Secret Sharing and Information Inequalities

Tarik Kaced

Post-doctoral fellow at the Institute of Network Coding
The Chinese University of Hong Kong

February 27, 2013

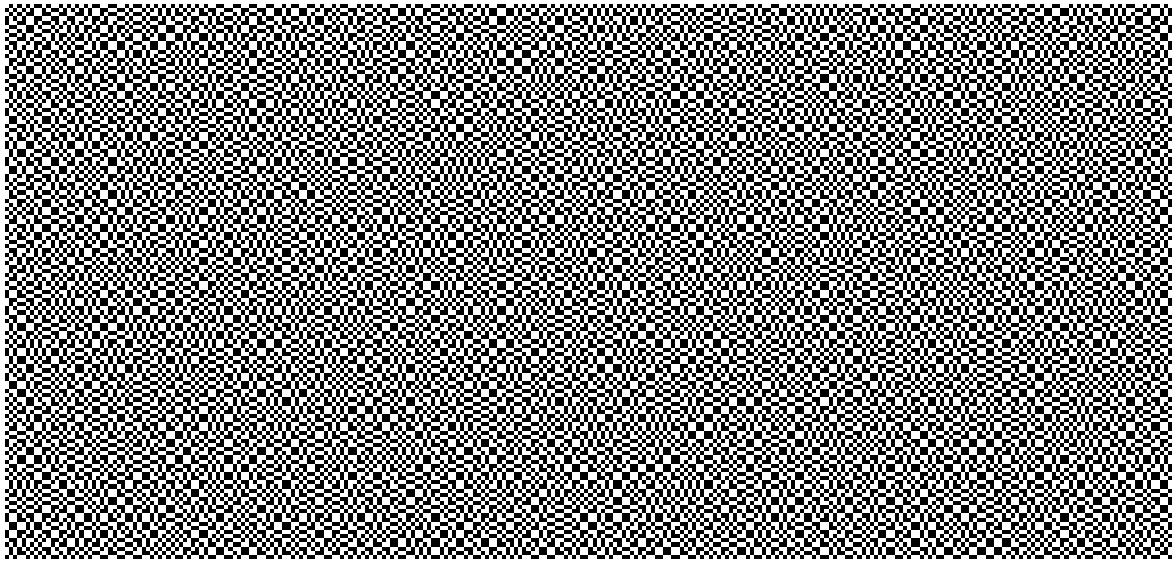
香港中文大學
The Chinese University of Hong Kong

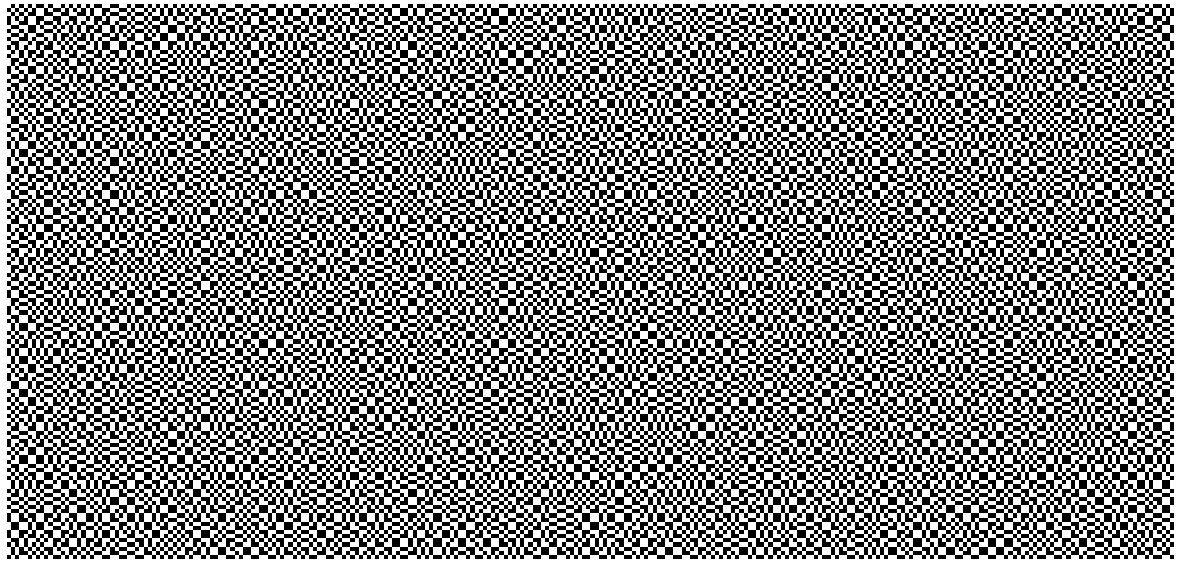
What is this talk about ?

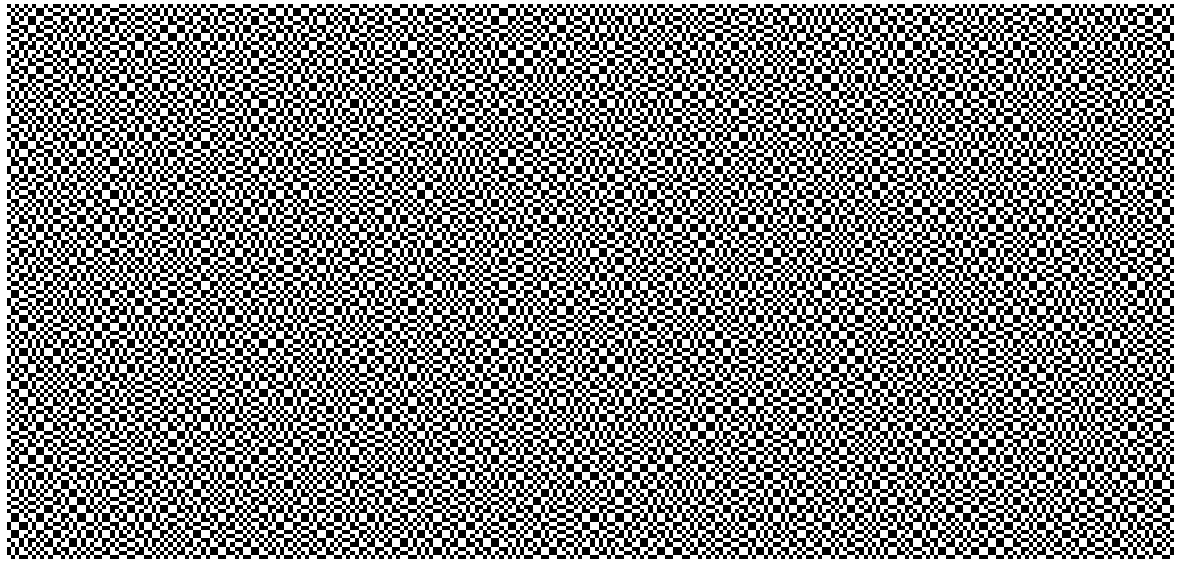
... why, information inequalities and secret sharing, of course!

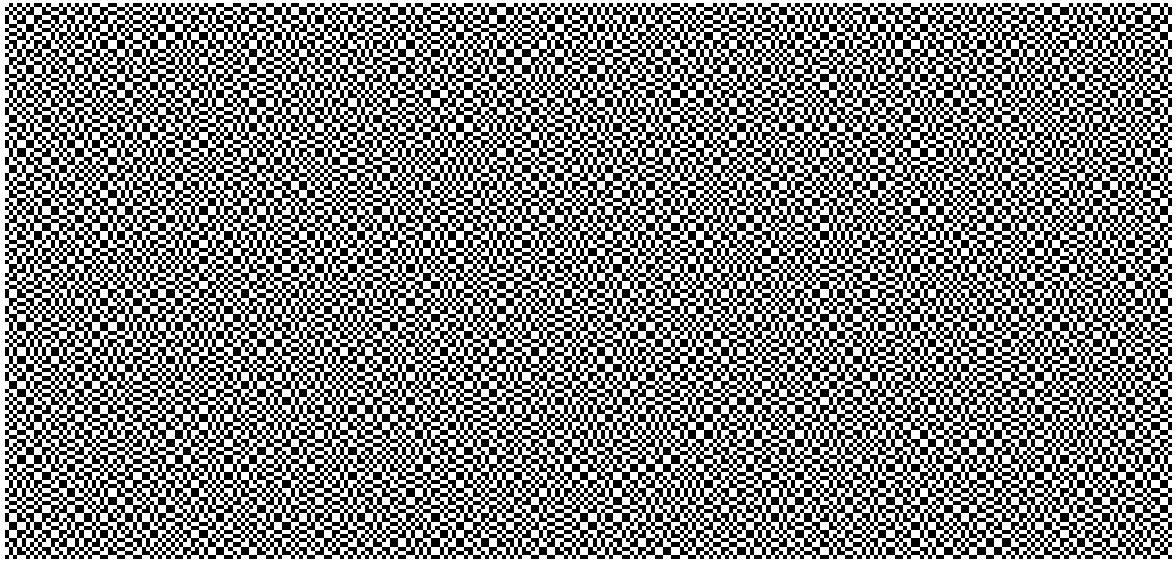
1. **Secret Sharing**
2. **Quasi-perfect Secret Sharing**
3. **Information Inequalities**
4. **Essentially Conditional Inequalities**
5. **Information Inequalities and Secret Sharing**
6. **Prospects & Open Questions**

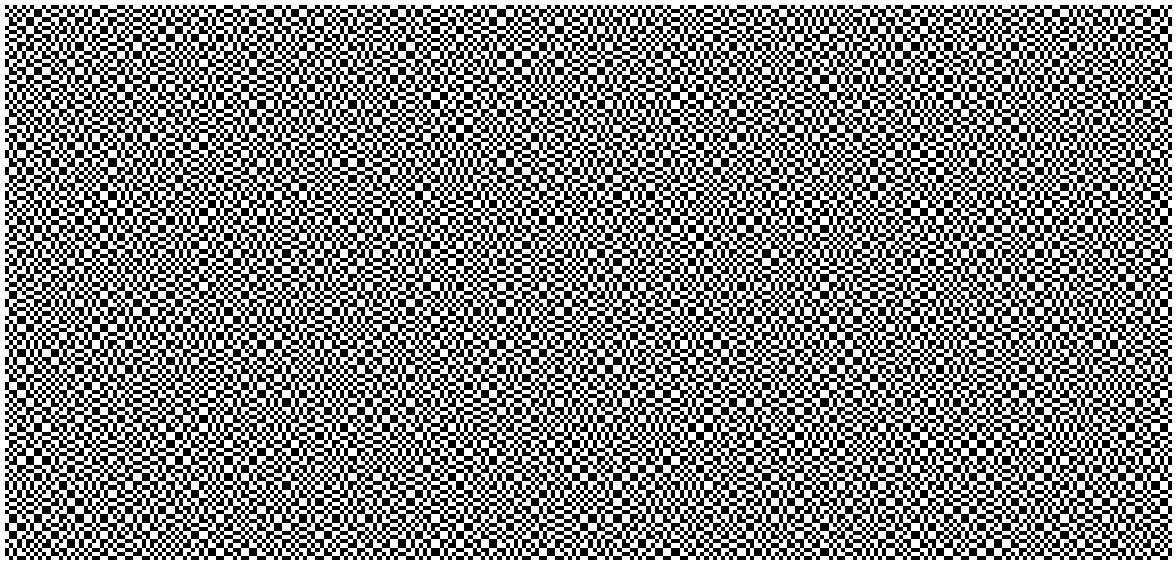
Secret Sharing

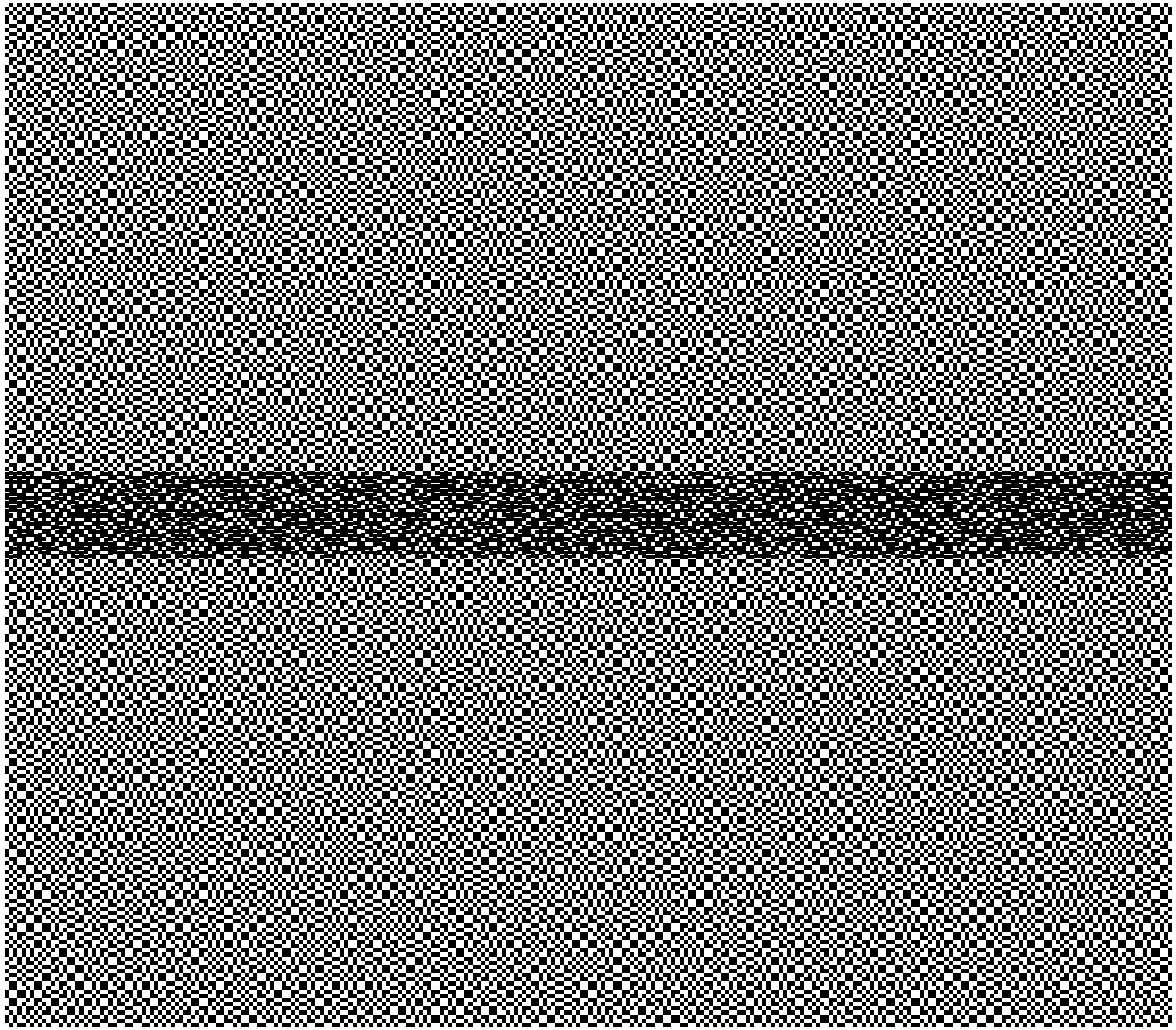


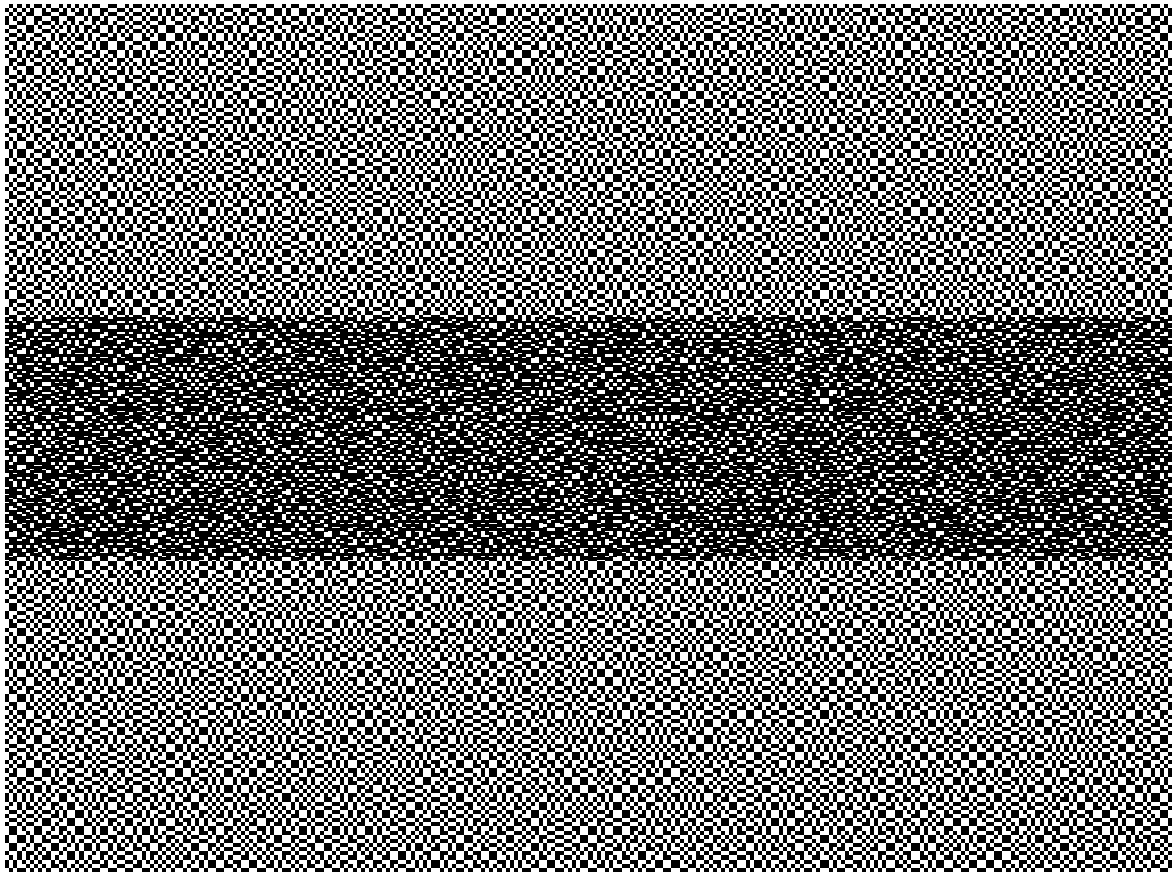


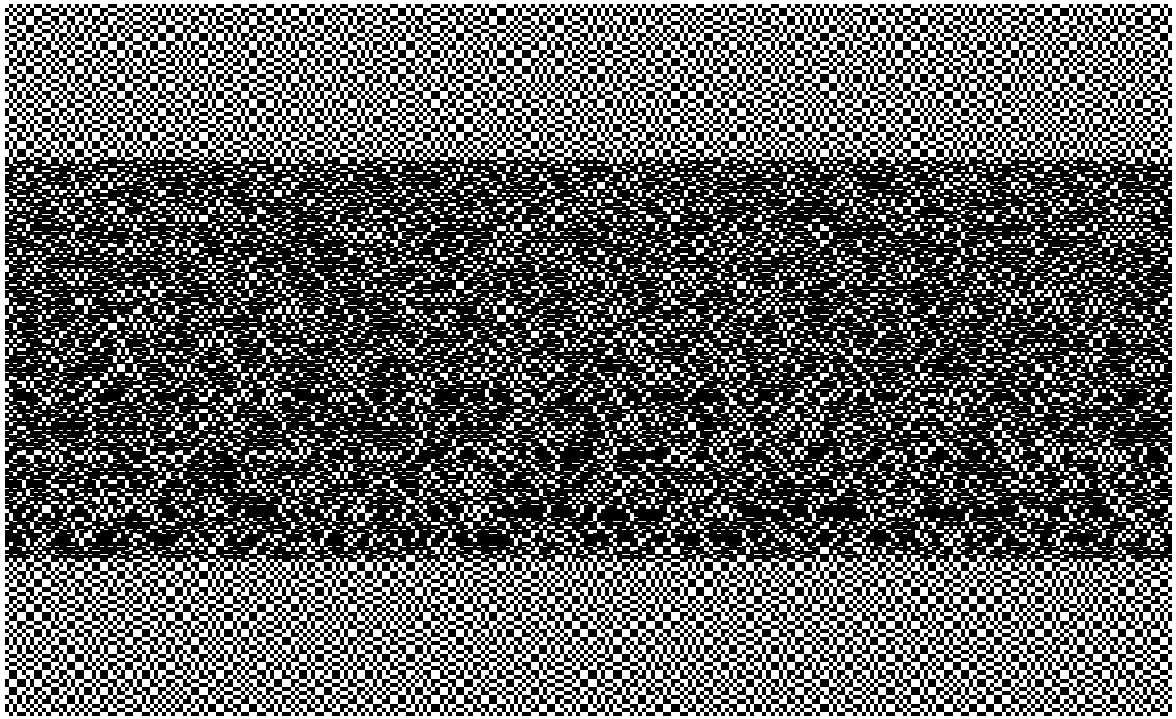


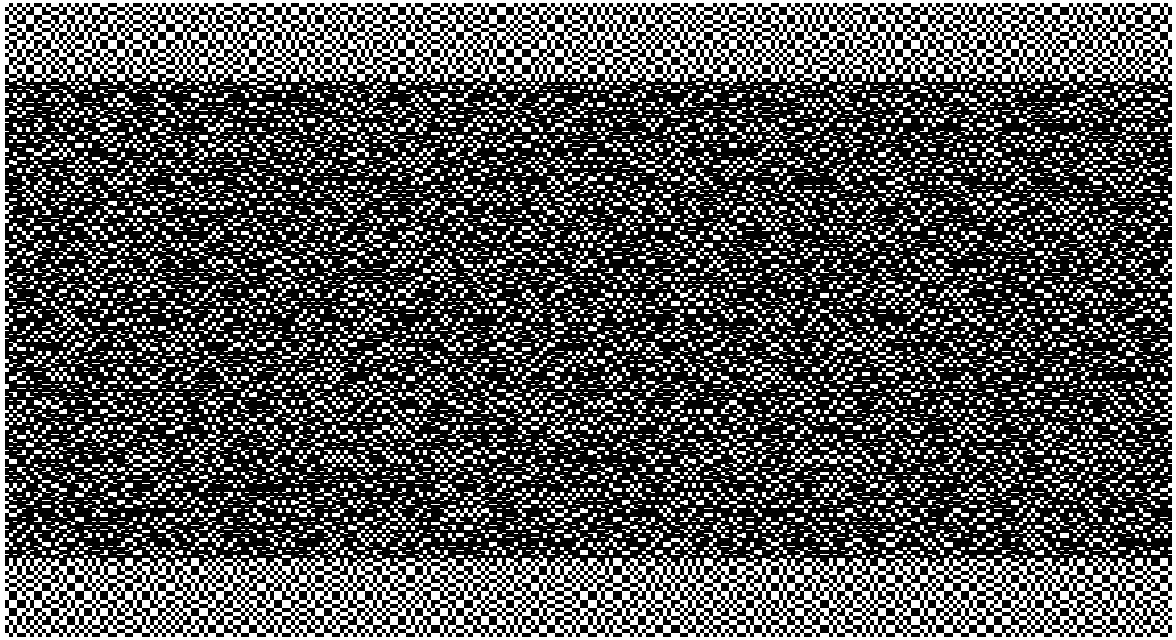


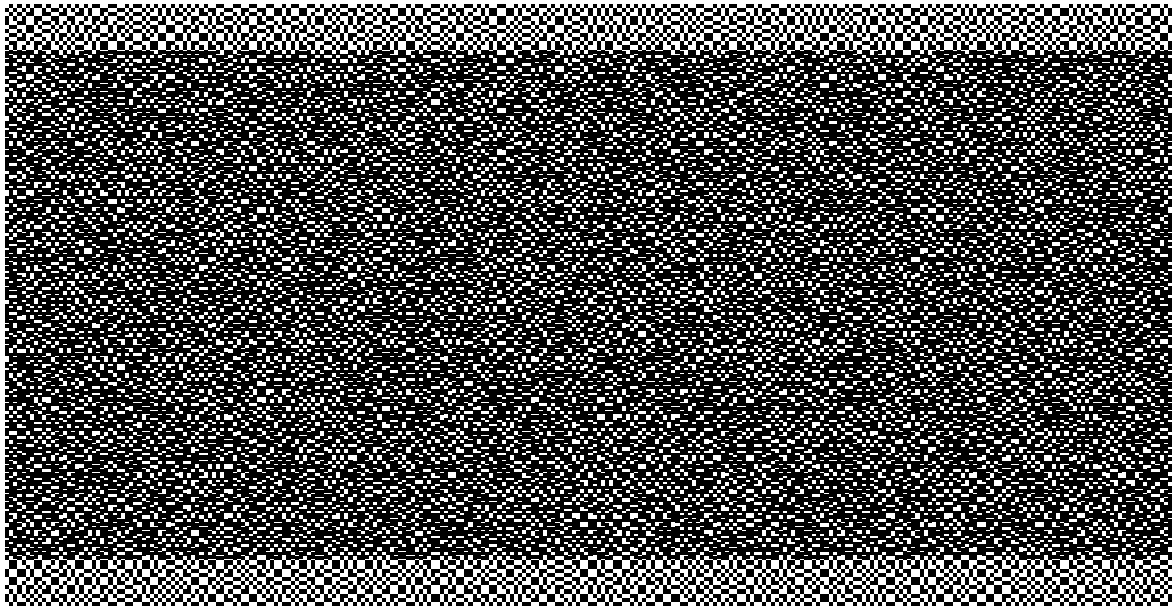


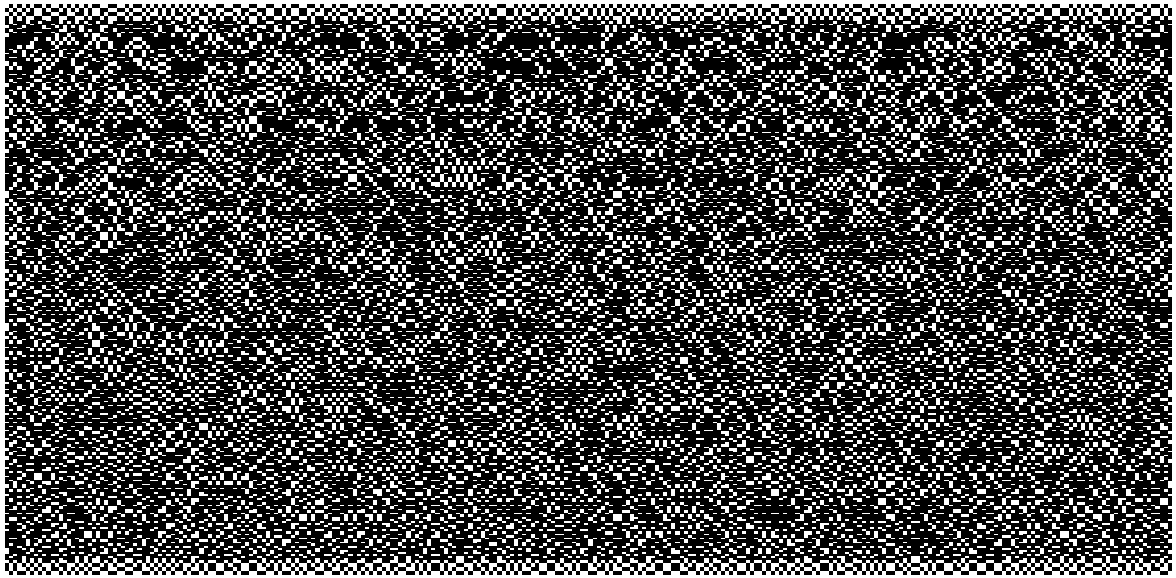


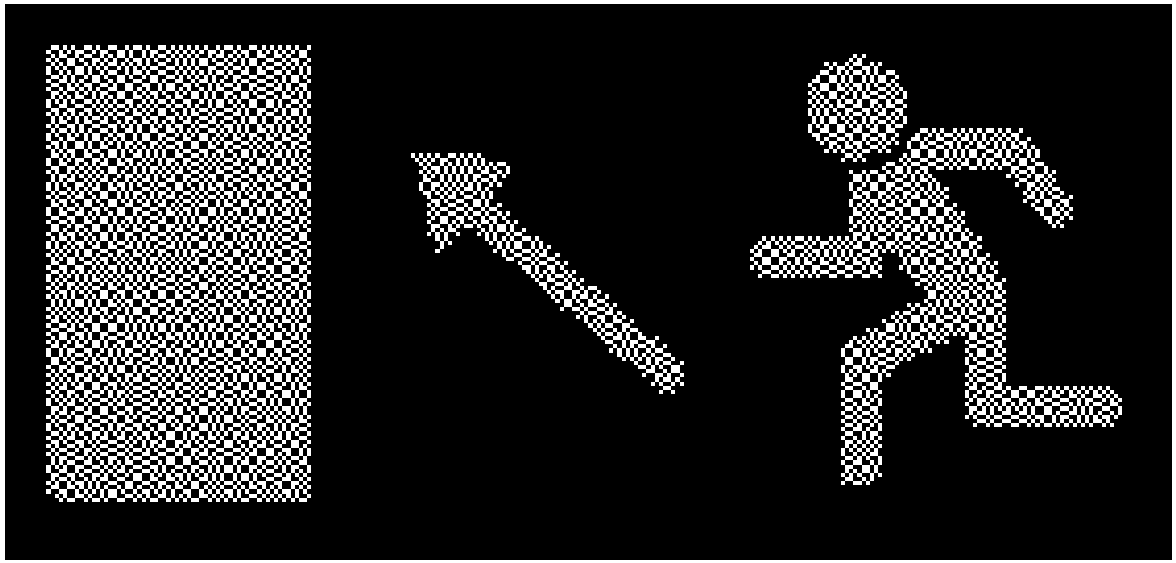


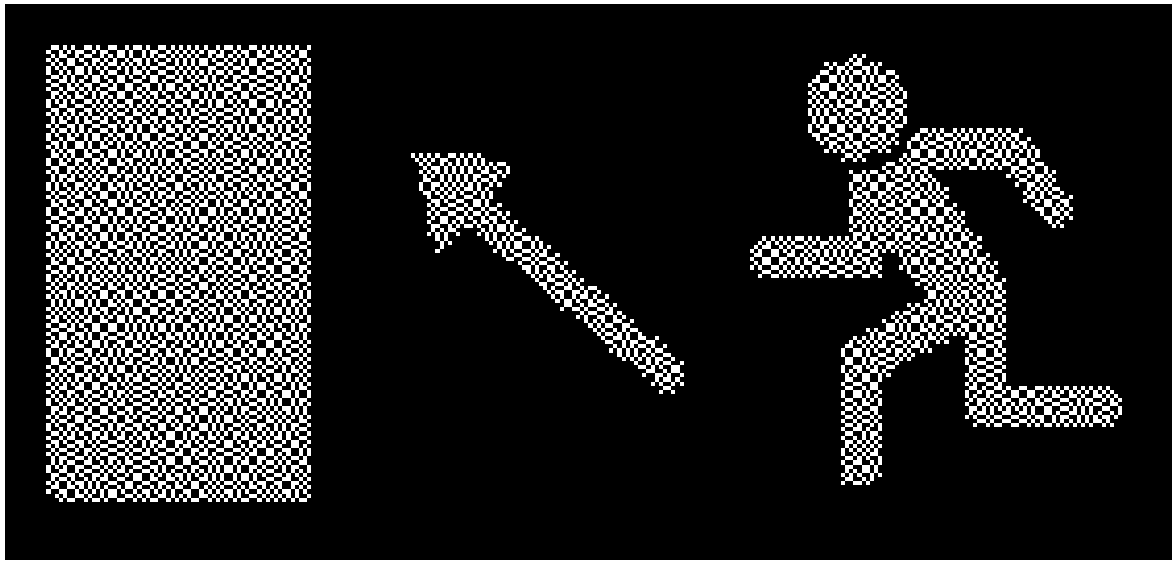












The Queen shall secure the British Strike Force code

What might she do ?

The Queen shall secure the British Strike Force code

What might she do ?

The Queen shall secure the British Strike Force code

What might she do ?

42 42 42 42 42 42 42

The Queen shall secure the British Strike Force code

What might she do ?

42 42 42 42 42 42 42







The Queen shall secure the British Strike Force code

What might she do ?

42 42 42 42 42 42 42







The Queen shall secure the British Strike Force code

What might she do ?

893 163 347 213 73 903 37

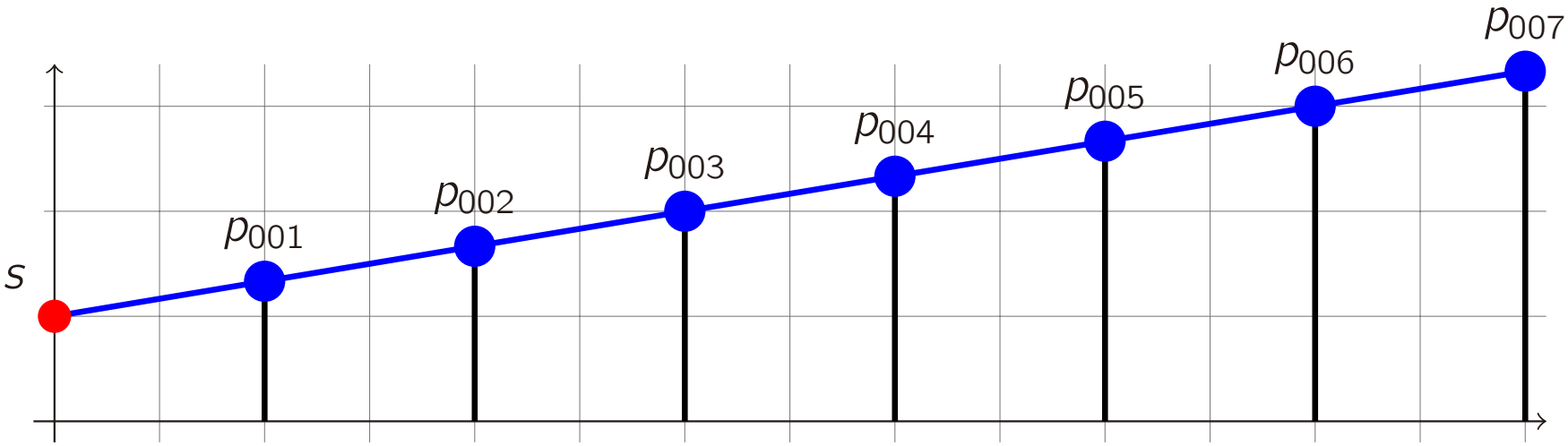


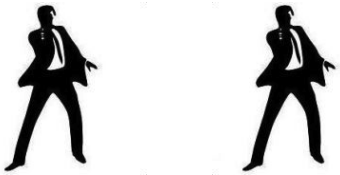




The Queen shall secure the British Strike Force code

What might she do ?





Threshold secret sharing: Shamir's scheme

Problem. For n participants:

- assign one share to each participant
- require at least m to uncover the secret
- less than m have no information

Threshold secret sharing: Shamir's scheme

Problem. For n participants:

- assign one share to each participant
- require at least m to uncover the secret
- less than m have no information

Shamir's scheme (1979)

1. Encode the secret as $s \in \mathbb{F}_q$ where $q > n$
2. Generate $p(X) = c_{m-1}X^{m-1} + \ldots + c_1 X + s$ with random $c_i \in \mathbb{F}_q$
3. Give the share $p(i)$ to participant i

Threshold secret sharing: Shamir's scheme

Problem. For n participants:

- assign one share to each participant
- require at least m to uncover the secret
- less than m have no information

Shamir's scheme (1979)

1. Encode the secret as $s \in \mathbb{F}_q$ where $q > n$
2. Generate $p(X) = c_{m-1}X^{m-1} + \ldots + c_1 X + s$ with random $c_i \in \mathbb{F}_q$
3. Give the share $p(i)$ to participant i

A polynomial of degree $m-1$ is uniquely defined by m of its values at distinct points.

What is an Access structure ?

Definition (**Access structure)**

An access structure Γ on $\mathcal{P}$ is a **monotone** family of subset of $\mathcal{P}$:

$$\Gamma \subseteq \mathscr{P}(\mathcal{P}) \text{ such that } \forall A \in \Gamma, A \subseteq B \Rightarrow B \in \Gamma$$

What is an Access structure ?

Definition (**Access structure)**

An access structure Γ on $\mathcal{P}$ is a **monotone** family of subset of $\mathcal{P}$:

$$\Gamma \subseteq \mathscr{P}(\mathcal{P}) \text{ such that } \forall A \in \Gamma, A \subseteq B \Rightarrow B \in \Gamma$$

Examples:

(m, n)-threshold access structure

For n participants, a subset is authorized if it contains at least m people:

$$\Gamma_{(m,n)} = \{A \subseteq \mathcal{P} : |A| \geq m\}$$

What is an Access structure ?

Definition (**Access structure)**

An access structure Γ on $\mathcal{P}$ is a **monotone** family of subset of $\mathcal{P}$:

$$\Gamma \subseteq \mathscr{P}(\mathcal{P}) \text{ such that } \forall A \in \Gamma, A \subseteq B \Rightarrow B \in \Gamma$$

Examples:

Hypergraph structures

- Vertices are participants
- Hyperedges are minimal authorized groups

What is an Access structure ?

Definition (**Access structure)**

An access structure Γ on $\mathcal{P}$ is a **monotone** family of subset of $\mathcal{P}$:

$$\Gamma \subseteq \mathscr{P}(\mathcal{P}) \text{ such that } \forall A \in \Gamma, A \subseteq B \Rightarrow B \in \Gamma$$

Examples:

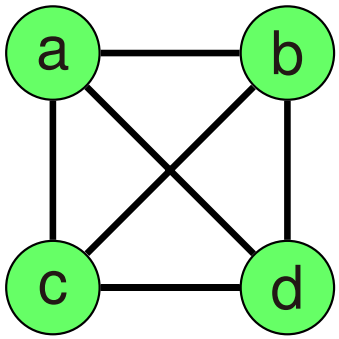
What is an Access structure ?

Definition (**Access structure)**

An access structure Γ on $\mathcal{P}$ is a **monotone** family of subset of $\mathcal{P}$:

$$\Gamma \subseteq \mathscr{P}(\mathcal{P}) \text{ such that } \forall A \in \Gamma, A \subseteq B \Rightarrow B \in \Gamma$$

Examples:



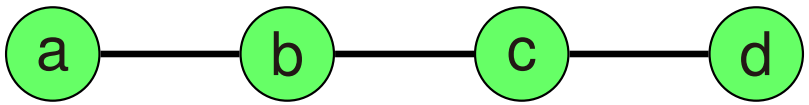
What is an Access structure ?

Definition (**Access structure)**

An access structure Γ on $\mathcal{P}$ is a **monotone** family of subset of $\mathcal{P}$:

$$\Gamma \subseteq \mathscr{P}(\mathcal{P}) \text{ such that } \forall A \in \Gamma, A \subseteq B \Rightarrow B \in \Gamma$$

Examples:



Problem?

Input:

- a finite discrete random variable s (secret)
- a set of n participants
- an access structure Γ that contains authorized groups.

Problem?

Input:

- a finite discrete random variable s (secret)
- a set of n participants
- an access structure Γ that contains authorized groups.

Goal: Find random variables (called shares) to be given to participants for implement the structure

Definition (**perfect secret-sharing schemes)**

A perfect secret sharing scheme for Γ is a tuple of discrete random variables $(\mathbf{s}, \mathbf{p}_1, \ldots, \mathbf{p}_n)$ such that :

- if the group A is authorized then the secret is uniquely determined by the shares of A
- if B is not authorized then the secret is independent of the shares of B

Definition (**perfect secret-sharing schemes)**

A perfect secret sharing scheme for Γ is a tuple of discrete random variables $(\mathbf{s}, \mathbf{p}_1, \ldots, \mathbf{p}_n)$ such that :

- if the group A is authorized then the secret is uniquely determined by the shares of A, i.e.,

$$A \in \Gamma \Rightarrow H(\mathbf{s}|\mathbf{A}) = 0$$

- if B is not authorized then the secret is independent of the shares of B, i.e.,

$$B \notin \Gamma \Rightarrow I(\mathbf{s}:\mathbf{B}) = 0$$

Definition (**perfect secret-sharing schemes)**

A perfect secret sharing scheme for Γ is a tuple of discrete random variables $(\mathbf{s}, \mathbf{p}_1, \ldots, \mathbf{p}_n)$ such that :

- if the group A is authorized then the secret is uniquely determined by the shares of A, i.e.,

$$A \in \Gamma \Rightarrow H(\mathbf{s}|\mathbf{A}) = 0$$

- if B is not authorized then the secret is independent of the shares of B, i.e.,

$$B \notin \Gamma \Rightarrow I(\mathbf{s}:\mathbf{B}) = 0$$

Definition (**Efficiency)**

The information ratio of a scheme is defined by:

$$\rho = \max_{p \in \mathcal{P}} \frac{H(\mathbf{p})}{H(\mathbf{s})}$$

Basic properties of perfect schemes

Propositions (Folklore)

- Every access structure can be implemented
- If a participant p appears in a minimal set of Γ then $H(\mathbf{p}) \geq H(\mathbf{s})$

Basic properties of perfect schemes

Propositions (Folklore)

- Every access structure can be implemented
- If a participant p appears in a minimal set of Γ then $H(\mathbf{p}) \geq H(\mathbf{s})$

Definition (**Ideal**)

A scheme is said ideal if $\rho = 1$.
An access structure Γ *is ideal if there exists an ideal scheme for* Γ.

Basic properties of perfect schemes

Propositions (Folklore)

- Every access structure can be implemented
- If a participant p appears in a minimal set of Γ then $H(\mathbf{p}) \geq H(\mathbf{s})$

Definition (**Ideal**)

A scheme is said ideal if $\rho = 1$.
An access structure Γ *is ideal if there exists an ideal scheme for* Γ.

Remark: Shamir's threshold scheme is ideal

Ideal schemes are matroidal

Proposition

Any linear matroid defines an ideal secret sharing scheme.

Theorem (Brickell-Davenport 1996)

For any ideal perfect secret sharing scheme $r(A) = \frac{H(A)}{H(s)}$ *defines the rank function of a matroid over* $\mathcal{P} \cup \{s\}$.

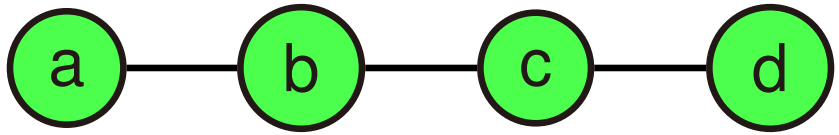
Theorem (Martí-Farré, Padró 2007)

If Γ *does not induce a matroid then* $\rho(\Gamma) \geq \frac{3}{2}$

only ideal access structures?

There exists non-ideal access structures.

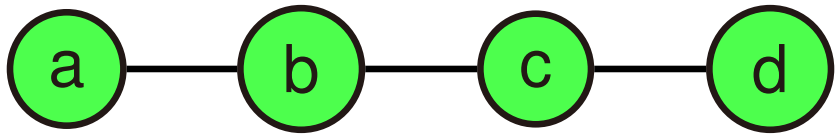
The access structure P_4:



is not ideal.

There exists non-ideal access structures.

The access structure P_4:



is not ideal.

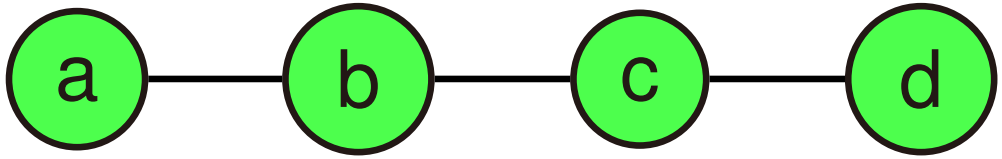
Proposition (Folklore) — proven later

For any scheme, it holds that $\rho \geq \frac{3}{2}$.

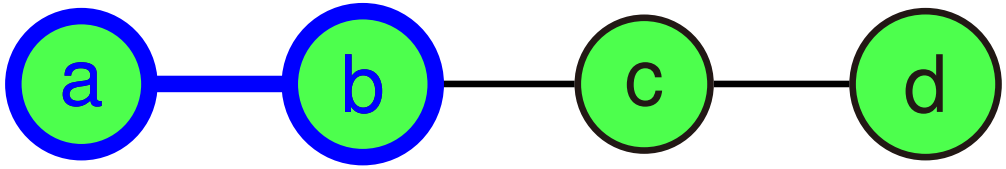
Proposition (Folklore) — proven hereafter

There exists a scheme with information ratio $\rho = \frac{3}{2}$.

A scheme for P_4

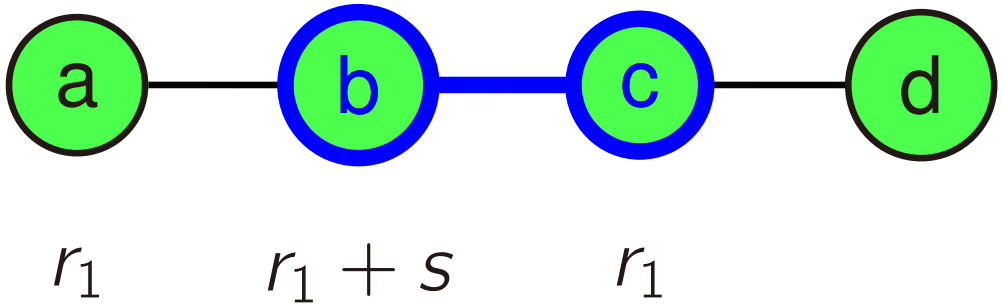


A scheme for P_4

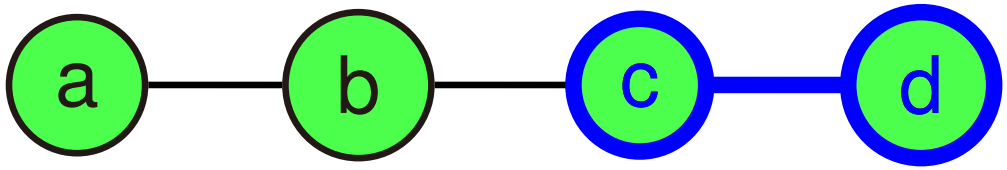


r_1 $r_1 + s$

A scheme for P_4



A scheme for P_4

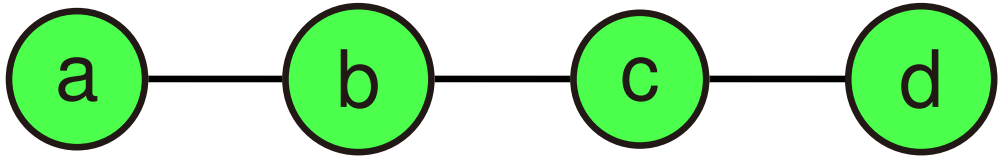


r_1 $r_1 + s$ r_1

$r_2 + s$ r_2

$$\rho = 2$$

A scheme for P_4

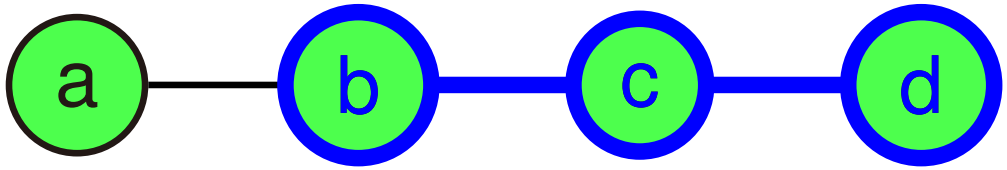


r_1 $r_1 + s_1$ r_1

$r_2 + s_1$ r_2

$$\rho = 2$$

A scheme for P_4



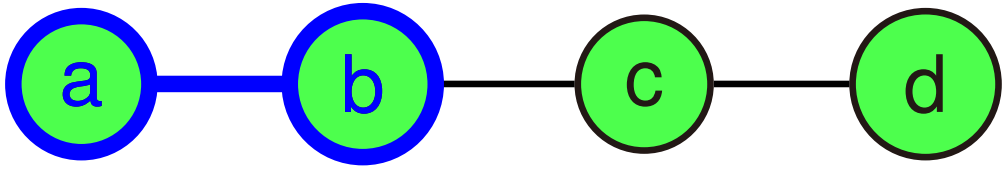
$$r_1 \qquad r_1 + s_1 \qquad r_1$$

$$r_2 + s_1 \qquad r_2$$

$$r_3 \qquad r_3 + s_2 \qquad r_3$$

$$\rho = 2$$

A scheme for P_4



$$r_1 \qquad r_1 + s_1 \qquad r_1$$

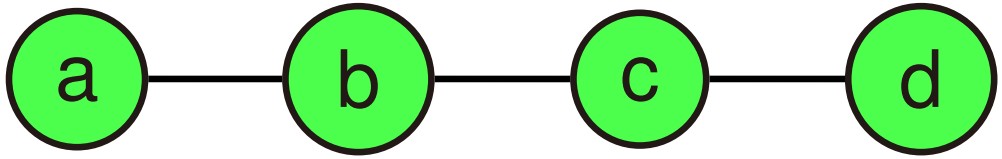
$$r_2 + s_1 \qquad r_2$$

$$r_3 \qquad r_3 + s_2 \qquad r_3$$

$$r_4 \qquad r_4 + s_2$$

$$\rho = 2$$

A scheme for P_4



$$r_1 \qquad r_1 + s_1 \qquad r_1$$

$$r_2 + s_1 \qquad r_2$$

$$r_3 \qquad r_3 + s_2 \qquad r_3$$

$$r_4 \qquad r_4 + s_2$$

$$\rho = \frac{3}{2}$$

Efficiency gap

Theorem (Csirmaz, 1994)

There exist a family of access structures Γ_n such that:

$$\rho(\Gamma_n) \geq \frac{n}{4 \log n}$$

Efficiency gap

Theorem (Csirmaz, 1994)

There exist a family of access structures Γ_n such that:

$$\rho(\Gamma_n) \geq \frac{n}{4 \log n}$$

Upper vs. Lower bounds:

$$\underbrace{\frac{n}{4 \log n} \quad \leq \quad \rho(\Gamma) \quad \leq \quad 2^{O(n)}}$$

Open Problem:
fill the gap

General technique: Information Inequalities.

Quasi-perfect Secret Sharing

Why quasi-perfect schemes?

(Hint: nobody's perfect)

Perfect schemes are restrictive

What if we relax perfectness and allow leaks ?

Contributions:

- introduce general definitions for quasi-perfect secret sharing
- formulate basic questions & properties
- study asymptotic properties of the efficiency parameters
- relate to a Kolmogorov complexity version

New parameters: the leakages.

Definition

A perfect secret-sharing scheme for Γ is a tuple of discrete random variables $(s, p_1, \ldots, p_n)$ such that :

- if $A \in \Gamma$ then $H(s|A) = 0$
- if $B \notin \Gamma$ then $I(s:B) = 0$

New parameters: the leakages.

Definition

A secret-sharing scheme for Γ is a tuple of discrete random variables $(s, p_1, \ldots, p_n)$ such that :

- if $A \in \Gamma$ then $H(s|A) \leq \underbrace{\varepsilon H(s)}_{\text{missing information}}$
- if $B \notin \Gamma$ then $I(s:B) \leq \underbrace{\delta H(s)}_{\text{information leak}}$

New parameters: the leakages.

Definition

A secret-sharing scheme for Γ is a tuple of discrete random variables $(s, p_1, \ldots, p_n)$ such that :

- if $A \in \Gamma$ then $H(s|A) \leq \underbrace{\varepsilon H(s)}_{\text{missing information}}$
- if $B \notin \Gamma$ then $I(s:B) \leq \underbrace{\delta H(s)}_{\text{information leak}}$

Parameters of a scheme:

- ε : missing information ratio.
- δ : information leak ratio.
- ρ : information ratio (efficiency).

Quasi-perfect Secret Sharing

Definition

An access structure Γ can be **quasi-perfectly implemented with information ratio** ρ if there exists a sequence of secret-sharing schemes such that:

(1) the $\limsup$ of the information ratio does not exceed ρ;

(2) the missing information ratio tends to zero;

(3) the information leak ratio tends to zero.

Algorithmic Scheme

Definition

An access structure Γ can be **algorithmically implemented with information ratio** ρ if there exists a sequence of algorithmic secret-sharing schemes with secrets s_n such that

(0) the complexity of s_n tends to infinity;

(1) the lim sup of the information ratio does not exceed ρ;

(2) the missing information ratio tends to zero;

(3) the information leak ratio tends to zero.

Algorithmic secret sharing:

- Replace Entropy (H) by Complexity (C) in the definition
- Replace random variables by binary strings

Getting rid of missing information

- Assume we have a scheme *with* missing information
- Can it be made into a scheme *without* missing information ?

Getting rid of missing information

- Assume we have a scheme *with* missing information
- Can it be made into a scheme *without* missing information ?

Theorem (K. 2011)

Any scheme can be converted into a scheme without missing information but with (possibly) bigger leak and share size

Getting rid of missing information

- Assume we have a scheme *with* missing information
- Can it be made into a scheme *without* missing information ?

Theorem (K. 2011)

Any scheme can be converted into a scheme without missing information but with (possibly) bigger leak and share size

Idea:

- materialize the missing information for each group
- add it to participants' shares

Basic Properties of QP Schemes

Corollary (K. 2011, Missing information is unimportant)

If an access structure Γ can be quasi-perfectly implemented, then it has a quasi-perfect implementation without missing information for the same information ratio.

Basic Properties of QP Schemes

Corollary (K. 2011, Missing information is unimportant)

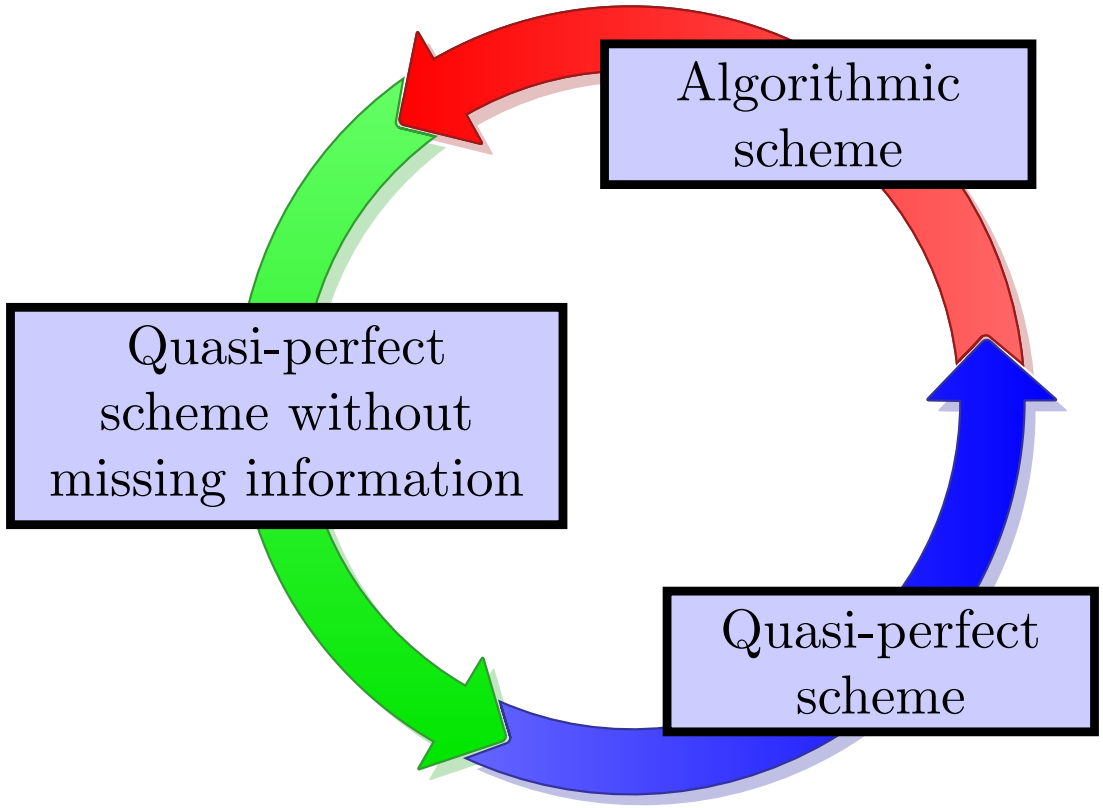
If an access structure Γ can be quasi-perfectly implemented, then it has a quasi-perfect implementation without missing information for the same information ratio.

Theorem (K. 2012, Uniform distribution on secrets)

If some access structure Γ can be quasi-perfectly implemented with information ratio ρ, it can be quasi-perfectly implemented with the same ratio by schemes with uniformly distributed secrets.

Equivalence between secret sharing flavors

Theorem[K, 2011]: Given access structure Γ and information ratio ρ:



Remark: still true when ε, δ tend to fixed constants.

Changing the secret size

Suppose we have a scheme for sharing N-bits secrets.

- Question: Can we modify it to share $\ell < N$ bits ?
- scaling up is natural (independent copies)
- scaling down quasi-perfect schemes is nontrivial
- Notice: We also want to reduce the leak δN

Reducing the size of the secret

Theorem (K. 2011)

Any scheme for N-bit secrets w/ info leak δN (N large enough) can be converted into a scheme for 1 bit secret w/ info leak $O(\delta^{\frac{2}{3}})$ and the same size for shares.

Reducing the size of the secret

Theorem (K. 2011)

Any scheme for N-bit secrets w/ info leak δN (N large enough) can be converted into a scheme for 1 bit secret w/ info leak $O(\delta^{\frac{2}{3}})$ and the same size for shares.

Proof sketch : (probabilistic method)

- randomly cut the secret set into two equal parts
- define new secret accordingly
- show that a random cut achieves the given leak
- uses Höffding inequality to prove existence

A weak separation result

Proposition (K. 2011)

There is an access structure which can be implemented quasi-perfectly such that:

- *the information ratio of each scheme is exactly* 1*,*
- *without information leak,*
- *with vanishing missing information.*

but has ***no perfect scheme*** *with information ratio exactly* 1*.*

The proof is mainly based on an argument of F. Matúš (1995).

A weak separation result

Proposition (K. 2011)

There is an access structure which can be implemented quasi-perfectly such that:

- *the information ratio of each scheme is exactly* 1*,*
- *without information leak,*
- *with vanishing missing information.*

but has ***no perfect scheme*** *with information ratio exactly* 1*.*

The proof is mainly based on an argument of F. Matúš (1995).

Open question: Can we achieve a more substantial separation ?
Not with the current technique using unconditional inequalities

Information Inequalities

Shannon's entropy

Let A be a **discrete** random variable on the alphabet Q, equipped with the **probability distribution** law $p : Q \to [0, 1]$. The **support** $\mathcal{S}_A$ consists of letters with positive probability.

$$H(A) = -\sum_{a \in \mathcal{S}_A} p(a) \log p(a) = \mathbb{E}_{\mathcal{S}_A} \log p$$

Shannon's entropy

Let A be a **discrete** random variable on the alphabet Q, equipped with the **probability distribution** law $p : Q \to [0, 1]$. The **support** $\mathcal{S}_A$ consists of letters with positive probability.

$$H(A) = -\sum_{a \in \mathcal{S}_A} p(a) \log p(a) = \mathbb{E}_{\mathcal{S}_A} \log p$$

- **Amount of information contained in a random variable**
- In general $0 \leq H(A) \leq \log |\mathcal{S}_A|$
- $H(A) = 0 \Leftrightarrow A$ is deterministic
- $H(A) = \log |\mathcal{S}_A| \Leftrightarrow A$ is uniformly distributed over $\mathcal{S}_A$

Shannon's Information Measures

Conditional Entropy:

$$H(X|Y) = H(XY) - H(Y)$$

Mutual Information:

$$I(X:Y) = H(X) + H(Y) - H(XY)$$

Conditional Mutual Information:

$$I(X:Y|Z) = H(XZ) + H(YZ) - H(XYZ) - H(Z)$$

Shannon's Information Measures

Conditional Entropy:

$$H(X|Y) = H(XY) - H(Y) \geq 0$$

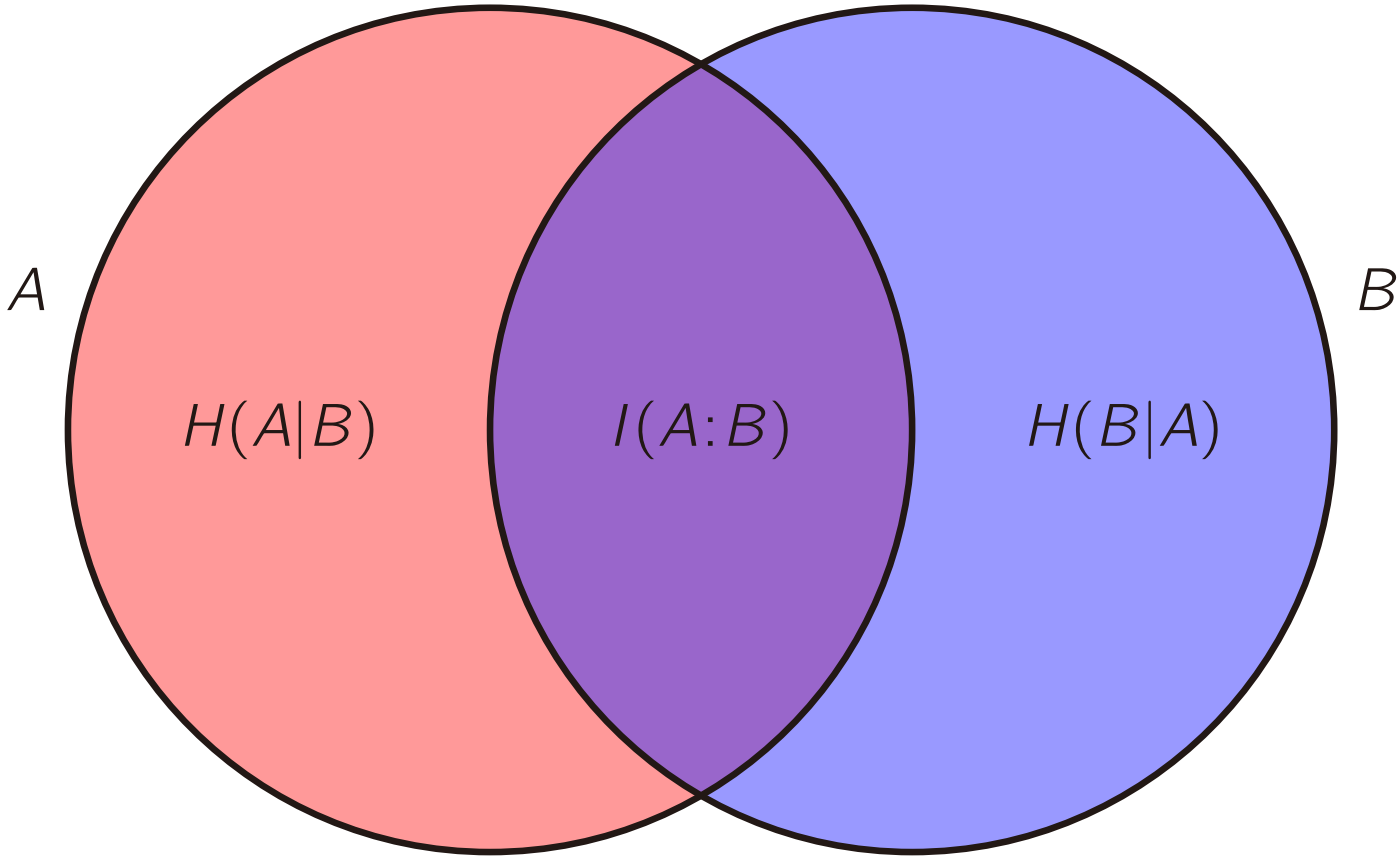
Mutual Information:

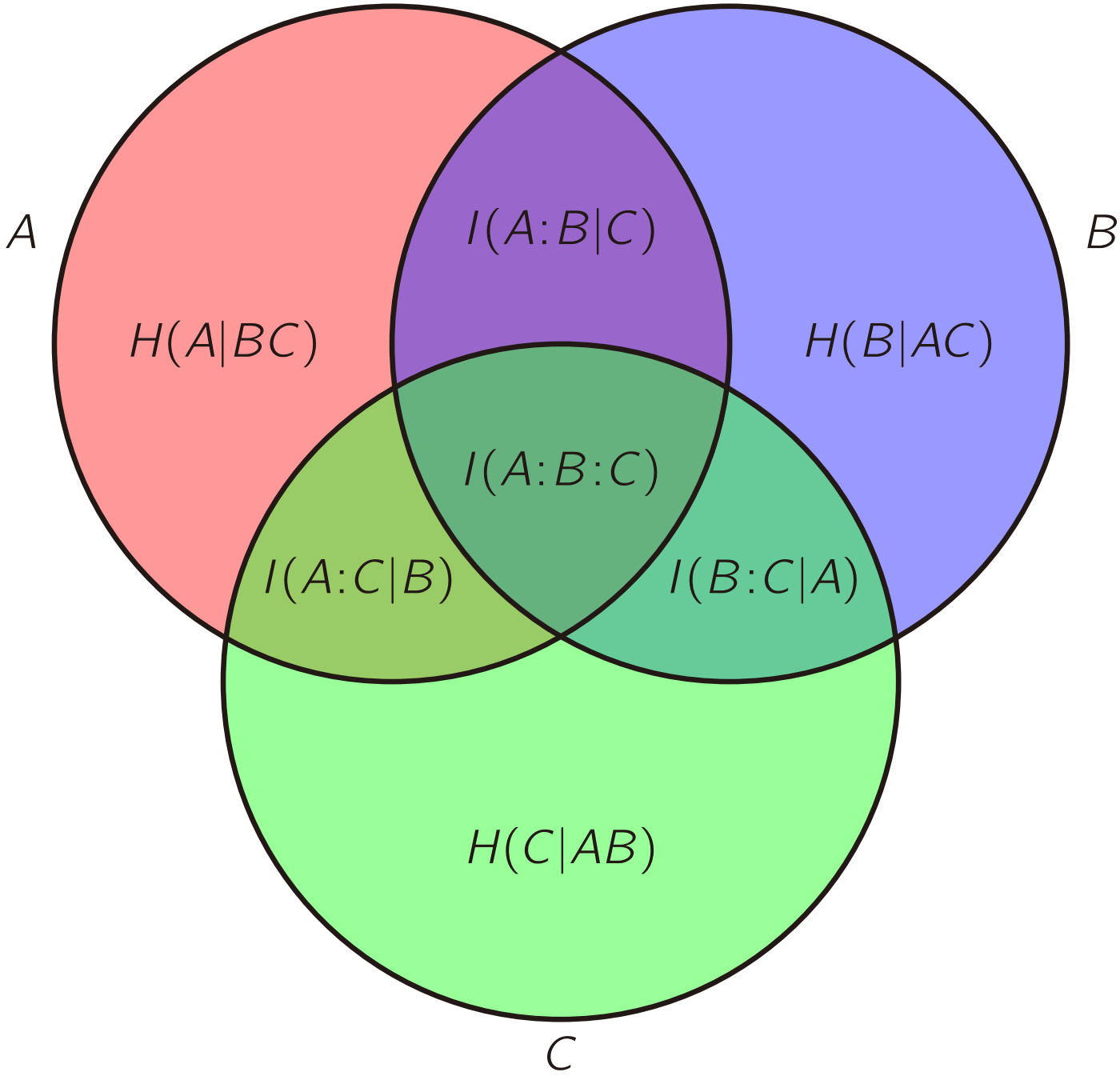
$$I(X:Y) = H(X) + H(Y) - H(XY) \geq 0$$

Conditional Mutual Information:

$$I(X:Y|Z) = H(XZ) + H(YZ) - H(XYZ) - H(Z) \geq 0$$

Basic Inequality


A
B
H(A|B)
I(A:B)
H(B|A)


A
B
C
H(A|BC)
I(A:B|C)
H(B|AC)
I(A:B:C)
I(A:C|B)
I(B:C|A)
H(C|AB)

Linear information inequalities

Pippenger (1986): **What are the laws of Information Theory?**

Linear information inequalities

Pippenger (1986): **What are the laws of Information Theory?**

Basic inequality:

$$H(ab) \leq H(a) + H(b) \qquad [I(a:b) \geq 0]$$
$$H(abc) + H(c) \leq H(ac) + H(bc) \qquad [I(a:b|c) \geq 0]$$

Linear information inequalities

Pippenger (1986): **What are the laws of Information Theory?**

Basic inequality:

$$H(ab) \leq H(a) + H(b) \qquad [I(a:b) \geq 0]$$
$$H(abc) + H(c) \leq H(ac) + H(bc) \qquad [I(a:b|c) \geq 0]$$

Shannon-type inequalities: any positive combination of basic ineq., e.g.,

$$H(a) \leq H(a|b) + H(a|c) + I(b:c)$$

Linear information inequalities

Pippenger (1986): **What are the laws of Information Theory?**

Basic inequality:

$$\begin{aligned} H(ab) &\leq H(a) + H(b) && [I(a:b) \geq 0] \\ H(abc) + H(c) &\leq H(ac) + H(bc) && [I(a:b|c) \geq 0] \end{aligned}$$

Shannon-type inequalities: any positive combination of basic ineq., e.g.,

$$H(a) \leq H(a|b) + H(a|c) + I(b:c)$$

Non-Shannon-type inequalities, e.g., [Z. Zhang, R. W. Yeung, 1998] :

$$\begin{aligned} I(c:d) \quad \leq \quad & I(c:d|a) + I(c:d|b) + I(a:b) + \\ & + I(c:d|a) + I(a:c|d) + I(a:d|c) \end{aligned}$$

Counterpart to Kolmogorov Complexity

For any binary strings x, y:

$$C(x) = \text{length of a shortest program printing } x,$$
$$C(x|y) = \text{length of a shortest program printing } x \text{ given input } y.$$

And up to $O(\log |xy|)$,

$$C(x) \geq 0,$$
$$C(x|y) \geq 0,$$
$$C(x) + C(y) \geq C(x, y).$$

Counterpart to Kolmogorov Complexity

For any binary strings x, y:

$$C(x) = \text{length of a shortest program printing } x,$$
$$C(x|y) = \text{length of a shortest program printing } x \text{ given input } y.$$

And up to $O(\log |xy|)$,

$$C(x) \geq 0,$$
$$C(x|y) \geq 0,$$
$$C(x) + C(y) \geq C(x, y).$$

Theorem (Inequalities are the same, Hammer *et al*)

An inequality is valid for Shannon iff it is valid for Kolmogorov up to a logarithmic term

Essentially Conditional Inequalities

Conditional information inequalities

If [some linear constraints for entropies]
then [a linear inequality for entropies].

Conditional information inequalities

If [some linear constraints for entropies]
then [a linear inequality for entropies].

- **Example 1 (trivial):** If $I(b:c) = 0$, then $H(a) \leq H(a|b) + H(a|c)$.
  Explanation:
  $H(a) \leq H(a|b) + H(a|c) + I(b:c)$.

Conditional information inequalities

If [some linear constraints for entropies]
then [a linear inequality for entropies].

- **Example 1 (trivial):** If $I(b:c) = 0$, then $H(a) \leq H(a|b) + H(a|c)$.

  Explanation:

  $H(a) \leq H(a|b) + H(a|c) + I(b:c)$.

- **Example 2 (trivial):** If $I(c:d|e) = I(c:e|d) = I(d:e|c) = 0$, then $I(c:d) \leq I(c:d|a) + I(c:d|b) + I(a:b)$.

  Explanation:

  $I(c:d) \leq I(c:d|a) + I(c:d|b) + I(a:b) + I(c:d|e) + I(c:e|d) + I(d:e|c)$.

Conditional information inequalities

If [some linear constraints for entropies]
then [a linear inequality for entropies].

- **Example 1 (trivial):** If $I(b:c) = 0$, then $H(a) \leq H(a|b) + H(a|c)$.

  Explanation:

  $H(a) \leq H(a|b) + H(a|c) + I(b:c)$.

- **Example 2 (trivial):** If $I(c:d|e) = I(c:e|d) = I(d:e|c) = 0$, then $I(c:d) \leq I(c:d|a) + I(c:d|b) + I(a:b)$.

  Explanation:

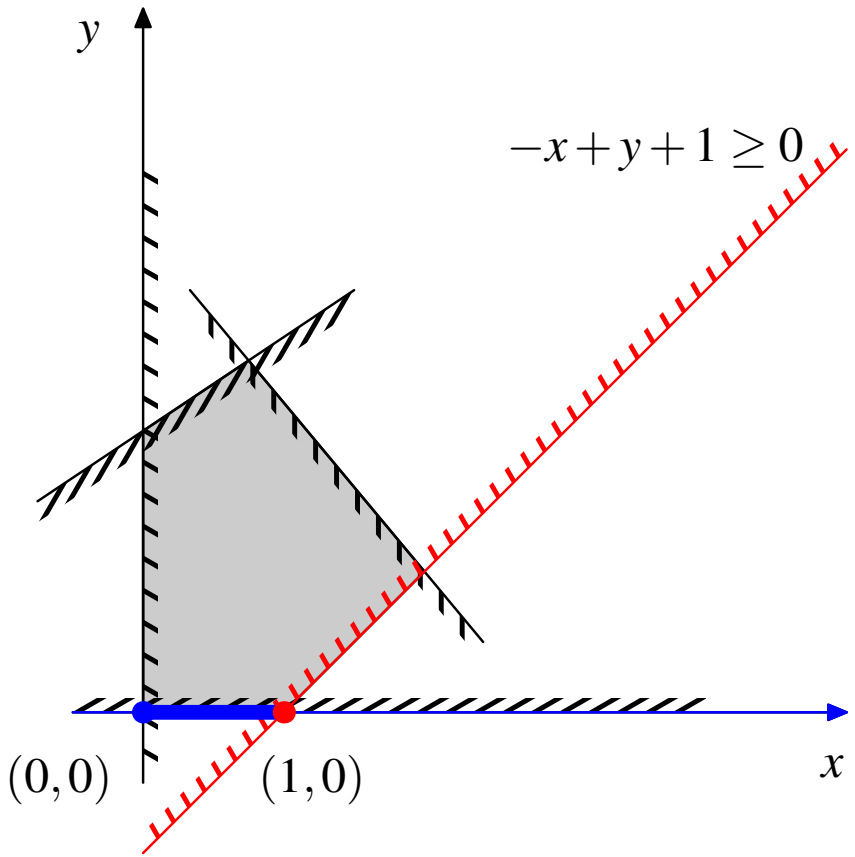
  $I(c:d) \leq I(c:d|a) + I(c:d|b) + I(a:b) + I(c:d|e) + I(c:e|d) + I(d:e|c)$.

- **Example 3 (nontrivial) [Zhang–Yeung 1997]:** If $I(a:b) = I(a:b|c) = 0$, then $I(c:d) \leq I(c:d|a) + I(c:d|b)$.

  Any explanation???

Trivial Conditional Inequalities

For (x, y) in the gray set: if $y = 0$ then $x \leq 1$



It follows from $-x + y + 1 \geq 0$.

WARNING: This picture is symbolic.

Nontrivial Conditional Inequalities

$$\underbrace{I(a:b) = I(a:b|c) = 0}_{\text{[Zhang–Yeung 97]}} \qquad \underbrace{\begin{array}{l} I(a:b|c) = I(b:d|c) = 0, \text{ or} \\ I(a:c|d) = I(a:d|c) = 0, \text{ or} \\ I(a:c|d) = I(c:d|a) = 0 \end{array}}_{\text{[Matúš 99/2007]}} \qquad \underbrace{H(c|a,b) = I(a:b|c) = 0}_{\text{[Romashchenko,K. 2011]}}$$

$$I(c:d) \leq I(c:d|a) + I(c:d|b) + I(a:b)$$

Nontrivial Conditional Inequalities

$$\underbrace{I(a:b) = I(a:b|c) = 0}_{\text{[Zhang–Yeung 97]}} \qquad \underbrace{\begin{array}{l} I(a:b|c) = I(b:d|c) = 0, \text{ or} \\ I(a:c|d) = I(a:d|c) = 0, \text{ or} \\ I(a:c|d) = I(c:d|a) = 0 \end{array}}_{\text{[Matúš 99/2007]}} \qquad \underbrace{H(c|a,b) = I(a:b|c) = 0}_{\text{[Romashchenko,K. 2011]}}$$

$$I(c:d) \leq I(c:d|a) + I(c:d|b) + I(a:b)$$

Theorem (Romashchenko, K. 2011/2012)

All of these statements are essentially conditional inequalities.

Essentially Conditional Inequalities

- **Z. Zhang, R. W. Yeung 97:**
  if $I(a:b) = I(a:b|c) = 0$, then $I(c:d) \leq I(c:d|a) + I(c:d|b)$.

Essentially Conditional Inequalities

- **Z. Zhang, R. W. Yeung 97:**

  if $I(a:b) = I(a:b|c) = 0$, then $I(c:d) \leq I(c:d|a) + I(c:d|b)$.

- **Theorem** [Romashchenko, K. 2011] This inequality is *essentially conditional*, i.e.,

  for all κ_1, κ_2 the inequality:

$$I(c:d) \leq I(c:d|a) + I(c:d|b) + \kappa_1 I(a:b) + \kappa_2 I(a:b|c)$$

  is not valid.

Proof by ad-hoc example

Claim: For any κ_1, κ_2 there exist (a, b, c, d) such that:

$$I(c:d) \not\leq I(c:d|a) + I(c:d|b) + \kappa_1 I(a:b) + \kappa_2 I(a:b|c)$$

Proof by ad-hoc example

Claim: For any κ_1, κ_2 there exist (a, b, c, d) such that:

$$I(c{:}d) \not\leq I(c{:}d|a) + I(c{:}d|b) + \kappa_1 I(a{:}b) + \kappa_2 I(a{:}b|c)$$

Proof:

a	b	c	d	Prob$[a, b, c, d]$
0	0	0	1	$(1-\varepsilon)/4$
0	1	0	0	$(1-\varepsilon)/4$
1	0	0	1	$(1-\varepsilon)/4$
1	1	0	1	$(1-\varepsilon)/4$
1	0	1	1	ε

Proof by ad-hoc example

Claim: For any κ_1, κ_2 there exist (a, b, c, d) such that:

$$I(c:d) \not\leq I(c:d|a) + I(c:d|b) + \kappa_1 I(a:b) + \kappa_2 I(a:b|c)$$

Proof:

a	b	c	d	Prob$[a, b, c, d]$
0	0	0	1	$(1-\varepsilon)/4$
0	1	0	0	$(1-\varepsilon)/4$
1	0	0	1	$(1-\varepsilon)/4$
1	1	0	1	$(1-\varepsilon)/4$
1	0	1	1	ε

$$\begin{array}{ccccccccc} I(c:d) & \not\leq & I(c:d|a) & + & I(c:d|b) & + & \kappa_1 I(a:b) & + & \kappa_2 I(a:b|c) \\ \| & & \| & & \| & & \| & & \| \\ & & 0 & & 0 & & & & 0 \end{array}$$

Proof by ad-hoc example

Claim: For any κ_1, κ_2 there exist (a, b, c, d) such that:

$$I(c:d) \not\leq I(c:d|a) + I(c:d|b) + \kappa_1 I(a:b) + \kappa_2 I(a:b|c)$$

Proof:

a	b	c	d	Prob$[a, b, c, d]$
0	0	0	1	$(1-\varepsilon)/4$
0	1	0	0	$(1-\varepsilon)/4$
1	0	0	1	$(1-\varepsilon)/4$
1	1	0	1	$(1-\varepsilon)/4$
1	0	1	1	ε

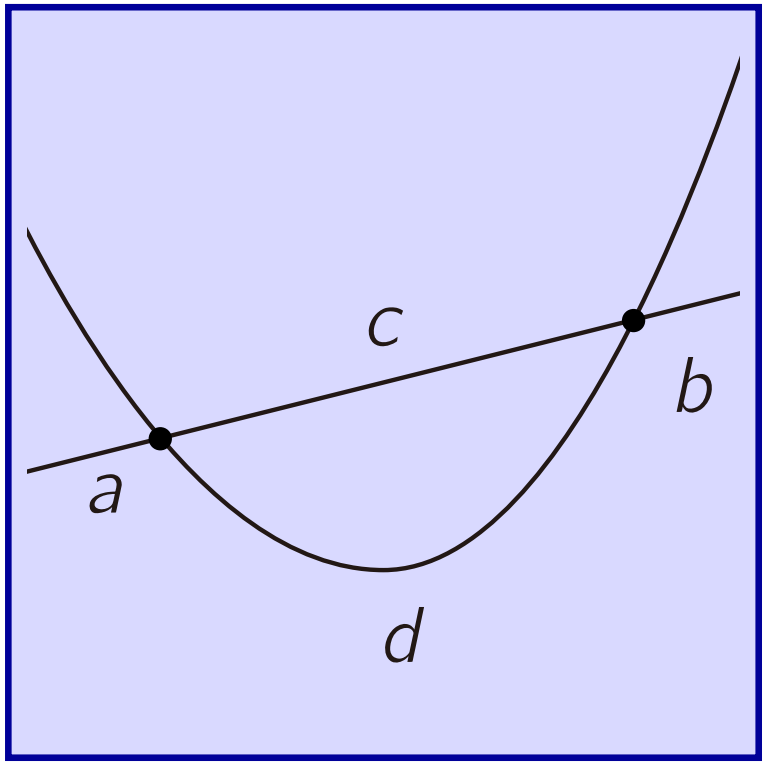
$$\begin{array}{ccccccccc} I(c:d) & \not\leq & I(c:d|a) & + & I(c:d|b) & + & \kappa_1 I(a:b) & + & \kappa_2 I(a:b|c) \\ \| & & \| & & \| & & \| & & \| \\ \Theta(\varepsilon) & \not\leq & 0 & + & 0 & + & O(\kappa_1 \varepsilon^2) & + & 0 \end{array}$$

Proof by geometric example

Construction of (a, b, c, d)

On the affine plane over $\mathbb{F}_q$:

1. Pick a random a non-vertical line c.
2. Pick two random points a and b on c.
3. Pick a random non-degenerate parabola d intersecting c exactly at a and b.

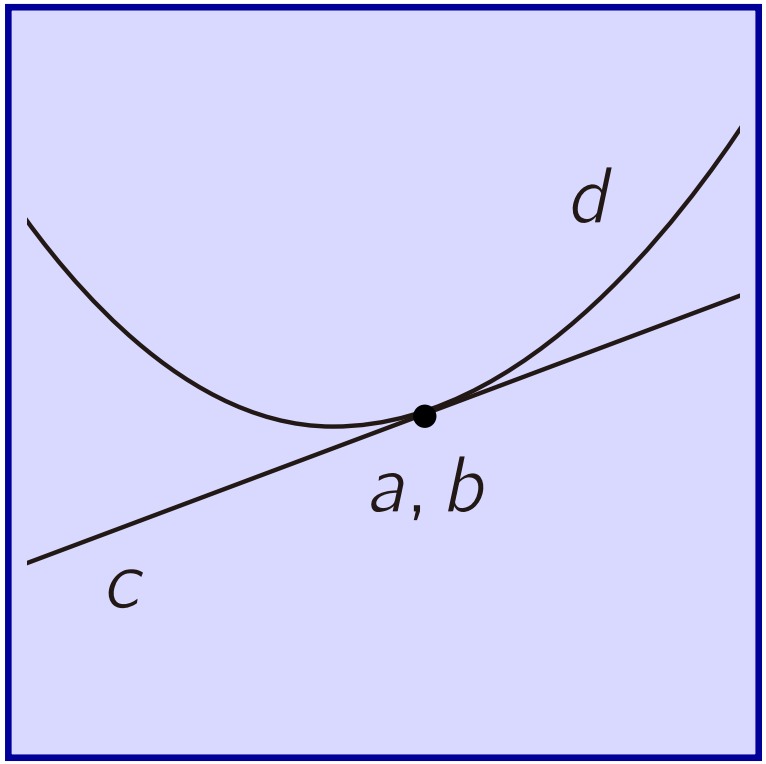


Proof by geometric example

Construction of (a, b, c, d)

On the affine plane over $\mathbb{F}_q$:

1. Pick a random a non-vertical line c.
2. Pick two random points a and b on c.
3. Pick a random non-degenerate parabola d intersecting c exactly at a and b.

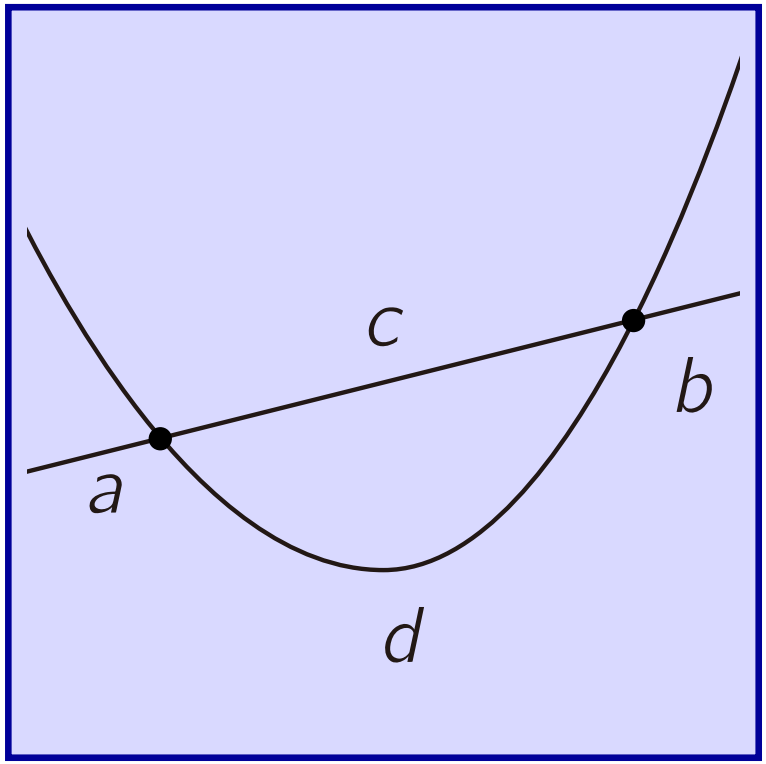


Proof by geometric example

Construction of (a, b, c, d)

On the affine plane over $\mathbb{F}_q$:

1. Pick a random a non-vertical line c.
2. Pick two random points a and b on c.
3. Pick a random non-degenerate parabola d intersecting c exactly at a and b.

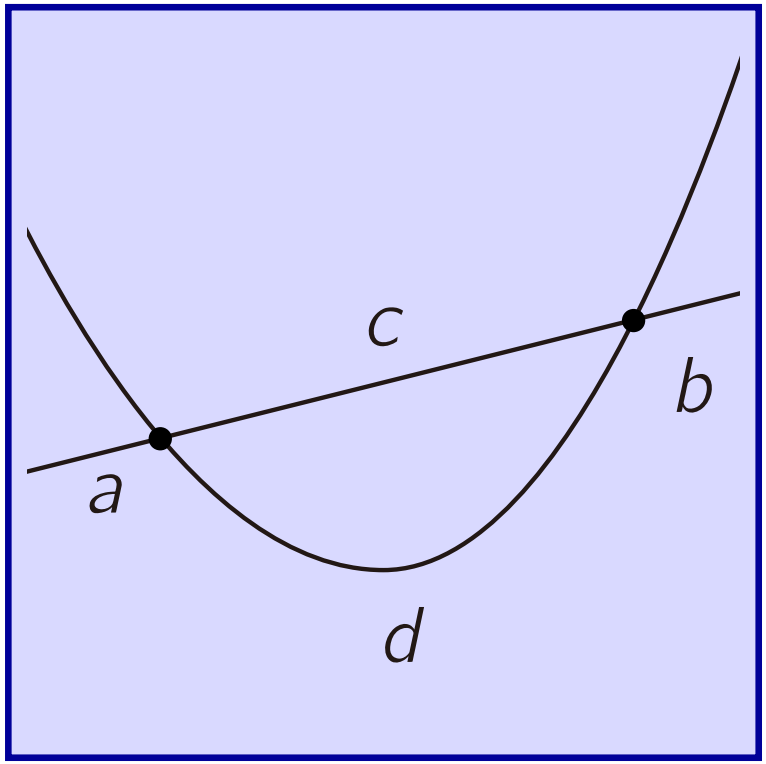


Proof by geometric example

Construction of (a, b, c, d)

On the affine plane over $\mathbb{F}_q$:

1. Pick a random a non-vertical line c.
2. Pick two random points a and b on c.
3. Pick a random non-degenerate parabola d intersecting c exactly at a and b.



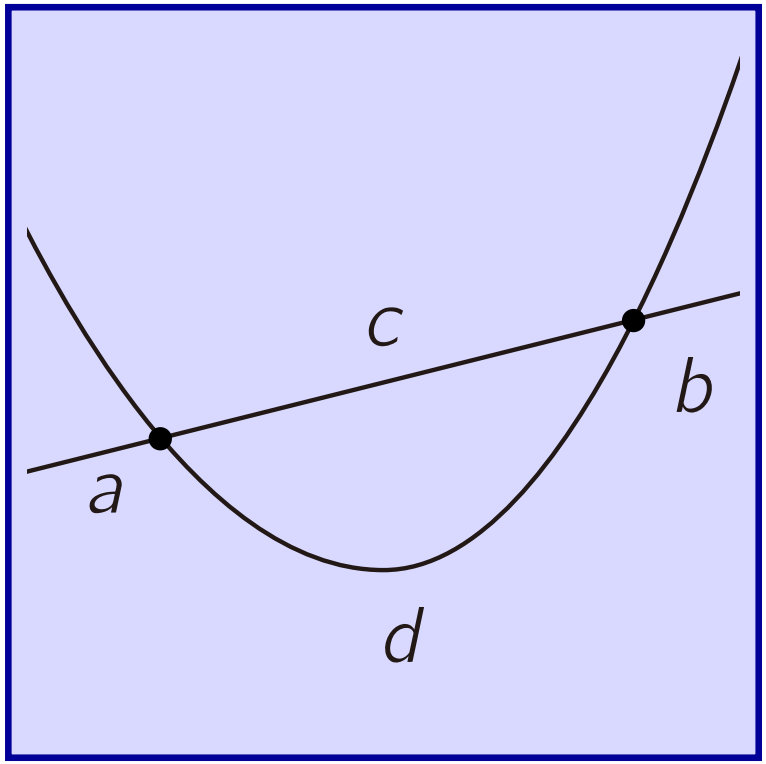
$$I(c{:}d) \leq \kappa[I(c{:}d|a) + I(c{:}d|b) + I(a{:}b) + I(a{:}b|c) + H(c|ab)]$$

Proof by geometric example

Construction of (a, b, c, d)

On the affine plane over $\mathbb{F}_q$:

1. Pick a random a non-vertical line c.
2. Pick two random points a and b on c.
3. Pick a random non-degenerate parabola d intersecting c exactly at a and b.



$$I(c{:}d) \leq \kappa[I(c{:}d|a) + I(c{:}d|b) + I(a{:}b) + I(a{:}b|c) + H(c|ab)]$$

$$1 + \frac{1}{q} \not\leq O\left(\kappa \frac{\log q}{q}\right)$$

Non-robustness of some conditional inequalities

$$I(a:b) = I(a:b|c) = 0 \Rightarrow I(c:d) \leq I(c:d|a) + I(c:d|b) \qquad \text{(ZY97)}$$

In fact we have a stronger result. Let $\epsilon > 0$, assume

- $I(a:b) \leq \epsilon$.
- $I(a:b|c) \leq \epsilon$.
- $H(a, b, c, d) = const$.

Non-robustness of some conditional inequalities

$$I(a:b) = I(a:b|c) = 0 \Rightarrow I(c:d) \leq I(c:d|a) + I(c:d|b) \qquad \text{(ZY97)}$$

In fact we have a stronger result. Let $\epsilon > 0$, assume

- $I(a:b) \leq \epsilon$.
- $I(a:b|c) \leq \epsilon$.
- $H(a, b, c, d) = const$.

Then the ratio

$$\frac{I(c:d)}{I(c:d|a) + I(c:d|b)}$$

can be made arbitrarily large.

Non-robustness of some conditional inequalities

$$I(a:b) = I(a:b|c) = 0 \Rightarrow I(c:d) \leq I(c:d|a) + I(c:d|b) \qquad \text{(ZY97)}$$

In fact we have a stronger result. Let $\epsilon > 0$, assume

- $I(a:b) \leq \epsilon$.
- $I(a:b|c) \leq \epsilon$.
- $H(a, b, c, d) = const$.

Then the ratio

$$\frac{I(c:d)}{I(c:d|a) + I(c:d|b)}$$

can be made arbitrarily large.

Non-robustness of some conditional inequalities

$$I(a:b) = I(a:b|c) = 0 \Rightarrow I(c:d) \leq I(c:d|a) + I(c:d|b) \qquad \text{(ZY97)}$$

In fact we have a stronger result. Let $\epsilon > 0$, assume

- $I(a:b) \leq \epsilon$.
- $I(a:b|c) \leq \epsilon$.
- $H(a, b, c, d) = const$.

Then the ratio

$$\frac{I(c:d)}{I(c:d|a) + I(c:d|b)}$$

can be made arbitrarily large.

Non-robustness of some conditional inequalities

$$I(a:b) = I(a:b|c) = 0 \Rightarrow I(c:d) \leq I(c:d|a) + I(c:d|b) \qquad \text{(ZY97)}$$

In fact we have a stronger result. Let $\epsilon > 0$, assume

- $I(a:b) \leq \epsilon$.
- $I(a:b|c) \leq \epsilon$.
- $H(a, b, c, d) = const$.

Then the ratio

$$\frac{I(c:d)}{I(c:d|a) + I(c:d|b)}$$

can be made arbitrarily large.

For almost entropic points

For n random variables, there $2^n - 1$ possible entropies.
When $n = 3$, there are 7 possible joint entropies:

$$(H(A), H(B), H(C), H(AB), H(AC), H(BC), H(ABC)) \in \mathbb{R}^7$$

Such a vector of entropies is called an **entropic point**.
An **almost entropic point** is the limit of a sequence of entropic points.

For almost entropic points

For n random variables, there $2^n - 1$ possible entropies.
When $n = 3$, there are 7 possible joint entropies:

$$(H(A), H(B), H(C), H(AB), H(AC), H(BC), H(ABC)) \in \mathbb{R}^7$$

Such a vector of entropies is called an **entropic point**.
An **almost entropic point** is the limit of a sequence of entropic points.

Theorem (Matúš 2007)

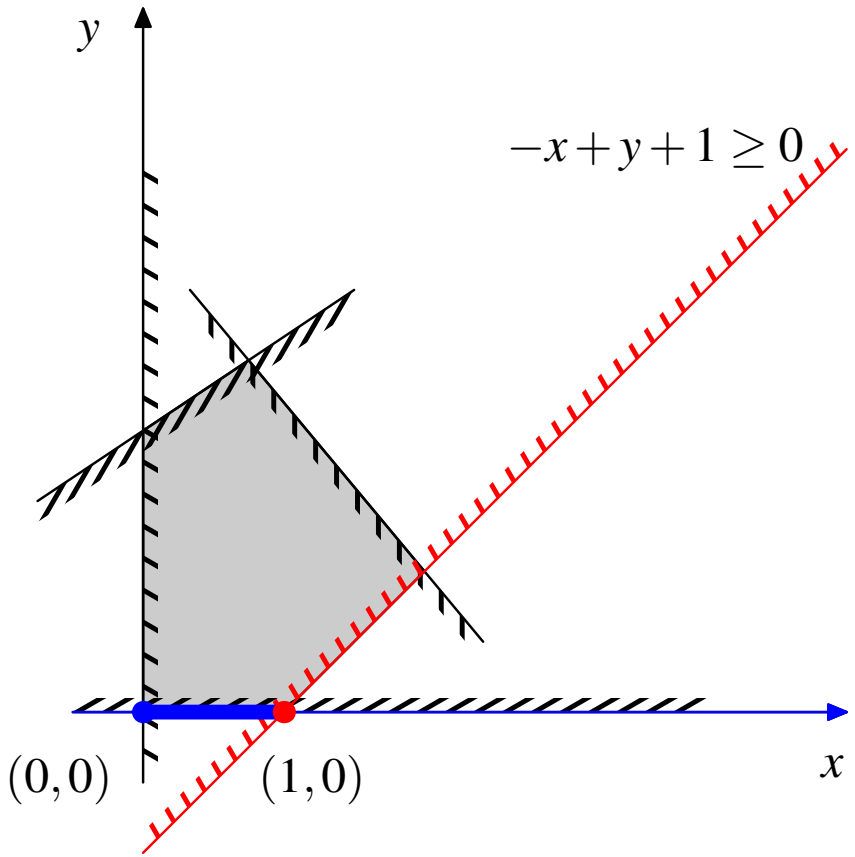
*Two essentially conditional inequalities **are valid** for all almost entropic points*

Theorem (Romashchenko, K. 2012)

*Two essentially conditional inequalities **are not valid** for all almost entropic points*

Geometric interpretation 1/3

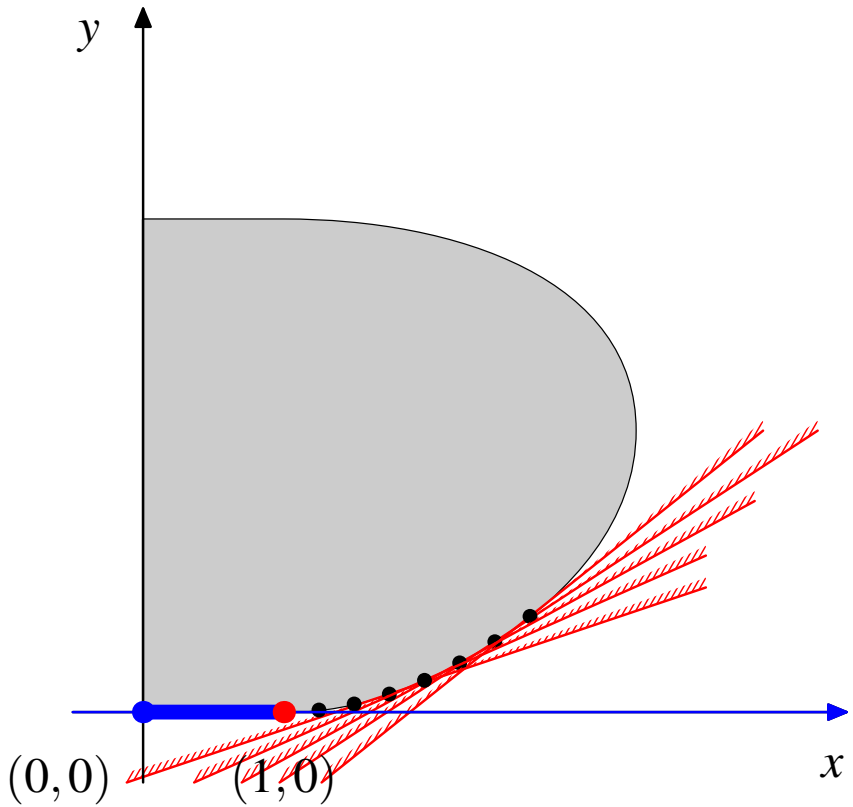
For (x, y) in the gray set: if $y = 0$ then $x \leq 1$



A trivial conditional inequality can be extended to an unconditional one.

Geometric interpretation 2/3

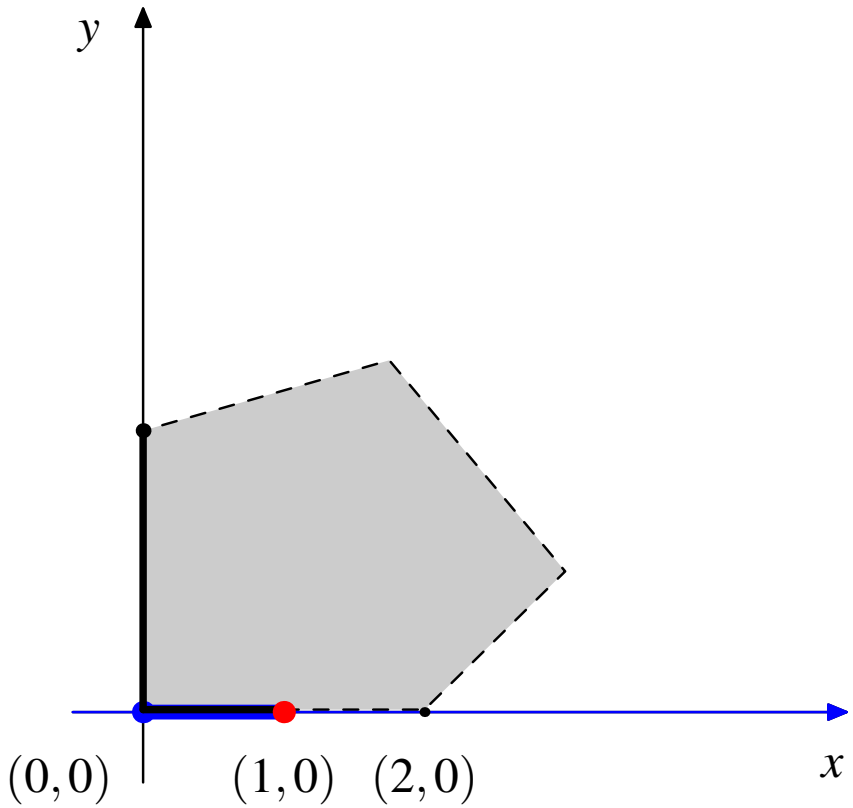
For (x, y) in the gray set: if $y = 0$ then $x \leq 1$



This conditional inequality is implied by an infinite family of tangent half-planes.

Geometric interpretation 3/3

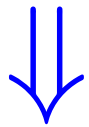
For (x, y) in the gray set: if $y = 0$ then $x \leq 1$



For the closure of this set, with the same constraint $y = 0$ we only have $x \leq 2$.

A Corollary

Theorem: There exist **essentially conditional** inequalities that hold for almost entropic points.



Theorem [Matúš 07] The cone of linear information inequalities with 4 random variables is **not polyhedral**, i.e., there exist infinitely many independent linear information inequalities.

Conditional Algorithmic Inequalities

even more subtleties

Need to add a precision for conditions: $f(N)$
(where N is the complexity of the tuple of strings)

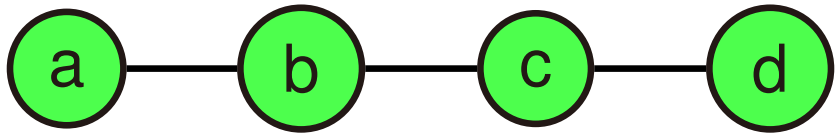
- Some inequalities are valid up to $O(f(N))$
- Some inequalities are valid up to (at least) $O\left(\sqrt{Nf(N)}\right)$
- Some inequalities are not valid ($O(N)$ counterexample)

Information Inequalities and Secret Sharing

Previously, on Secret Sharing.

There exist non-ideal access structures.

The access structure P_4:



is not ideal.

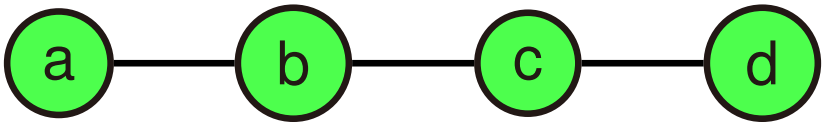
Proposition (Folklore) — proven hereafter

For any scheme, it holds that $\rho \geq \frac{3}{2}$.

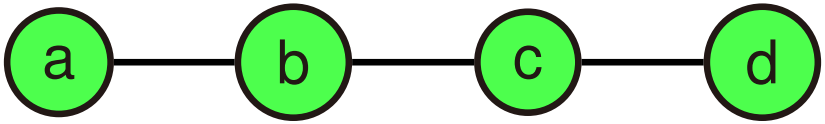
Proposition (Folklore) — proven earlier

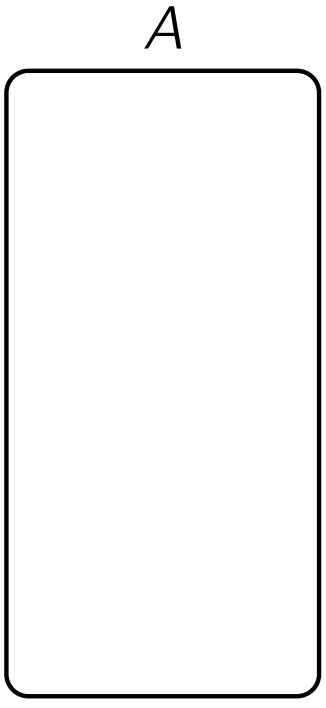
There exists a scheme with information ratio $\rho = \frac{3}{2}$.

Proof by (Venn) Information Diagram

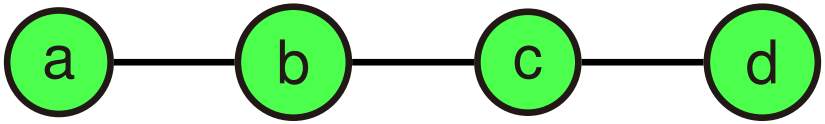


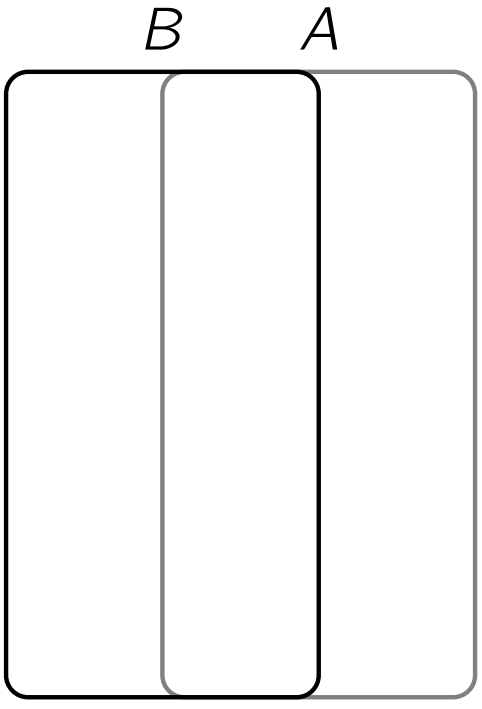
Proof by (Venn) Information Diagram



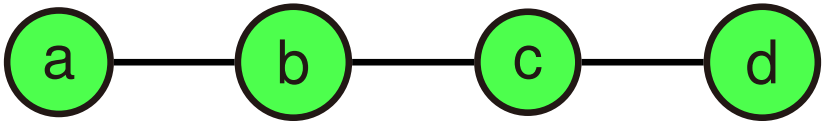


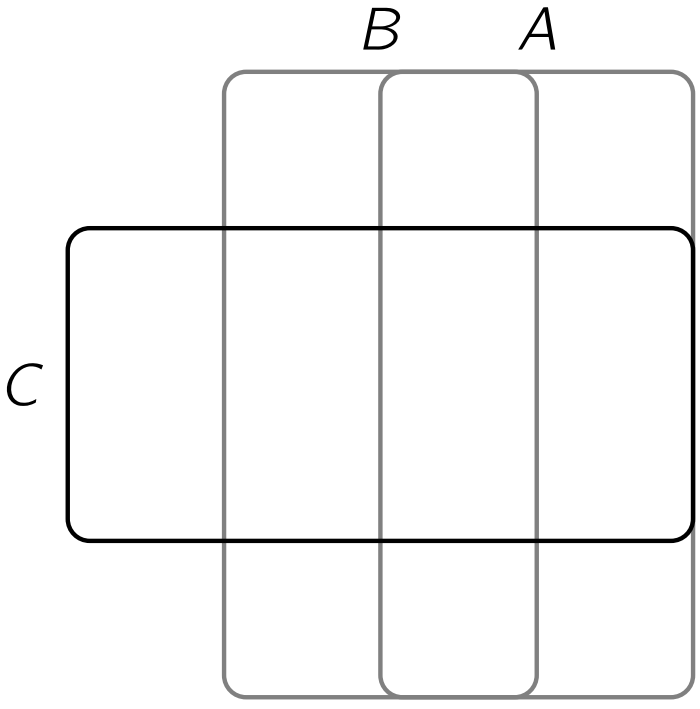
Proof by (Venn) Information Diagram



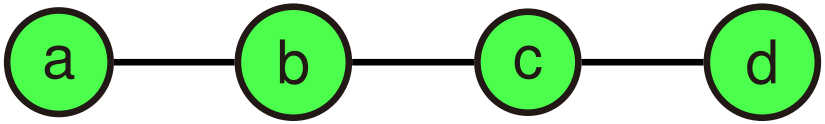


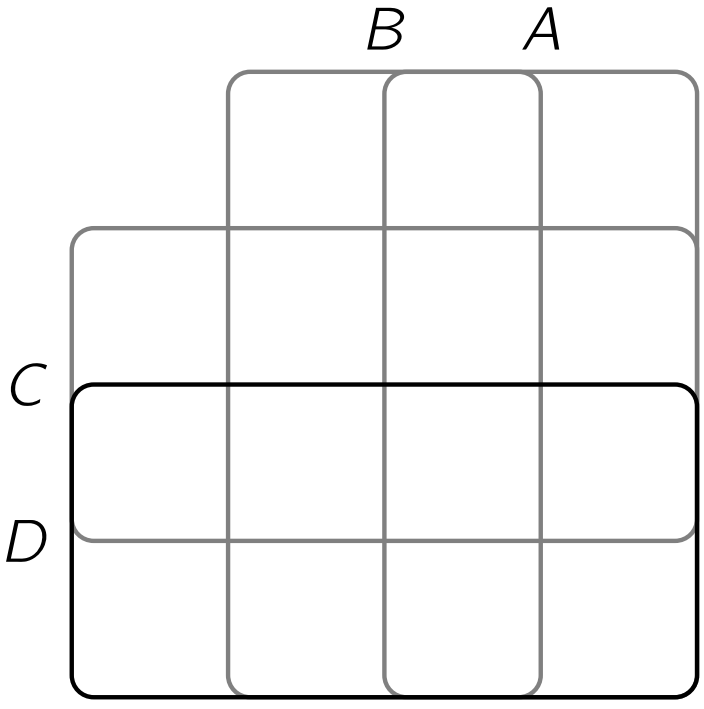
Proof by (Venn) Information Diagram



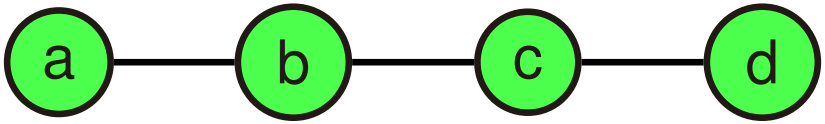


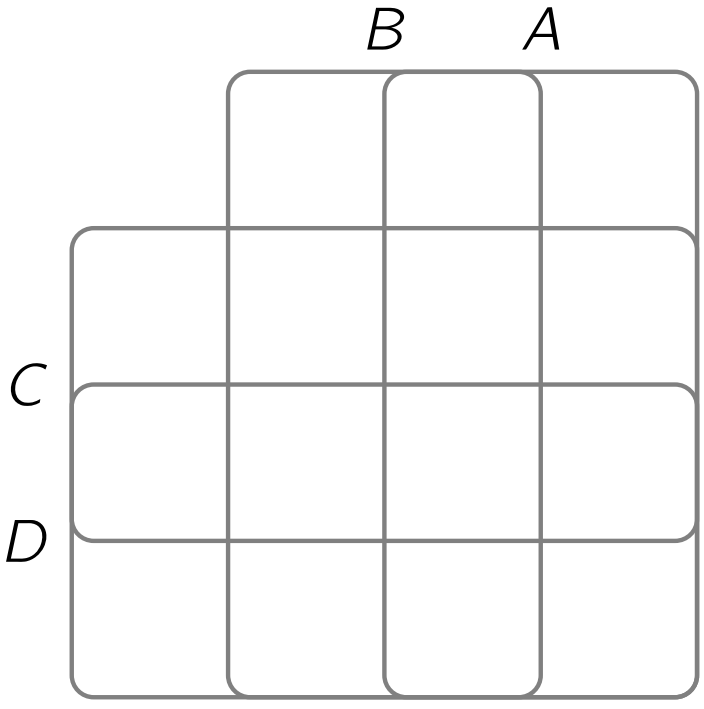
Proof by (Venn) Information Diagram



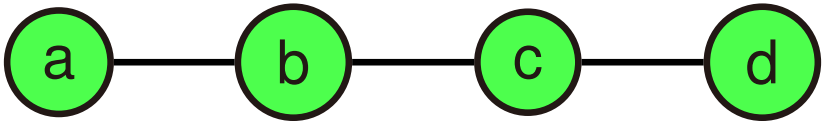


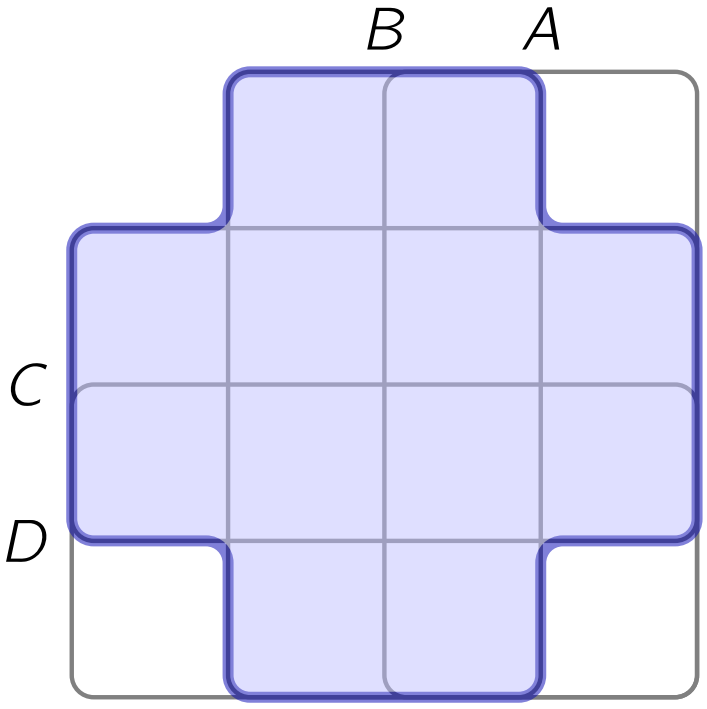
Proof by (Venn) Information Diagram





Proof by (Venn) Information Diagram

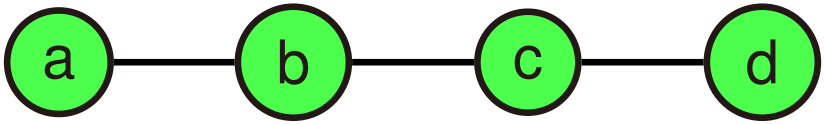


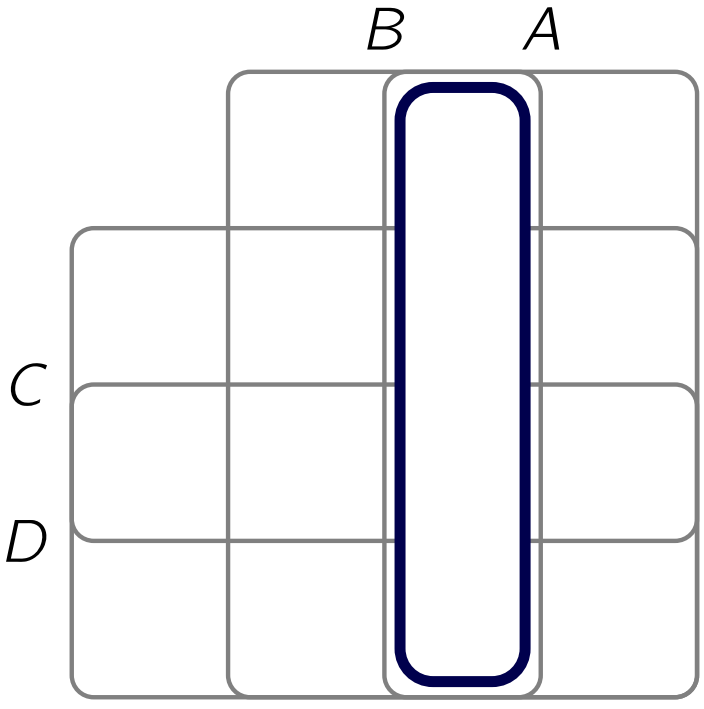


Cells contained in B or C represent:

$$H(BC)$$

Proof by (Venn) Information Diagram

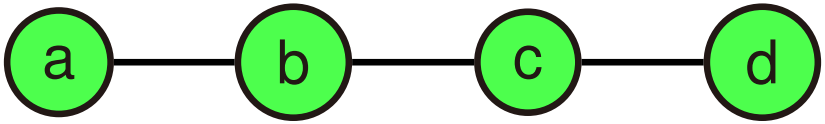


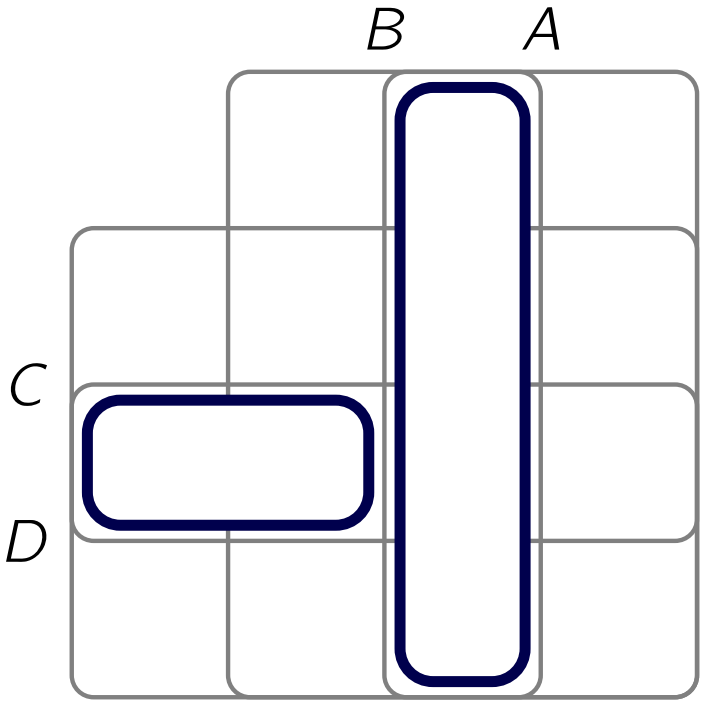


Cells contained in both A and B represent:

$$I(A:B)$$

Proof by (Venn) Information Diagram

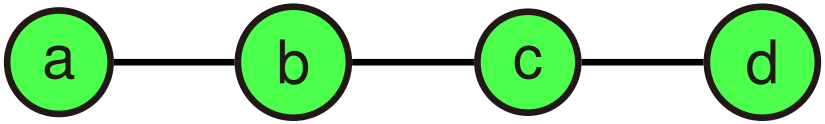


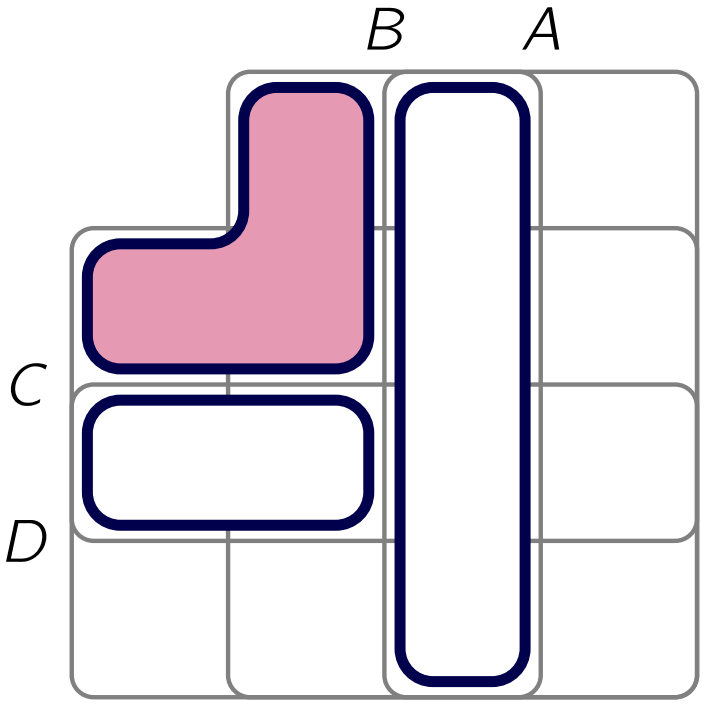


Cells contained in both C and D but not A represent:

$$I(C:D|A)$$

Proof by (Venn) Information Diagram

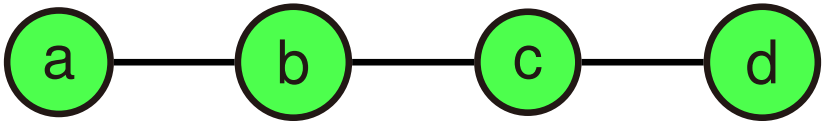


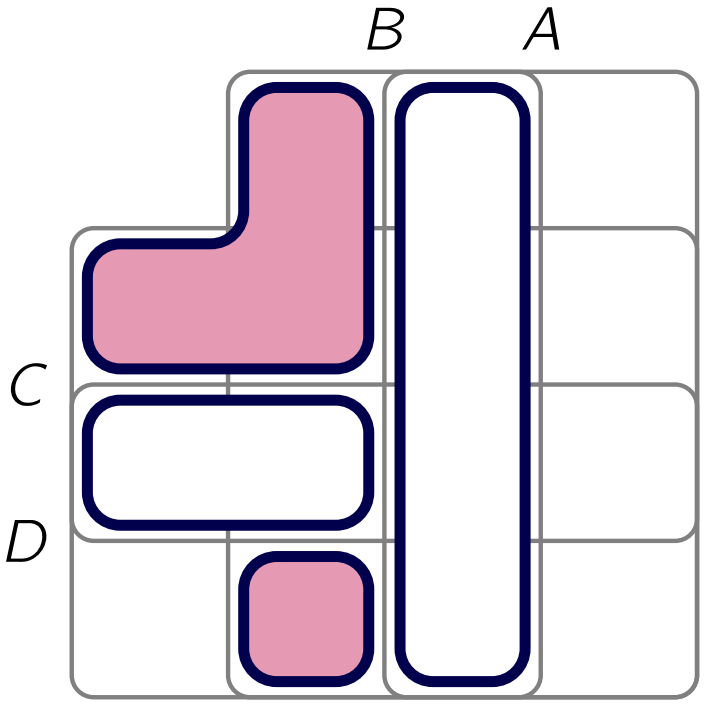


Cells contained in B or C but not A nor D represent:

$$H(BC|AD)$$

Proof by (Venn) Information Diagram

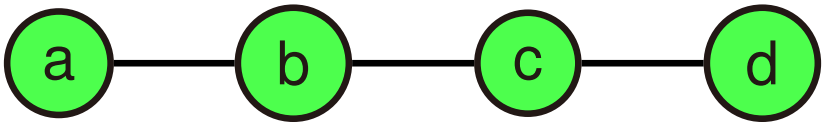


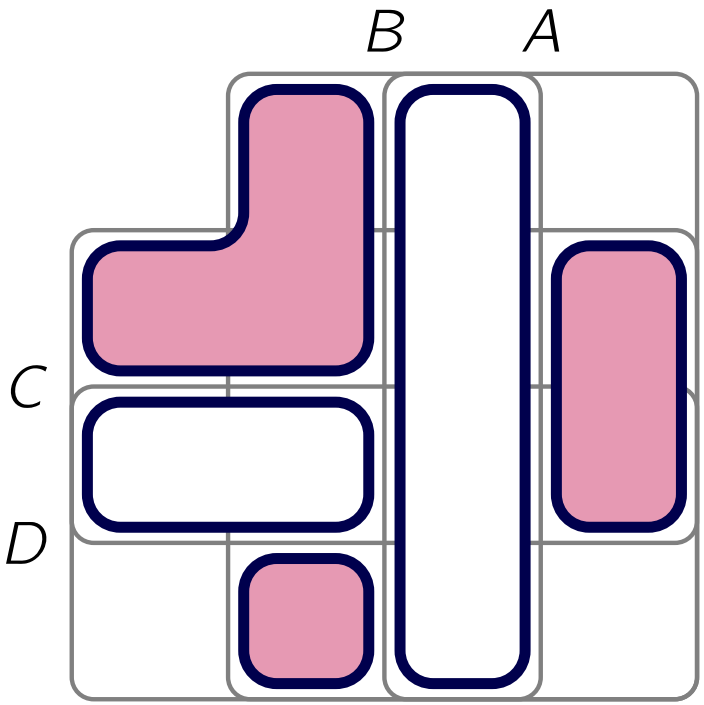


Cells contained in both B and D but not A nor C represent:

$$I(B:D|AC)$$

Proof by (Venn) Information Diagram

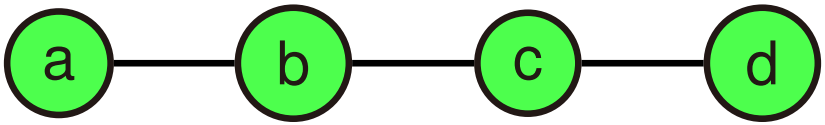


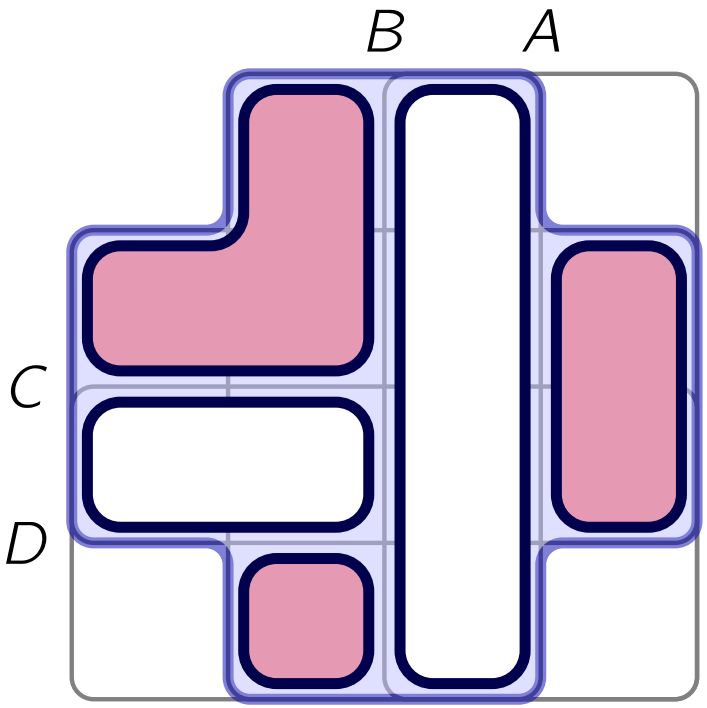


Cells contained in both A and C but not B represent:

$$I(A:C|B)$$

Proof by (Venn) Information Diagram

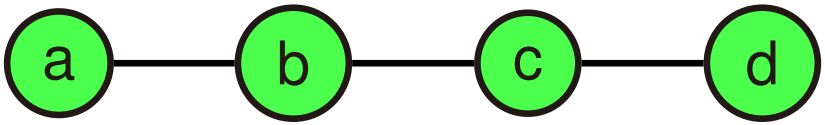


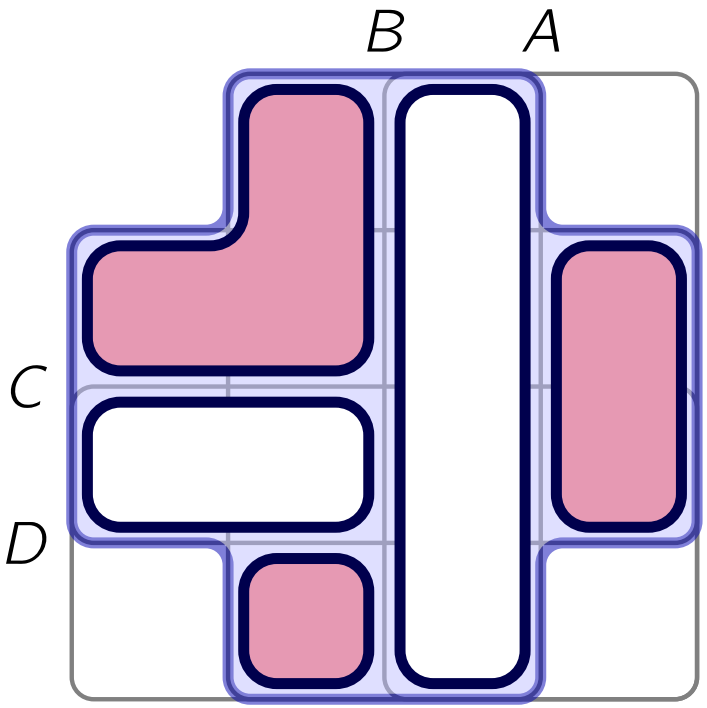


Actually, we just proved an identity without words...

$$H(BC) = I(A{:}C|B) + I(B{:}D|AC) + H(BC|AD) + I(A{:}B) + I(C{:}D|A).$$

Proof by (Venn) Information Diagram

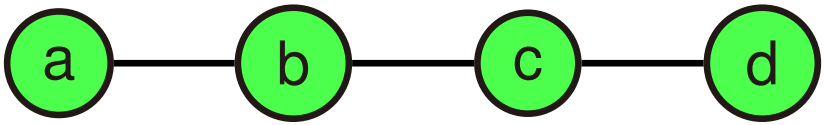


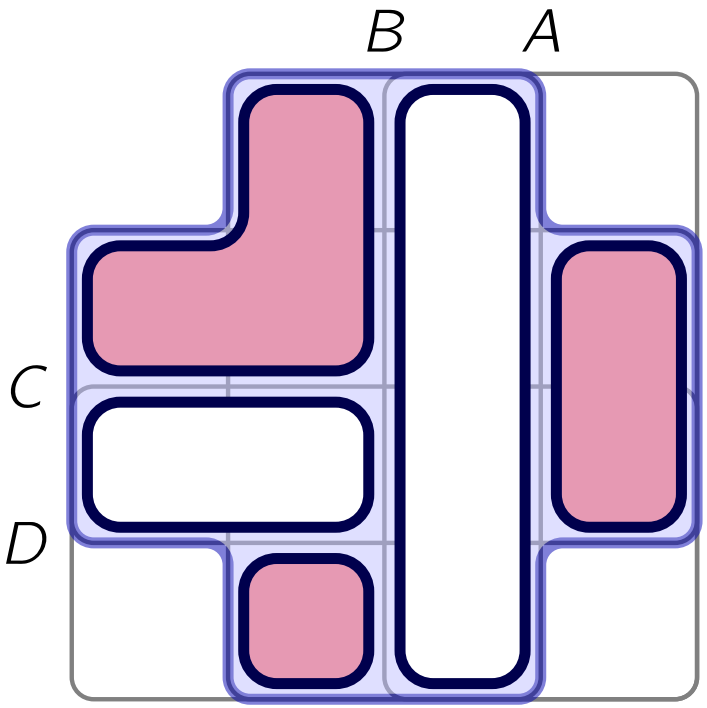


..or an inequality, since all quantities are non-negative.

$$H(BC) \geq I(A{:}C|B) + I(B{:}D|AC) + H(BC|AD).$$

Proof by (Venn) Information Diagram

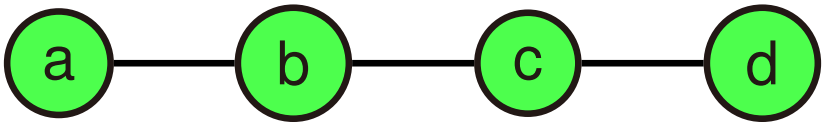


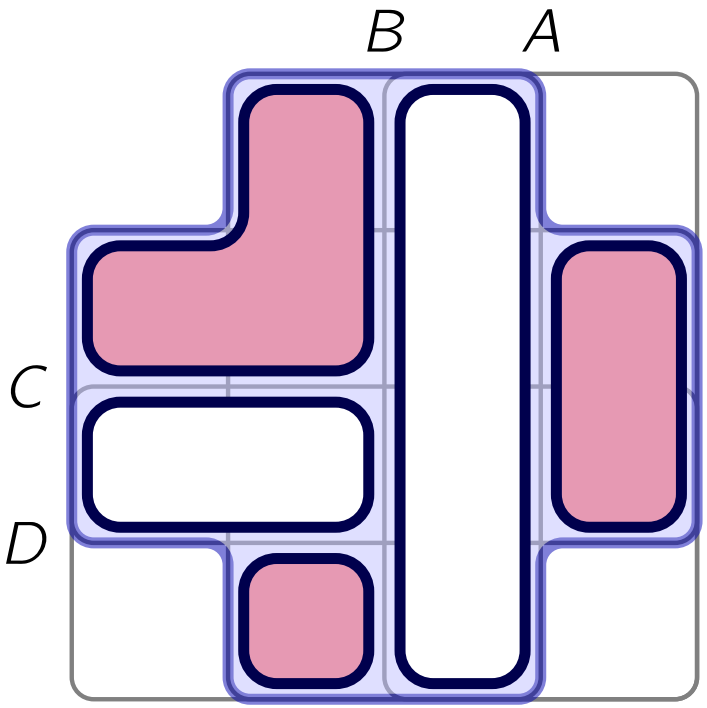


Using the perfect secret sharing requirements, we obtain:

$$H(BC) \geq 3H(S).$$

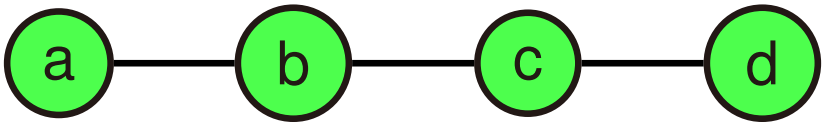
Proof by (Venn) Information Diagram

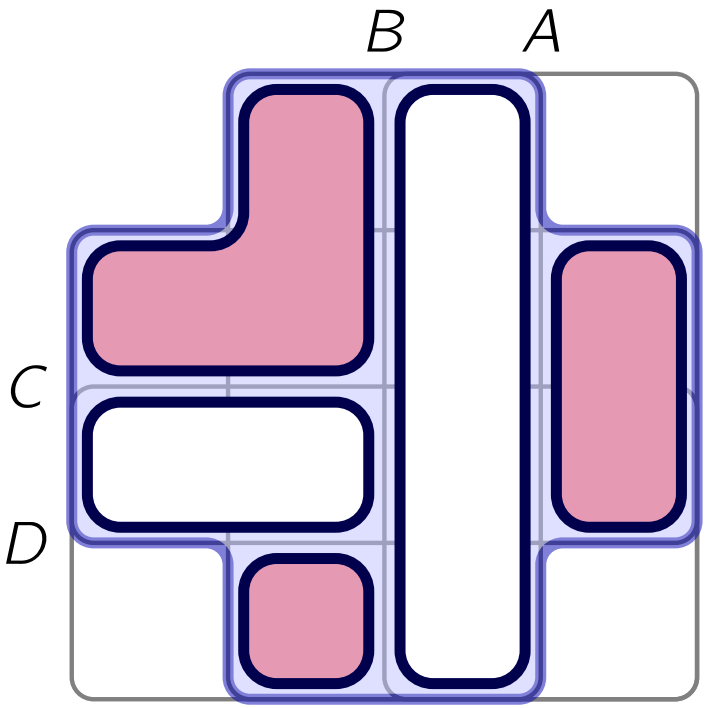




$H(B) \geq 1.5H(S)$ or $H(C) \geq 1.5H(S)$

Proof by (Venn) Information Diagram



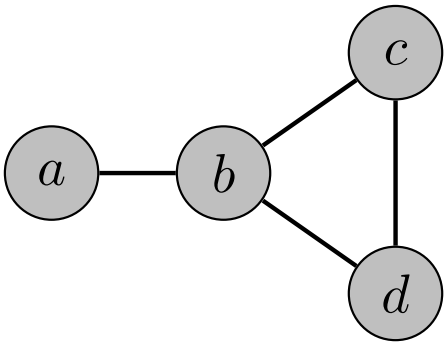


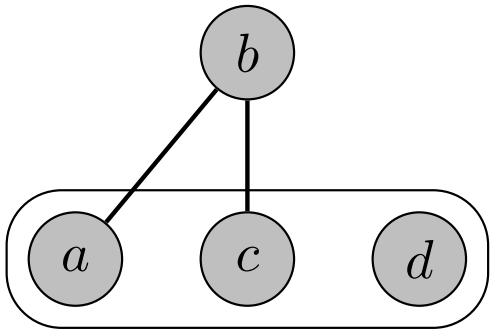
$$\rho(P_4) \geq \frac{3}{2}$$

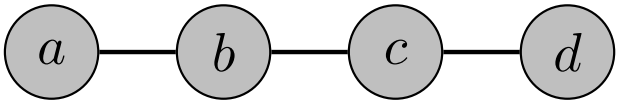
$$H(B) \geq 1.5H(S) \text{ or } H(C) \geq 1.5H(S)$$

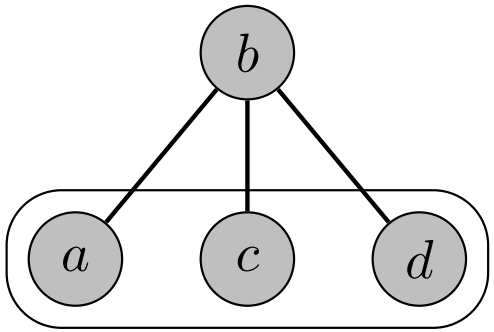
Corollary

The proof is valid for the following access structures









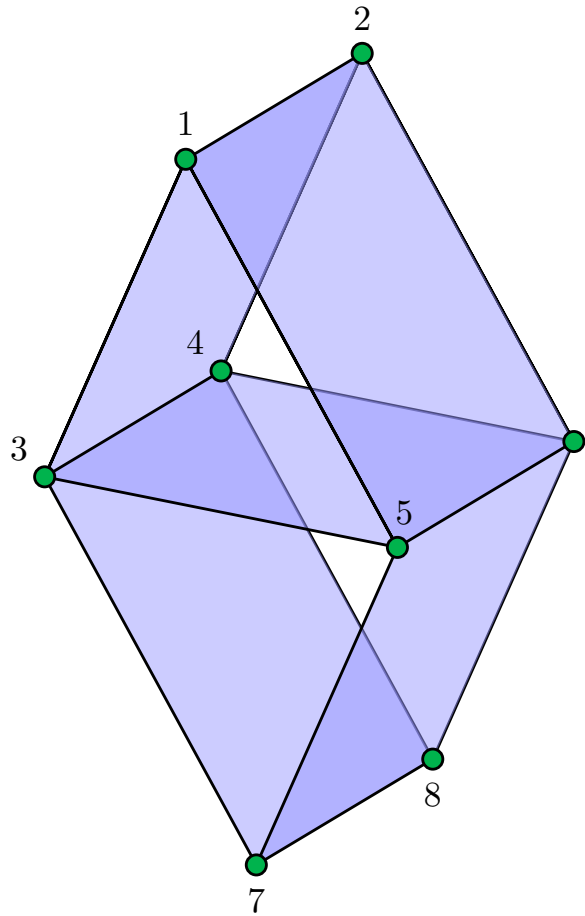
The Vámos matroid is far from ideal

Theorem (Current bounds)

For the two non-isomorphic access structures V_1 and V_6 related to the Vámos matroid:

$$\frac{9}{8} \leq \rho(V_1) \leq \frac{5}{4} \qquad \frac{19}{17} \leq \rho(V_6) \leq \frac{5}{4}$$

The proof is more involved and uses non-Shannon-type inequalities from Zhang-Yeung and Dougherty *et al*.



What is the power of non-Shannon inequalities?

Open question: Do perfect secret sharing schemes require shares of exponential size?

1. Best known Shannon-type lower bound: $\theta\left(\frac{n}{\log n}\right)$.
2. Best possible Shannon-type lower bound: $\theta(n)$
3. Best possible lower bound using (non-Shannon-type) ineq. up to 5 variables: $\theta(n)$

Recent results:

- Using k-variables inequalities: $\theta(\text{poly}(n))$ (Padró preprint)
- Equivalence of the 2 known techniques for non-Shannon-type inequalities (K. submitted)

Prospects & Open Questions

Open questions and future research

1. Can quasi-perfect schemes be substantially more efficient than (plain) perfect schemes?
2. (Related) Can we use essentially conditional inequalities in secret sharing.
3. What are the (asymptotic) properties of optimal secret sharing schemes
4. General picture: study almost entropic points at the boundary of the entropy region.
5. Also, what is the type of one of Matúš' essentially conditional inequality?

Merci de votre attention.

Des questions?