:\, h(A \cup \{p_0\}) = h(A)\}$

Fujishige 1978, Csirmaz 1997

Lower Bounds from Polymatroids

For a polymatroid $\mathcal{S} = (Q, h)$, we define $\sigma(\mathcal{S}) = \max_{p \in Q} h(\{p\})$

Every polymatroid $\mathcal{S} = (Q, h)$ with an atomic point $p_0 \in Q$ defines an access structure on $P = Q - p_0$

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

In this situation, we say that $\mathcal{S}$ is a Γ-polymatroid

$$\kappa(\Gamma) = \inf\{\sigma(\mathcal{S}) \ : \ \Gamma = \Gamma_{p_0}(\mathcal{S})\}$$

Lower Bounds from Polymatroids

For a polymatroid $\mathcal{S} = (Q, h)$, we define $\sigma(\mathcal{S}) = \max_{p \in Q} h(\{p\})$

Every polymatroid $\mathcal{S} = (Q, h)$ with an atomic point $p_0 \in Q$ defines an access structure on $P = Q - p_0$

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

In this situation, we say that $\mathcal{S}$ is a Γ-polymatroid

$$\kappa(\Gamma) = \inf\{\sigma(\mathcal{S}) \,:\, \Gamma = \Gamma_{p_0}(\mathcal{S})\}$$

A secret sharing scheme Σ for Γ defines a polymatroid $\mathcal{S} = \mathcal{S}(\Sigma)$ such that $\Gamma = \Gamma_{p_0}(\mathcal{S})$ and $\sigma(\Sigma) = \sigma(\mathcal{S})$

Therefore $\kappa(\Gamma) \leq \sigma(\mathcal{S}) = \sigma(\Sigma)$

Lower Bounds from Polymatroids

For a polymatroid $\mathcal{S} = (Q, h)$, we define $\sigma(\mathcal{S}) = \max_{p \in Q} h(\{p\})$

Every polymatroid $\mathcal{S} = (Q, h)$ with an atomic point $p_0 \in Q$ defines an access structure on $P = Q - p_0$

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

In this situation, we say that $\mathcal{S}$ is a Γ-polymatroid

$$\kappa(\Gamma) = \inf\{\sigma(\mathcal{S}) \,:\, \Gamma = \Gamma_{p_0}(\mathcal{S})\}$$

A secret sharing scheme Σ for Γ defines a polymatroid $\mathcal{S} = \mathcal{S}(\Sigma)$ such that $\Gamma = \Gamma_{p_0}(\mathcal{S})$ and $\sigma(\Sigma) = \sigma(\mathcal{S})$

Therefore $\kappa(\Gamma) \le \sigma(\mathcal{S}) = \sigma(\Sigma)$

Theorem

For every access structure Γ

$$\kappa(\Gamma) \le \sigma(\Gamma) \le \lambda(\Gamma)$$

How Good Are Combinatorial Lower Bounds?

Theorem (Csirmaz 1997)

There exist a family of access structures with

$$\sigma(\Gamma_n) \geq \kappa(\Gamma_n) \geq \frac{n}{\log n}$$

This is the best known general lower bound on σ

But, on the other hand

Theorem (Csirmaz 1997)

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

This seems to imply that $\kappa(\Gamma)$
must be in general much smaller than $\sigma(\Gamma)$

Nevertheless no strong separation result
between these parameters is known

How Good Are Combinatorial Lower Bounds?

No strong separation result between κ and σ is known

The first examples of access structures with $\kappa(\Gamma) < \sigma(\Gamma)$ have been found recently by using non-Shannon information inequalities (Beimel, Livne, and P. 2008)

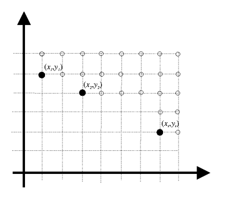
Nevertheless, non-Shannon information inequalities cannot give strong separation results (Beimel and Orlov 2008)

Problem

Is $\sigma(\Gamma) = \kappa(\Gamma)$ for every bipartite access structure?

Multipartite Polymatroids

Let Γ be a bipartite access structure on $P = P_1 \cup P_2$.



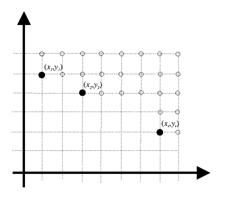
$$\kappa(\Gamma) = \inf\{\sigma(\mathcal{S}) \,:\, \Gamma = \Gamma_{p_0}(\mathcal{S})\}$$

We prove that we can restrict to $(\{p_0\}, P_1, P_2)$-partite polymatroids $\mathcal{S} = (Q, h)$ such that $h(A)$ depends only on $|A \cap \{p_0\}|, |A \cap P_1|, |A \cap P_2|$

In addition, $\kappa(\Gamma)$ is independent from $|P_i|$
It depends only on the minimal points

We do not know if the same applies to λ or σ

Finding Lower Bounds by Linear Programming



Such a polymatroid $\mathcal{S} = (Q, h)$ is determined by the values $h(x_0, x_1, x_2)$ with $0 \leq x_0 \leq 1$ and $0 \leq x_i \leq |P_i|$.

To compute $\kappa(\Gamma)$ we have to minimize $\max\{h(0,1,0), h(0,0,1)\}$ among all vectors $h \in \mathbb{R}^{2N_1N_2}$ satisfying

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

This can be formulated as a linear programming problem

Some Bounds

By applying these techniques, we obtain

Theorem

If $\min \Gamma = \{(x_1, y_1), (x_2, 0)\}$ *with* $x_1, x_2, y_1 > 0$, *then*

$$\kappa(\Gamma) = \sigma(\Gamma) = \lambda(\Gamma) = \frac{2(x_2 - x_1) - 1}{x_2 - x_1}.$$

In addition, by using linear programming, we determined the value of $\kappa(\Gamma)$ for several access structures with three minimal points

For future work,

Determine the values of these parameters for every bipartite access structure

Are there gaps between κ, σ, and λ
in the family of the bipartite access structures?

Duality and Minors

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

The minors of access structures are defined by the operations

$$\Gamma \setminus Z = \{A \subseteq P - Z : A \in \Gamma\} \qquad \Gamma / Z = \{A \subseteq P - Z : A \cup Z \in \Gamma\}$$

Bipartite access structures are closed by duality and minors

Theorem

If Γ' is a minor of Γ, then

$$\kappa(\Gamma') \leq \kappa(\Gamma) \qquad \sigma(\Gamma') \leq \sigma(\Gamma) \qquad \lambda(\Gamma') \leq \lambda(\Gamma)$$

Theorem (Jackson and Martin 1994,Martí-Farré and P. 2007)

For every access structure Γ,

$$\lambda(\Gamma^*) = \lambda(\Gamma) \qquad \kappa(\Gamma^*) = \kappa(\Gamma)$$

The relationship between $\sigma(\Gamma^*)$ and $\sigma(\Gamma)$ is unknown