How to Use Undiscovered Information Inequalities: Direct Applications of the Copy Lemma.

Emirhan Gürpınar (ENS de Lyon) and Andrei Romashchenko (LIRMM)

July 09, IEEE ISIT 2019

The talk in two phrases:

To apply new non-Shannon type inequalities you do not need to prove them.

Toy example: secret sharing on the Vámos matroid.

General definition of secret sharing

- secret S_0 (e.g., uniformly distributed on $\{0,1\}^k$)
- n participants
- **access structure**: a family of authorized groups $C_1, \ldots, C_m$

General definition of secret sharing

- secret S_0 (e.g., uniformly distributed on $\{0,1\}^k$)
- n participants
- **access structure**: a family of authorized groups $C_1, \ldots, C_m$

perfect secret sharing scheme: a distribution $(S_0, S_1, \ldots, S_n)$ such that

- a collection of shares S_i from each authorized group gives **all** information on S_0
- a collection of shares S_i from any *non-authorized* group gives **no** information on S_0

Secret sharing for n participants

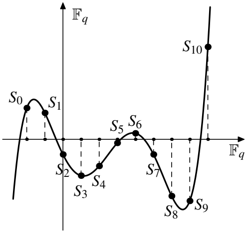
secret key: S_0 uniformly distributed on $\{0,1\}^k$

Standard example:

- any group of $\geq t$ participants knows the secret
- any group of $< t$ participants know nothing about the secret

Classical solution (Shamir scheme):

- fix points $x_0, x_1, \ldots, x_n$ in $\mathbb{F}_{2^k}$ (public information)
- choose a secret random polynomial $Q(x)$ of degree $\leq t-1$
- the i-th participant obtains $S_i = Q(x_i)$, $i = 1, \ldots, n$
- let the **secret** $S_0 = Q(x_0)$



Secret sharing for n participants

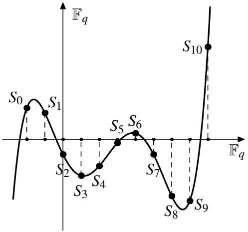
secret key: S_0 uniformly distributed on $\{0,1\}^k$

Standard example:

- any group of $\geq t$ participants knows the secret
- any group of $< t$ participants know nothing about the secret

Classical solution (Shamir scheme):

- fix points $x_0, x_1, \ldots, x_n$ in $\mathbb{F}_{2^k}$ (public information)
- choose a secret random polynomial $Q(x)$ of degree $\leq t-1$
- the i-th participant obtains $S_i = Q(x_i)$, $i = 1, \ldots, n$
- let the **secret** $S_0 = Q(x_0)$



Given $\geq t$ pairs $(x_i, Q(x_i))$ we reconstruct $Q(x)$ and S_0.

Secret sharing for n participants

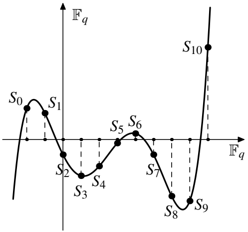
secret key: S_0 uniformly distributed on $\{0,1\}^k$

Standard example:

- any group of $\geq t$ participants knows the secret
- any group of $< t$ participants know nothing about the secret

Classical solution (Shamir scheme):

- fix points $x_0, x_1, \ldots, x_n$ in $\mathbb{F}_{2^k}$ (public information)
- choose a secret random polynomial $Q(x)$ of degree $\leq t-1$
- the i-th participant obtains $S_i = Q(x_i)$, $i = 1, \ldots, n$
- let the **secret** $S_0 = Q(x_0)$



Given $< t$ pairs $(x_i, Q(x_i))$ we know nothing about S_0:
all values of S_0 remain **possible** and even **equiprobable**.

Computing the information ratio

Information ratio of a secret sharing scheme: $\frac{\max H(S_i)}{H(S_0)}$.

Fundamental problem: minimize information ratio for a given access structure.

Computing the information ratio

Information ratio of a secret sharing scheme: $\frac{\max H(S_i)}{H(S_0)}$.

Fundamental problem: minimize information ratio for a given access structure.

Very simple example:

- 4 participants
- **minimal** authorized groups:
  $\{1, 2\}$, $\{2, 3\}$, $\{3, 4\}$

Question: What is the optimal information ratio for this access structure?

There is a simple construction with information ratio $= 3/2$.

Shannon's inequalities $\Longrightarrow$ we cannot do better.

Computing the information ratio

Very simple example:

- 4 participants
- **minimal** authorized groups:
  $\{1,2\}$, $\{2,3\}$, $\{3,4\}$

Question: What is the optimal information ratio for this access structure?

Shannon's inequalities: information ratio $\geq 3/2$.

Computer-assisted proof:

- write down all equations that define the access structure
- write down all *basic inequalities* for Shannon's entropy of $(S_0, S_1, S_2, S_3, S_4)$
- write that $H(S_i) \leq T$ for $i = 1, 2, 3, 4$
- ask your favorite **linear programming solver** to find $\min(T)$

The answer: minimal $T = (3/2)H(S_0)$.

Ideal secret sharing: from linear structures to matroids

Ideal secret sharing scheme: information ratio $= 1$.

usual examples of ideal secret sharing: linear schemes / linear access structures

Linear access structure: there is a family of vectors $\mathbf{v}_0, \mathbf{v}_1 \ldots, \mathbf{v}_s$ such that

$\{i_1, \ldots, i_s\}$ **know the secret** IFF $\mathbf{v}_0$ is in the span of $\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_s}$.

Ideal secret sharing: from linear structures to matroids

Matroid on the *ground set* U: a function rk on subsets of U such that

- $\mathrm{rk}(A)$ is a non negative integer
- $\mathrm{rk}(A) \leq |A|$
- $\mathrm{rk}(A \cup \{x\}) \leq \mathrm{rk}(A) + 1$
- $\mathrm{rk}(A) \leq \mathrm{rk}(A \cup B)$
- $\mathrm{rk}(A \cup B \cup C) + \mathrm{rk}(C) \leq \mathrm{rk}(A \cup C) + \mathrm{rk}(B \cup C)$

Examples: vector matroids; graphic matroids; algebraic matroid...

Ideal secret sharing: from linear structures to matroids

Matroid on the *ground set* U: a function rk on subsets of U such that

- $\mathrm{rk}(A)$ is a non negative integer
- $\mathrm{rk}(A) \leq |A|$
- $\mathrm{rk}(A \cup \{x\}) \leq \mathrm{rk}(A) + 1$
- $\mathrm{rk}(A) \leq \mathrm{rk}(A \cup B)$
- $\mathrm{rk}(A \cup B \cup C) + \mathrm{rk}(C) \leq \mathrm{rk}(A \cup C) + \mathrm{rk}(B \cup C)$

Examples: vector matroids; graphic matroids; algebraic matroid...

An access structure on a matroid: the *ground set* is the set of participants, and

$i_1, \ldots, i_s$ **know the secret** IFF adding $\mathbf{v}_0$ to $\{\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_s}\}$ preserves the rank

matroids and ideal secret sharing

[Brickell–Davenport]: The access structure of every ideal secret sharing scheme can be defined on a matroid.

Natural conjecture: For every access structure on a matroid there is an ideal secret sharing scheme

matroids and ideal secret sharing

[Brickell–Davenport]: The access structure of every ideal secret sharing scheme can be defined on a matroid.

Natural conjecture: For every access structure on a matroid there is an ideal secret sharing scheme

The conjecture looks plausible: This is true for **linear** access structures.

very plausible: Shannon's inequalities cannot disprove it.

matroids and ideal secret sharing

[Brickell–Davenport]: The access structure of every ideal secret sharing scheme can be defined on a matroid.

Natural conjecture: For every access structure on a matroid there is an ideal secret sharing scheme

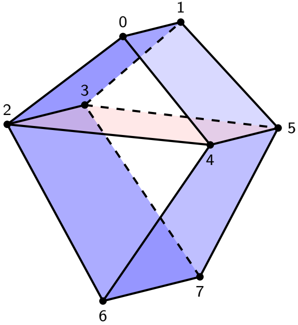
The conjecture looks plausible: This is true for **linear** access structures.

very plausible: Shannon's inequalities cannot disprove it.

But there is a counter-example [Seymour]: Vámos matroid

Vámos matroid

ground set $= \{0, 1, 2, 3, 4, 5, 6, 7\}$



$\mathrm{rk}(\text{one point}) = 1$

$\mathrm{rk}(\text{two points}) = 2$

$\mathrm{rk}(\text{three points}) = 3$

$\mathrm{rk}(\{0, 1, 2, 3\}) = \mathrm{rk}(\{0, 1, 4, 5\}) = \mathrm{rk}(\{2, 3, 6, 7\}) = \mathrm{rk}(\{4, 5, 6, 7\}) = \mathrm{rk}(\{2, 3, 4, 5\}) = 3$

$\mathrm{rk}(\text{other sets}) = 4$

Our toy problem: secret sharing on Vámos matroid

upper bound: information ratio $\leq 4/3$

lower bound:

Seymour 1992	> 1
Beimel–Livne 2006	$\geq 1 + \Omega(1/\sqrt{k})$ for a secret of size k
Beimel–Livne–Padro 2008	$\geq 11/10$
Metcalf-Burton 2011	$\geq 9/8 = 1.125$
Hadian 2013	$\geq 67/59 \approx 1.135593$
Farràs–Kaced–Martín–Padró 2018	$\geq 33/29 \approx 1.137931$
this talk	$\geq 561/491 \approx 1.142566$

Our toy problem: secret sharing on Vámos matroid

upper bound: information ratio $\leq 4/3$

lower bound:

Seymour 1992	> 1
Beimel–Livne 2006	$\geq 1 + \Omega(1/\sqrt{k})$ for a secret of size k
Beimel–Livne–Padro 2008	$\geq 11/10$
Metcalf-Burton 2011	$\geq 9/8 = 1.125$
Hadian 2013	$\geq 67/59 \approx 1.135593$
Farràs–Kaced–Martín–Padró 2018	$\geq 33/29 \approx 1.137931$
this talk	$\geq 561/491 \approx 1.142566$

Our bound follows from new (unknown!) inequalities for Shannon's entropy.
They still remain undiscovered, but we have already applied them.

Classical approach

Write a **linear program** as follows.

Constraints:

- equations from the definition of a **perfect secret sharing**
- all **Shannon-type** inequalities for entropy, $I(* : * \mid *) \geq 0$
- (optional) symmetry conditions

Objective function:

minimize $\left[\max_i \frac{H(\text{secret share}_i)}{H(\text{secret})} \right]$

Classical approach

Write a **linear program** as follows.

Constraints:

- equations from the definition of a **perfect secret sharing**
- all **Shannon-type** inequalities for entropy, $I(* : * \,|\, *) \geq 0$
- (optional) symmetry conditions

Objective function:

minimize $\Big[\max\limits_i \frac{H(\text{secret share}_i)}{H(\text{secret})}\Big]$

Answer: **trivial**, information ratio ≥ 1

Modern approach

Write a **linear program** as follows

Constraints:

- equations from the definition of a **perfect secret sharing**
- all **Shannon-type** inequalities $I(* : * \mid *) \geq 0$
- some **known non-Shannon-type** inequalities
- (optional) symmetry conditions

Objective function:

minimize $\left[\max_i \frac{H(\text{secret share}_i)}{H(\text{secret})} \right]$

Modern approach

Write a **linear program** as follows

Constraints:

- equations from the definition of a **perfect secret sharing**
- all **Shannon-type** inequalities $I(* : * \mid *) \geq 0$
- some **known non-Shannon-type** inequalities
- (optional) symmetry conditions

Objective function:

minimize $\left[\max_i \frac{H(\text{secret share}_i)}{H(\text{secret})} \right]$

Answer: some non-trivial bounds!
[Beimel-Livne-Padro 2008], [Metcalf-Burton 2011], [Hadian 2013]

PostModern approach

Write a **linear program** as follows

Constraints:

- equations from the definition of a **perfect secret sharing**
- all **Shannon-type** inequalities $I(* : * \mid *) \geq 0$
- ~~some **known non-Shannon-type** inequalities~~
- new variables and constraints borrowed from proofs of non-Shannon-type inequalities
- (optional) symmetry conditions

Objective function:

minimize $\left[\max_i \frac{H(\text{secret share}_i)}{H(\text{secret})}\right]$

PostModern approach

Write a **linear program** as follows

Constraints:

- equations from the definition of a **perfect secret sharing**
- all **Shannon-type** inequalities $I(* : * \mid *) \geq 0$
- ~~some **known non-Shannon-type** inequalities~~
- new variables and constraints borrowed from proofs of non-Shannon-type inequalities
- (optional) symmetry conditions

Objective function:

minimize $\left[\max_i \frac{H(\text{secret share}_i)}{H(\text{secret})} \right]$

Answer: [Farràs-Kaced-Martín-Padró 2018] and this paper

PostModern approach

Write a **linear program** as follows

Constraints:

- equations from the definition of a **perfect secret sharing**
- all **Shannon-type** inequalities $I(* : * \,|\, *) \geq 0$
- ~~some **known non-Shannon-type** inequalities~~
- oversimplified technical explanation:
  make **clones** of (S_0, S_1, S_6, S_7) conditional on (S_2, S_3, S_4, S_5) (twice!)
- (optional) symmetry conditions

Objective function:

minimize $\left[\max_i H(\text{secret share}_i)\right]$

Answer: information ratio $\geq 561/491 \approx 1.142566$

Modern approach vs. PostModern approach

Modern approach:

Stage 1: computer-aided search of non-Shannon type inequalities
[**cloning (Copy Lemma)** + linear programming]

Stage 2: computer-aided linear programming for secret sharing involving inequalities found on **Stage 1**

PostModern approach:

One Shot: computer-aided linear programming for a secret sharing problem involving **cloning**

Modern approach vs. PostModern approach

Modern approach:

Stage 1: computer-aided search of non-Shannon type inequalities [**cloning (Copy Lemma)** + linear programming]

Stage 2: computer-aided linear programming for secret sharing involving inequalities found on **Stage 1**

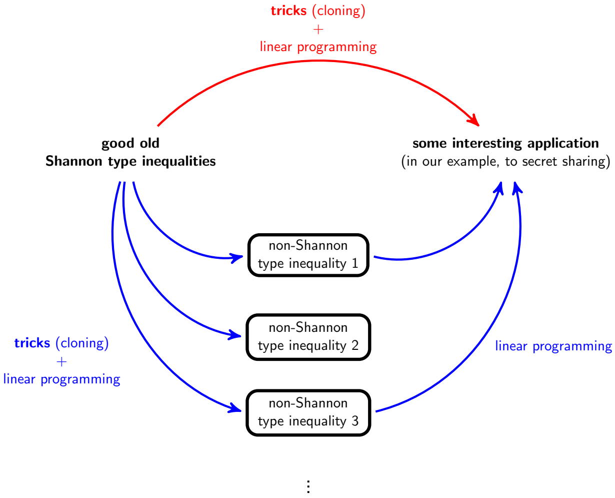
PostModern approach:

One Shot: computer-aided linear programming for a secret sharing problem involving **cloning**

Remark 1: $\frac{\text{this work}}{\text{Farràs–Kaced–Martín–Padró}} = \frac{\text{copy lemma + symmetries}}{\text{Ahlswde–Körner lemma}}$

Remark 2: This technique gives a “cheap” proof of the previously known bound for the Ingleton score.

In one picture: our technique vs. usual technique



Questions?