Bounds on the Information Ratios of Secret Sharing Schemes for Close Access Structures

Oriol Farràs
Jordi Ribes–González
Sara Ricci

Universitat Rovira i Virgili, Catalonia, Spain

Workshop on Mathematics of Information–Theoretic Cryptography

Main result

The optimal information ratio of secret sharing schemes is 1-Lipschitz

Theorem

For any two Γ, Γ',

$$|\sigma(\Gamma) - \sigma(\Gamma')| \leq \mathrm{dist}(\Gamma, \Gamma')$$

where

- $\sigma(\Gamma)$ *is the optimal information ratio of* Γ
- $\mathrm{dist}(\Gamma, \Gamma') = |\Gamma \cup \Gamma'| - |\Gamma \cap \Gamma'|$

Program

1. Definition of Secret Sharing
2. Motivation and Approach
3. Main result
4. Example for $\mathrm{dist}(\Gamma, \Gamma') = 1$

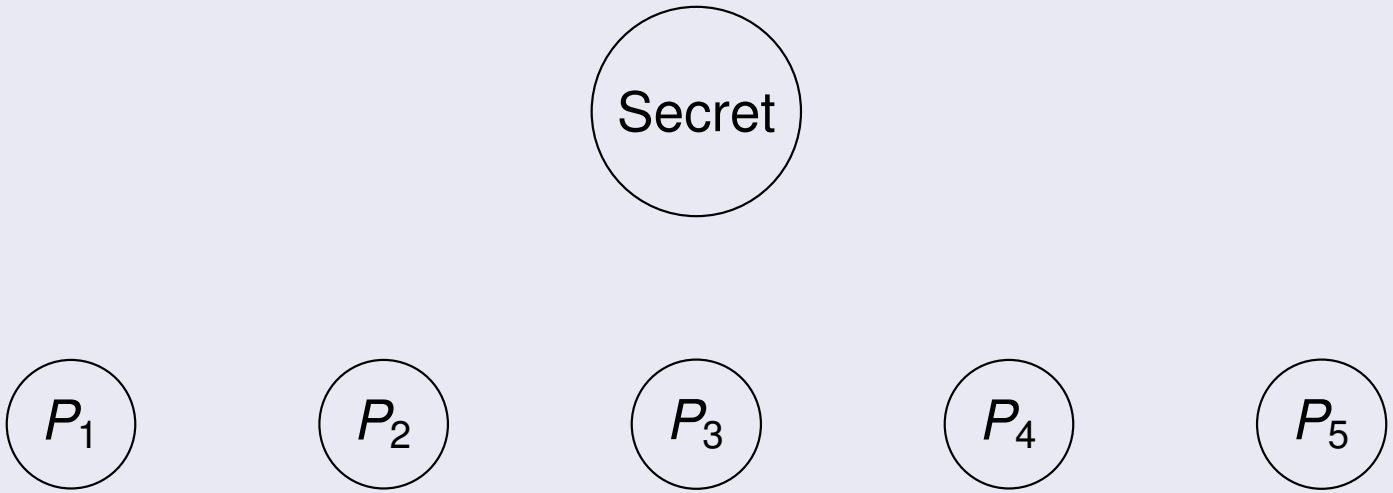
1. Definition of Secret Sharing
2. Motivation and Approach
3. Main result
4. Example for $\mathrm{dist}(\Gamma, \Gamma') = 1$

Secret Sharing Scheme

A method to protect a secret

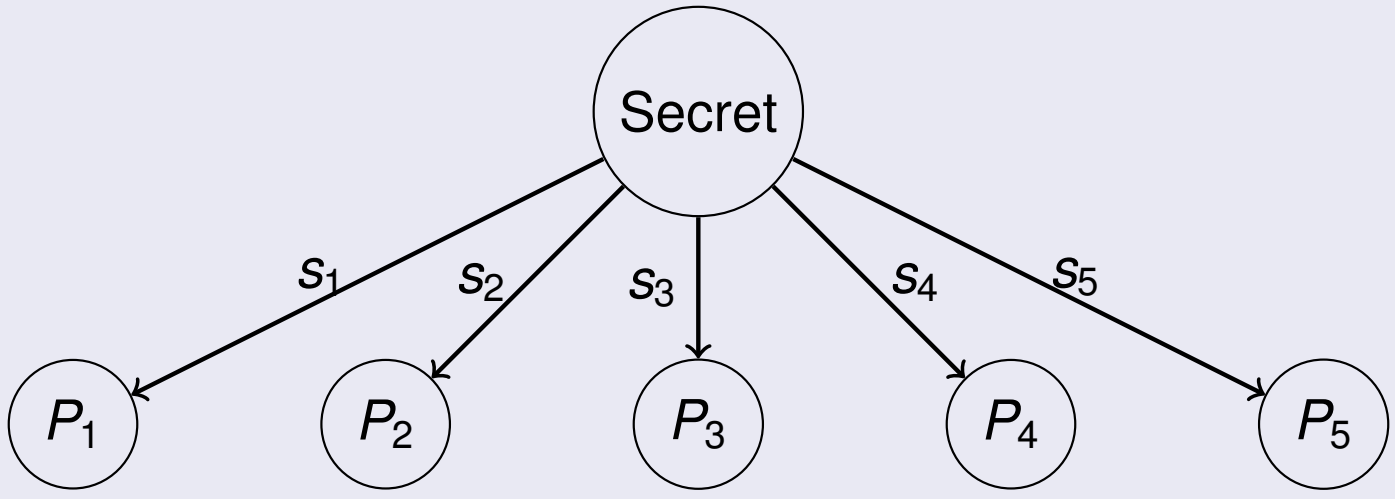
Secret Sharing Scheme

A method to protect a secret



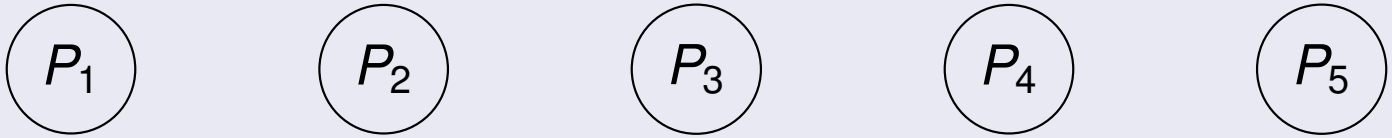
Secret Sharing Scheme

A method to protect a secret



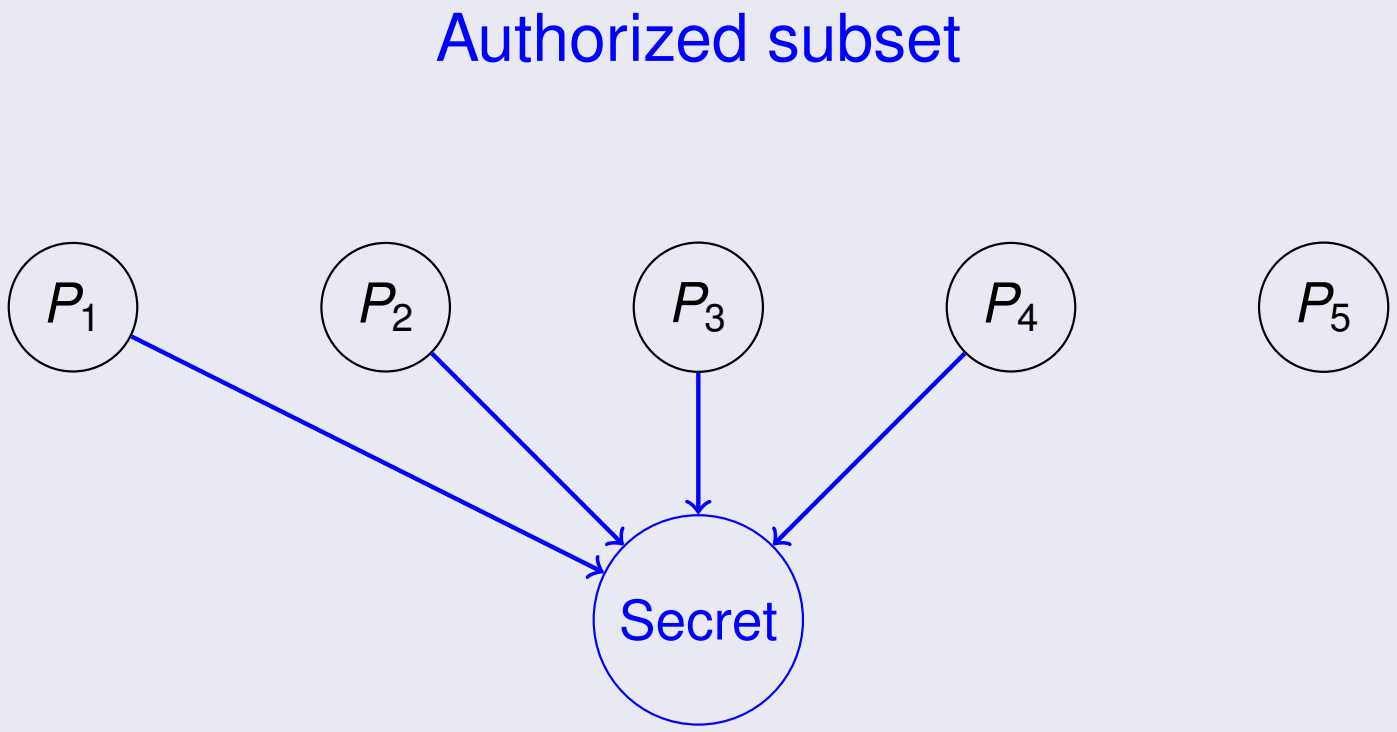
Secret Sharing Scheme

A method to protect a secret



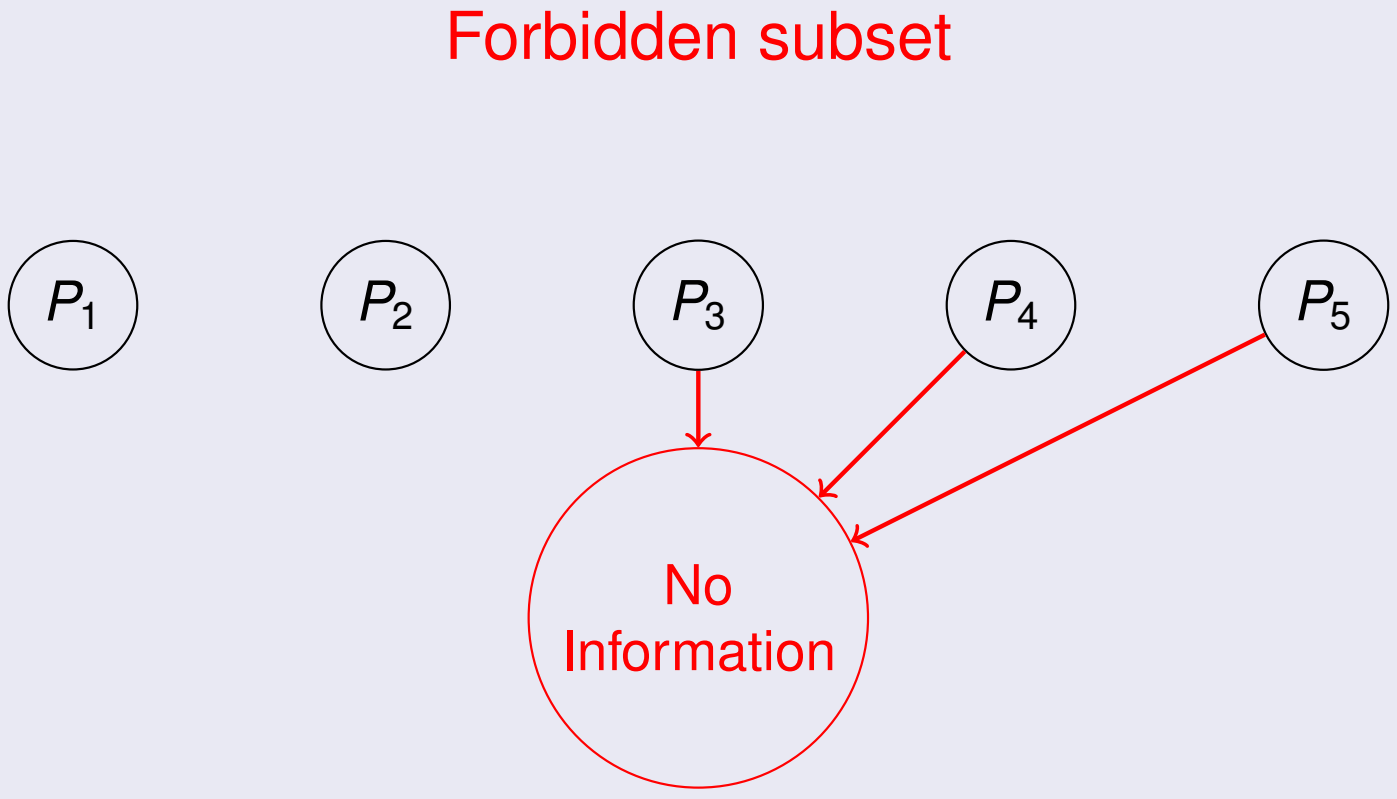
Secret Sharing Scheme

A method to protect a secret



Secret Sharing Scheme

A method to protect a secret



Secret Sharing Schemes II

- Shamir ('79), Blakley ('79), Ito, Saito, and Nishizeki ('87).
- Unconditionally secure.
- Perfect schemes: all subsets are forbidden or authorized.

- As a measure of efficiency, we consider the information ratio. For a secret sharing scheme Σ,

$$\sigma(\Sigma) = \frac{\max_i \log |S_i|}{\log |S|}.$$

  S: set of secrets
  S_i: set of shares of P_i
- For an access structure Γ, we define the optimal information ratio $\sigma(\Gamma)$ as the infimum of $\sigma(\Sigma)$ for all secret sharing schemes for Γ.

1 Definition of Secret Sharing

2 Motivation and Approach

3 Main result

4 Example for $\mathrm{dist}(\Gamma, \Gamma') = 1$

Motivation

Characterization of the access structures that admit efficient secret sharing schemes

- $\sigma(\Gamma) \geq 1$
- $\sigma(\Gamma) = 2^{O(n)}$ (Benaloh Leichter'89, Karchmer Wigderson'93 ...)
- there exists Γ with $\sigma(\Gamma) = \Omega(n/\log n)$ (Csirmaz'97)
- there exists Γ such that every linear secret sharing scheme realizing it has information ratio $2^{\Omega(n^{1/14}\log(n))}$ (Cook Pitassi Robere Rossman'16)

Find combinatorial properties of the ones admitting efficient schemes.

Known Results

For ideal access structures (the ones admitting a scheme of information ratio 1) there are important combinatorial results:

- Ideal access structures are ports of matroids (Brickell and Davenport'89)
- Ports of linear matroids admit ideal linear schemes
- If Γ is not a port of a matroid, then $\sigma(\Gamma) \geq 3/2$ (Martí-Farré, Padró'07)

Partial results for some particular families of access structures: weighted threshold (Beimel Weinreb'05), multipartite, graphs, ...

For other models of secret sharing

- Secret for NP access structures (Komargodski Naor Yogev'14)
- Secret sharing and zero knowledge proofs (Vaikuntanathan, Vasudevan'15)

Objective

Do “close" access structures have similar σ?

Positive approach: Find upper bounds on $|\sigma(\Gamma) - \sigma(\Gamma')|$ for any close Γ, Γ'.

Approach

Try to find a method such that given

- a secret sharing scheme Σ with access structure Γ, and
- an access structure Γ' that is close to Γ,

it constructs a scheme Σ' for Γ' with

$$\sigma(\Sigma') \text{ close to } \sigma(\Sigma).$$

Approach

Σ already satisfies the reconstruction conditions of most of the subsets in Γ'.

construct Σ' using Σ.

1 Definition of Secret Sharing

2 Motivation and Approach

3 Main result

4 Example for $\mathrm{dist}(\Gamma, \Gamma') = 1$

Operations

We define two operations on secret sharing schemes: $\wedge$ $\vee$.
Extension of Benaloh & Leichter operands.
Given Σ_1 and Σ_2 with the same set of secrets,

- $\Sigma_1 \vee \Sigma_2$ shares the secret s with Σ_1 and Σ_2 independently
- $\Sigma_1 \wedge \Sigma_2$ splits s into s_1 and s_2 and shares s_1 with Σ_1 and s_2 with Σ_2
- Defined for any kind of schemes

- $\Gamma(\Sigma_1 \vee \Sigma_2) = \Gamma(\Sigma_1) \cup \Gamma(\Sigma_2)$
- $\Gamma(\Sigma_1 \wedge \Sigma_2) = \Gamma(\Sigma_1) \cap \Gamma(\Sigma_2)$
- $\sigma(\Sigma_1 \vee \Sigma_2) = \sigma(\Sigma_1 \wedge \Sigma_2) \leq \sigma(\Sigma_1) + \sigma(\Sigma_2)$

Construction

Proposition

Let Γ, Γ' be two access structures. Let Σ a scheme realizing Γ. Then there exist Σ_1 and Σ_2 with

$$\sigma(\Sigma_1) + \sigma(\Sigma_2) \leq \mathrm{dist}(\Gamma, \Gamma') = |\Gamma \cup \Gamma'| - |\Gamma \cap \Gamma'|$$

satisfying that

$$\Sigma' = (\Sigma \wedge \Sigma_1) \vee \Sigma_2$$

realizes Γ'.

- Observe that $\sigma(\Sigma') \leq \sigma(\Sigma) + \mathrm{dist}(\Gamma, \Gamma')$
- If Σ is $(\mathbb{F}, \ell)$-linear, then Σ' is also $(\mathbb{F}, \ell)$-linear.

Theorem

For every Γ, Γ',

$$|\sigma(\Gamma) - \sigma(\Gamma')| \leq \mathrm{dist}(\Gamma, \Gamma')$$

Details

Theorem

For every Γ, Γ',

$$|\sigma(\Gamma) - \sigma(\Gamma')| \leq \mathrm{dist}(\Gamma, \Gamma')$$

Theorem

The optimal information ratio is 1-Lipschitz

A function $f : X \to Y$ is k-Lipschitz if for every $x, y \in X$,

$$\mathrm{dist}_Y(f(x), f(y)) \leq k \cdot \mathrm{dist}_X(x, y)$$

Details

Theorem

For every Γ, Γ',

$$|\sigma(\Gamma) - \sigma(\Gamma')| \leq \mathrm{dist}(\Gamma, \Gamma')$$

- Also valid if we restrict ourselves to $(\mathbb{F}, \ell)$-linear schemes, for any $\mathbb{F}$ and ℓ
- Also valid if we restrict to the size of the secret (e.g. for sharing one bit)
- Combinatorial nature (later more details).
- 1 is the Lipschitz norm of σ: σ is not $(1 - \delta)$-Lipschitz for any $\delta > 0$

Main result

Theorem

For any two Γ, Γ',

$$|\sigma(\Gamma) - \sigma(\Gamma')| \leq \mathrm{dist}(\Gamma, \Gamma')$$

- In the space of access structures, we have “hard" regions and “easy" regions.

$\Rightarrow$ if Γ admits an efficient scheme, then the close access structures also admit efficient schemes.

$\Rightarrow$ if Γ require large shares, then the close access structures also require large shares

- the proof is constructive
- we find similar properties for other computation models and for bounds on σ.
- MPC, ABE.

Other models of computation

- The main result is of combinatorial nature. We can extend it to other models of computation:
  - Montone Boolean formulas
  - Monotone Boolean circuits
  - Monotone span programs

Theorem

For every two monotone Boolean functions $F, G : \{0,1\}^n \to \{0,1\}$,

$$|L(F) - L(G)| \leq n \cdot \mathrm{dist}(F^{-1}(1), G^{-1}(1)),$$

where L is the total size of the shortest formula.

Methods for bounding the information ratio bounds

We study the behaviour of the most common techniques for bounding σ in order to understand their limitations.

κ: bound on σ when applying Shannon inequalities to the entropy of the shares and the secret

- $\kappa(\Gamma) \leq \sigma(\Gamma)$ for every Γ
- Most common bound in secret sharing
- Connection with polymatroids and linear programming (Csirmaz'98)

Theorem

For every Γ, Γ', $|\kappa(\Gamma) - \kappa(\Gamma')| \leq \mathrm{dist}(\Gamma, \Gamma')$

We also analyzed Razborov bound ('90) and Subcritical families technique (Beimel, Gál, Paterson' 95) for linear schemes, and they have different behaviours.

1 Definition of Secret Sharing

2 Motivation and Approach

3 Main result

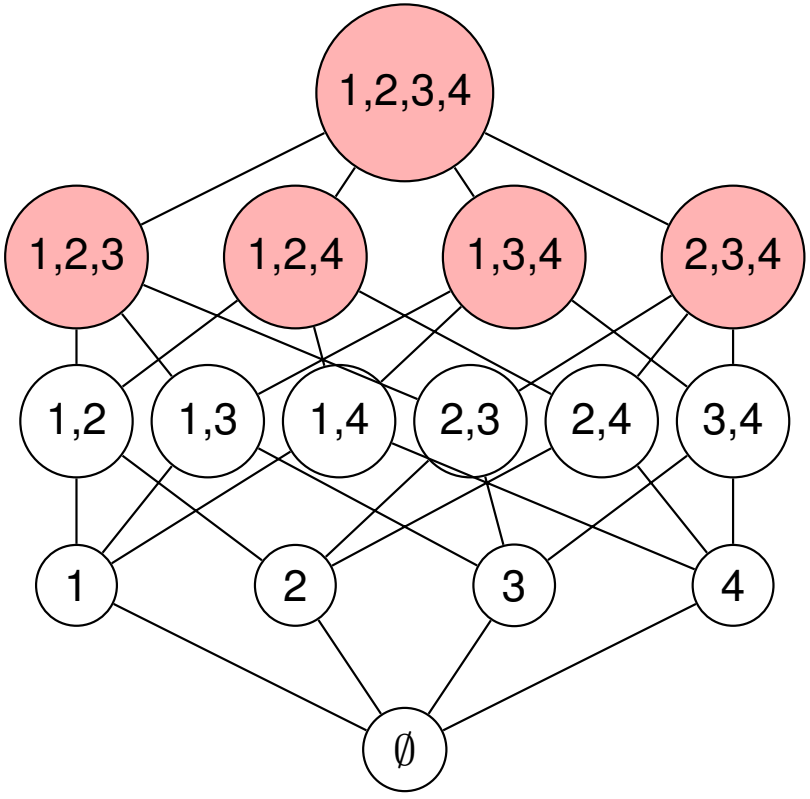
4 Example for $\mathrm{dist}(\Gamma, \Gamma') = 1$

Adding subsets

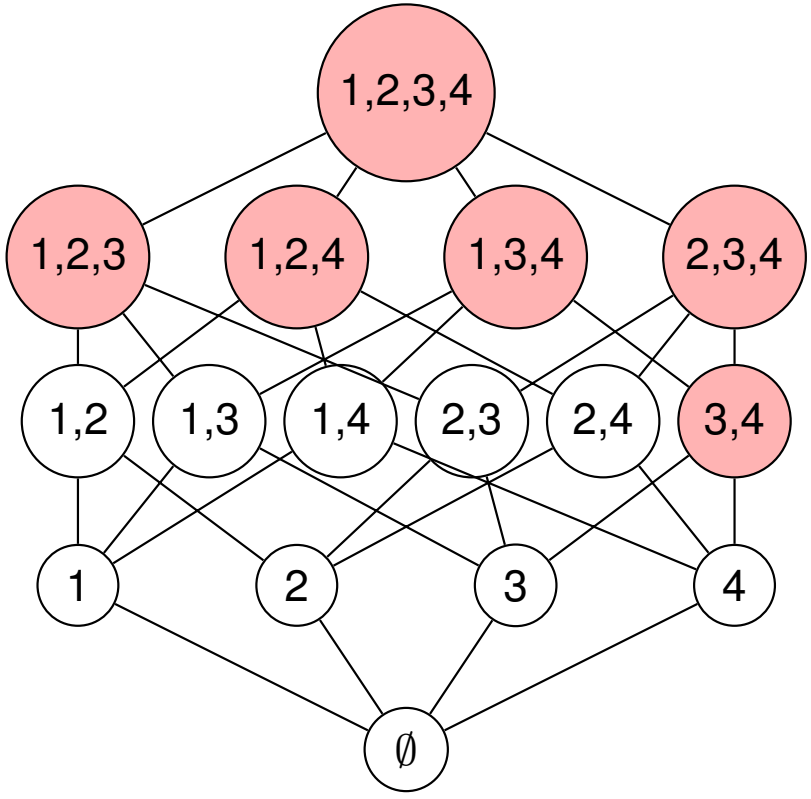
- Let Σ be a secret sharing scheme for Γ.
- Let $\Gamma' = \Gamma \cup \{A\}$ be an access structure.
- How can we construct a scheme for Γ'?

Adding subsets (I)

Γ



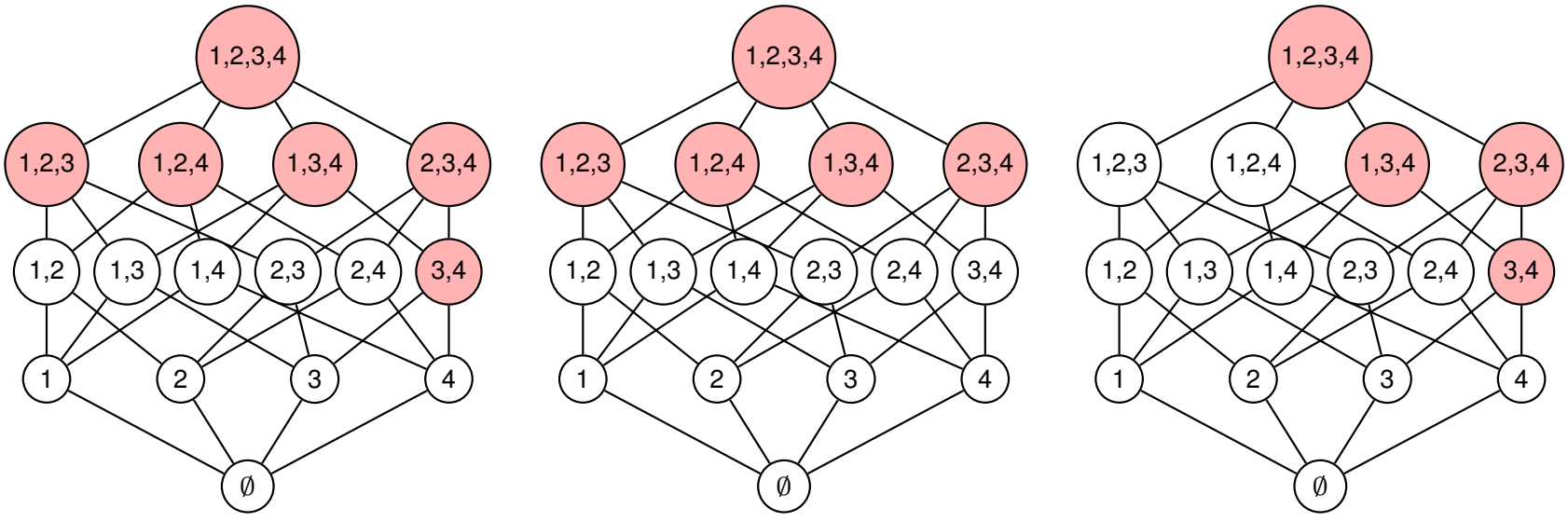
Γ'



$$\Gamma' = \Gamma \cup \{3, 4\}$$

Adding subsets (II)

Γ' Γ $\Gamma'' = \mathrm{cl}(\{3,4\})$



$\Gamma' = \Gamma \cup \Gamma''$, and Γ'' admits a scheme Σ'' with $\sigma(\Sigma'') = 1$

$\Sigma' = \Sigma \vee \Sigma''$ satisfies $\sigma(\Sigma') = \sigma(\Sigma) + 1$

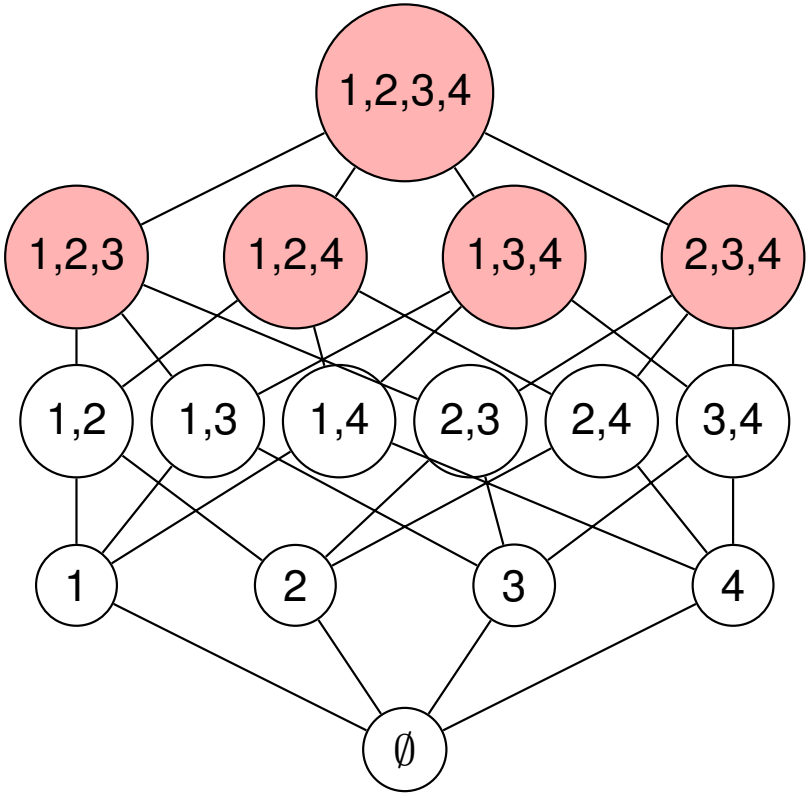
Adding subsets is easy. What about deleting subsets?

Deleting subsets

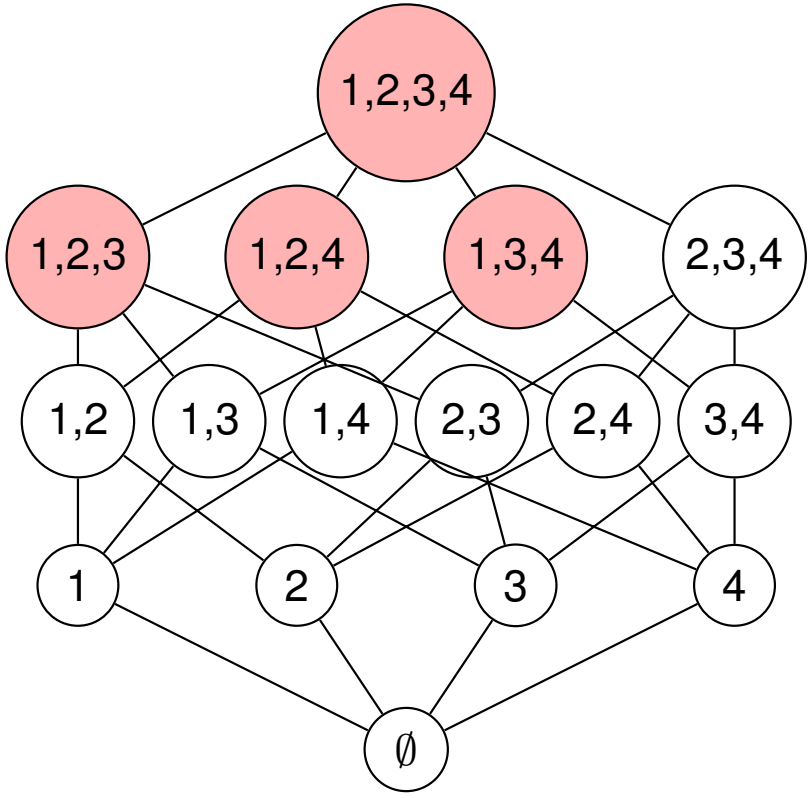
- Let Σ be a secret sharing scheme for Γ.
- Let $\Gamma' = \Gamma \setminus \{A\}$ be an access structure.
- How can we construct a scheme for Γ'?

Deleting subsets

Γ

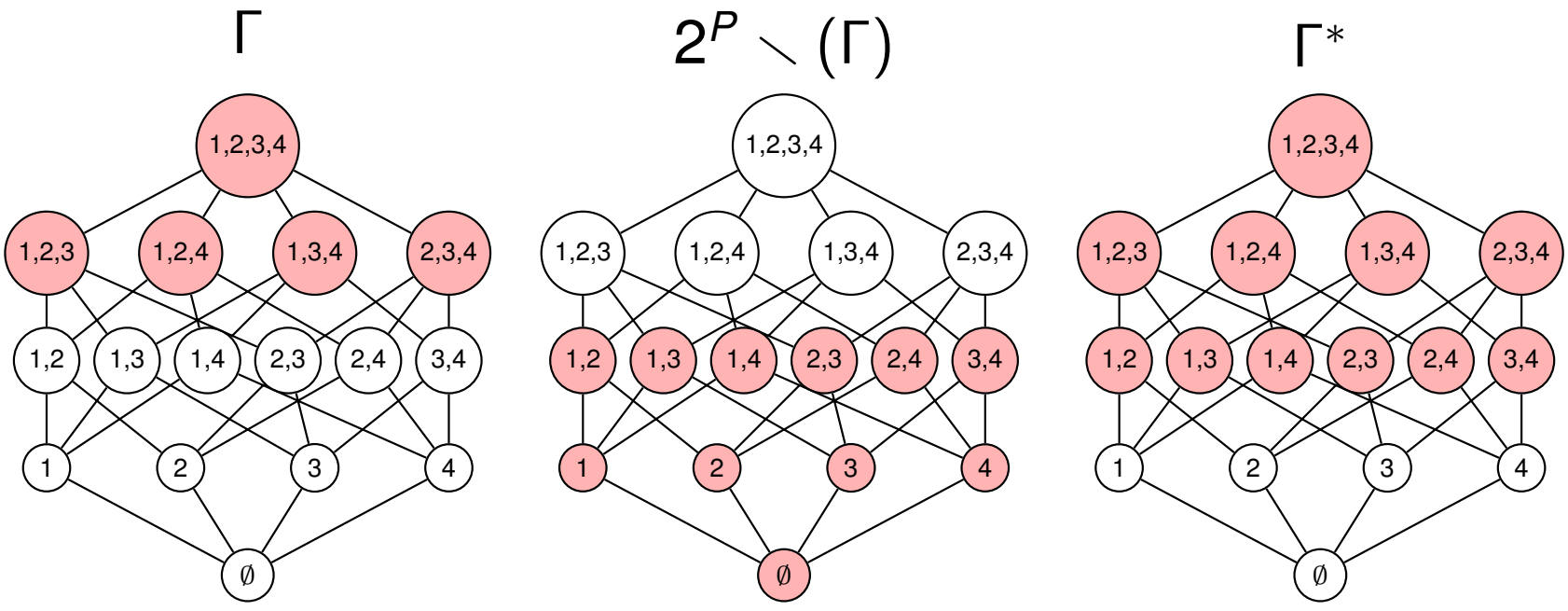


Γ'



$$\Gamma' = \Gamma \setminus \{2, 3, 4\}$$

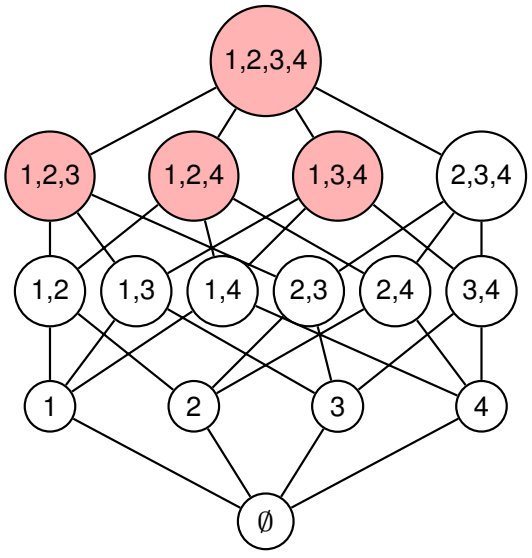
The dual of Γ



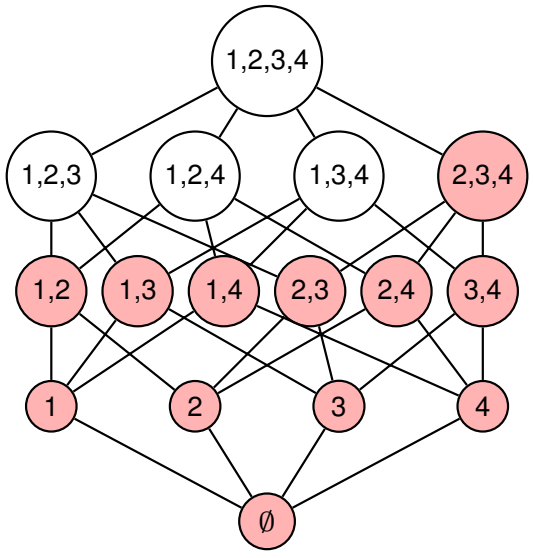
$$\Gamma^* = \{P \setminus B : B \notin \Gamma\}$$

The dual of Γ'

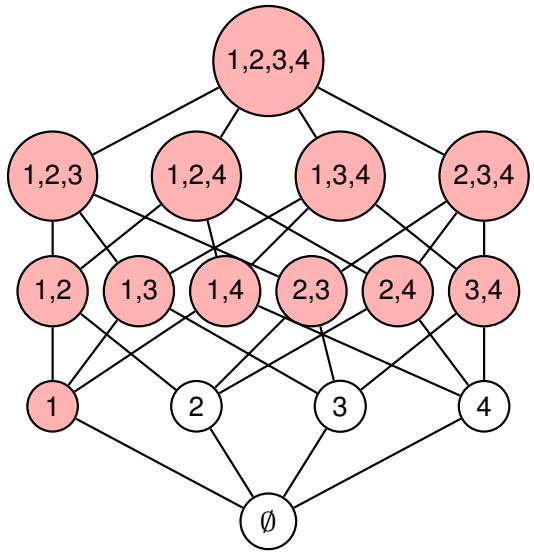
Γ'



$2^P \setminus (\Gamma')$



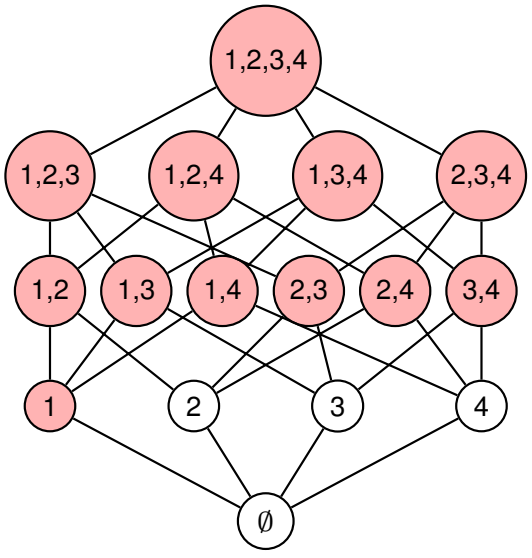
$(\Gamma')^*$



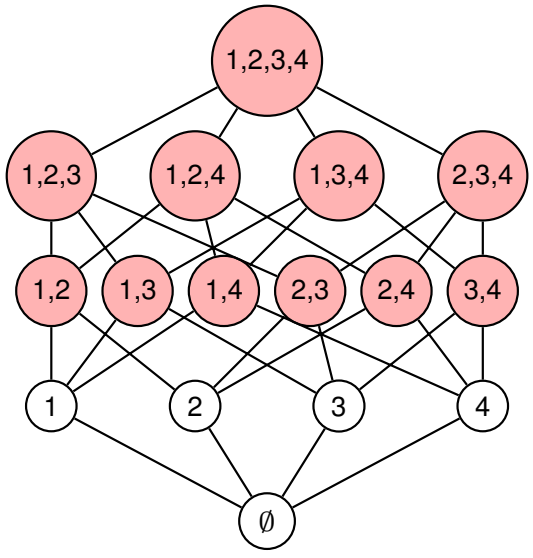
$$(\Gamma')^* = \{P \setminus B : B \notin \Gamma'\}$$

The Construction

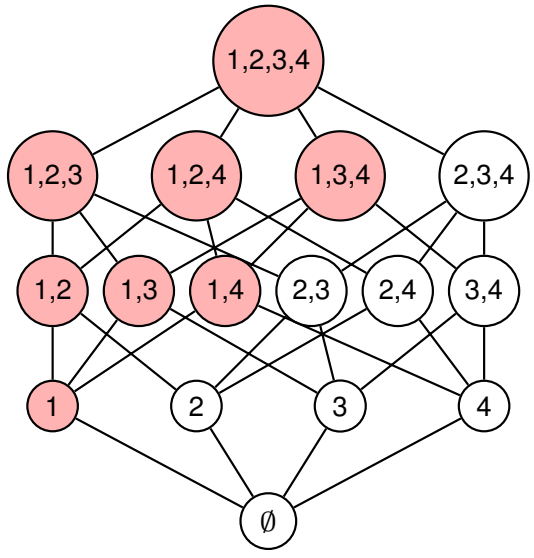
$(\Gamma')^*$



Γ^*



$\Gamma'' = \mathrm{cl}(\{1\})$



Since $(\Gamma')^* = \Gamma^* \cup \Gamma''$,

$$\Gamma' = (\Gamma')^{**} = (\Gamma^* \cup \Gamma'')^* = \Gamma^{**} \cap (\Gamma'')^* = \Gamma \cap (\Gamma'')^*$$

$(\Gamma'')^*$ admits a scheme Σ''^* with $\sigma(\Sigma''^*) = 1$, so

$$\Sigma' = \Sigma \wedge \Sigma''^* \text{ satisfies } \sigma(\Sigma') = \sigma(\Sigma) + 1$$

Deleting subsets

Beimel F. Minsk'12, Beimel F. Peter'16 study another problem:

- Let Σ be a secret sharing scheme for Γ.
- Let Γ' be an access structure with $\min\Gamma' \subseteq \min\Gamma$.
- How can we construct a scheme for Γ'?
- Good bounds for $\min\Gamma \subseteq \binom{P}{k}$ with $k \ll n$.

Complementary results, they cannot be compared:
$\mathrm{dist}(\Gamma, \Gamma')$ can be exponential on n even if $\mathrm{dist}(\min\Gamma, \min\Gamma') = 1$.

Conclusions and open problems

Theorem

For every Γ, Γ', $|\sigma(\Gamma) - \sigma(\Gamma')| \leq \mathrm{dist}(\Gamma, \Gamma')$

We prove that for $\mathrm{dist}(\Gamma, \Gamma') = 1$ we cannot improve the bound.

- what about for $\mathrm{dist}(\Gamma, \Gamma') > 1$?
- problem: we only know the exact value of σ for some access structures.

Theorem

For every Γ, Γ', $|\kappa(\Gamma) - \kappa(\Gamma')| \leq \mathrm{dist}(\Gamma, \Gamma')$

- Implications in information theory
- what about using non-Shannon inequalities?

Thank you

Available at https://eprint.iacr.org/2016/726