Exploring the Entropic Region

Laszlo Csirmaz

Rényi Institute, Budapest and UTIA, Prague

October 2021

Outline

Secret sharing

How to share the lock code among three people I don't trust?

Secret sharing

How to share the lock code among three people I don't trust?

Alice	4 7 2
Bob	1 5 6
Charlie	6 2 1
Code	1 4 9

Secret sharing

How to share the lock code among three people I don't trust?

Alice	4 7 2
Bob	1 5 6
Charlie	6 2 1
Code	1 4 9

$$\begin{array}{r}
4+1+6=1\,1\\
7+5+2=1\,4\\
2+6+1=\,9
\end{array}$$

Even if two of them colludes, they have no information.

Secret sharing

How to share the lock code among three people I don't trust?

Alice	4 7 2
Bob	1 5 6
Charlie	6 2 1
Code	1 4 9

$$\begin{array}{l} 4+1+6=1\boxed{1} \\ 7+5+2=1\boxed{4} \\ 2+6+1=\ \ \boxed{9} \end{array}$$

Even if two of them colludes, they have no information.

Easily generalizes for n shares.

More difficult structures, e.g., any pair is qualified?

Theorem (Ito–Shaito–Nishizeki, 1987)

Every structure is realizable by a perfect secret sharing scheme.

The price: share size could be exponentially large.

A secret sharing example

Four participants: a, b, c, d; qualified subsets: ab, bc, cd.
The secret $s_1 s_2$ is two bits; x, y, z, t are independent random bits.

a	b	c	d	
x	$x \oplus s_1$	x		
	y	$y \oplus s_2$	y	$\longleftarrow$ secret sharing
z	$z \oplus s_2$	$t \oplus s_1$	t	
2 bits	3 bits	3 bits	2 bits	$\longleftarrow$ share size

The **complexity** of this scheme is

$$\frac{\text{maximal share size}}{\text{secret size}} = \frac{3}{2}.$$

A secret sharing example

Four participants: a, b, c, d; qualified subsets: ab, bc, cd.
The secret $s_1 s_2$ is two bits; x, y, z, t are independent random bits.

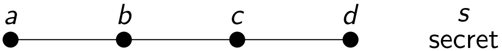
a	b	c	d	
x	$x \oplus s_1$	x		
	y	$y \oplus s_2$	y	$\longleftarrow$ secret sharing
z	$z \oplus s_2$	$t \oplus s_1$	t	
2 bits	3 bits	3 bits	2 bits	$\longleftarrow$ share size

The **complexity** of this scheme is

$$\frac{\text{maximal share size}}{\text{secret size}} = \frac{3}{2}.$$

Can we do better?

Using entropies to show that “no”



ξ and η are **independent** iff $\boldsymbol{H}(\xi\eta) = \boldsymbol{H}(\xi) + \boldsymbol{H}(\eta)$.
ξ **determines** η iff $\boldsymbol{H}(\xi\eta) = \boldsymbol{H}(\xi)$.
So we have

unqualified	qualified
$\boldsymbol{H}(as) = \boldsymbol{H}(a) + \boldsymbol{H}(s)$	$\boldsymbol{H}(abs) = \boldsymbol{H}(ab)$
$\boldsymbol{H}(bs) = \boldsymbol{H}(b) + \boldsymbol{H}(s)$	$\boldsymbol{H}(bcs) = \boldsymbol{H}(bc)$
$\boldsymbol{H}(acs) = \boldsymbol{H}(ac) + \boldsymbol{H}(s)$	$\boldsymbol{H}(abcs) = \boldsymbol{H}(abc)$
$\dots$	$\dots$
$\boldsymbol{H}(bds) = \boldsymbol{H}(bd) + \boldsymbol{H}(s)$	$\boldsymbol{H}(abcds) = \boldsymbol{H}(abcd)$

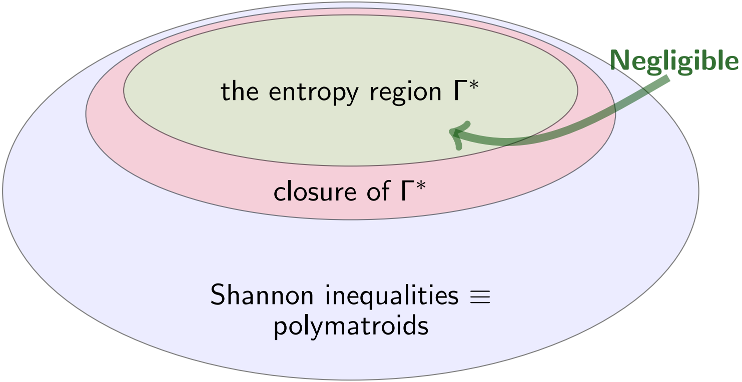
plus all Shannon inequalities, e.g., $\boldsymbol{H}(b)+\boldsymbol{H}(c) \geq \boldsymbol{H}(bc)$,

and derive from them that

one of $\boldsymbol{H}(a)$, $\boldsymbol{H}(b)$, $\boldsymbol{H}(c)$, $\boldsymbol{H}(d)$ is at least $\frac{3}{2}\boldsymbol{H}(s)$.

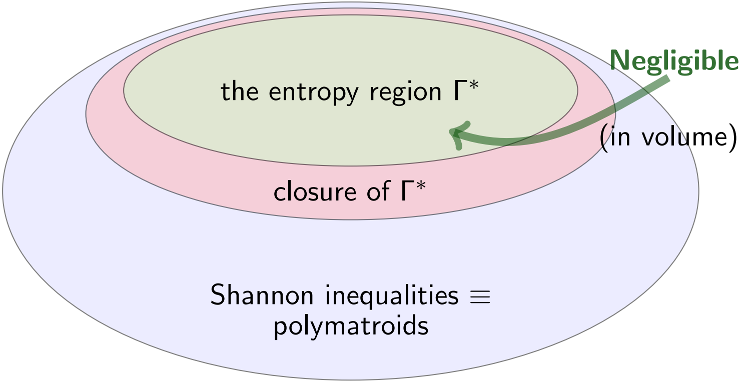
What is the problem?

The Shannon inequalities do not capture the entropy region.



What is the problem?

The Shannon inequalities do not capture the entropy region.



Find new bounds on Γ^*

Outline

Entropy

Let A be a **random variable** taking k values with probability

$$p_1, p_2, \ldots, p_k, \qquad (p_1 + p_2 + \cdots + p_k = 1).$$

The **entropy** of A is

$$\boldsymbol{H}(A) \stackrel{\text{def}}{=} \sum_{i=1}^{k} -p_i \log_2(p_i).$$

Entropy

Let A be a **random variable** taking k values with probability

$$p_1, p_2, \ldots, p_k, \qquad (p_1 + p_2 + \cdots + p_k = 1).$$

The **entropy** of A is

$$\boldsymbol{H}(A) \stackrel{\text{def}}{=} \sum_{i=1}^{k} -p_i \log_2(p_i).$$

The outcome of A can be described by $\boldsymbol{H}(A)$ bits.
$\boldsymbol{H}(A)$ is the **information content** of the event A.

Coin-flipping is 1 bit: $-\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{2}\log_2\frac{1}{2} = 1.$

The entropy region Γ^*

$f : 2^N \to \mathbb{R}$ is **entropic** if there are discrete random variables $\xi = \langle \xi_i : i \in N \rangle$ such that for each marginal $\xi_A = \langle \xi_i : i \in A \rangle$

$$f(A) = \boldsymbol{H}(\xi_A) \qquad A \subseteq N.$$

- The **entropy region** $\Gamma^* \subset \mathbb{R}^{2^N-1}$ is the set all entropic f on subsets of N.
- The **almost entropic** – **aent** region $\bar{\Gamma}^*$ is the closure of Γ^* in the usual Euclidean topology.

An entropic function f is a **polymatroid** since it satisfies

1. $f(\emptyset) = 0$ pointed
2. $f(B) \geq f(A)$ whenever $B \supseteq A$ monotone
3. $f(AC) + f(BC) \geq f(C) + f(ABC)$ submodular (Shannon)

The entropy region Γ^*

$f : 2^N \to \mathbb{R}$ is **entropic** if there are discrete random variables $\xi = \langle \xi_i : i \in N \rangle$ such that for each marginal $\xi_A = \langle \xi_i : i \in A \rangle$

$$f(A) = \boldsymbol{H}(\xi_A) \qquad A \subseteq N.$$

- The **entropy region** $\Gamma^* \subset \mathbb{R}^{2^N-1}$ is the set all entropic f on subsets of N.
- The **almost entropic** – **aent** region $\bar{\Gamma}^*$ is the closure of Γ^* in the usual Euclidean topology.

An entropic function f is a **polymatroid** since it satisfies

1. $f(\emptyset) = 0$ pointed
2. $f(B) \geq f(A)$ whenever $B \supseteq A$ monotone
3. $f(A, B|C) \geq 0$ submodular (Shannon)

How to define a distribution?

Simplest method: list the values and the probabilities.

ξ_1	ξ_2	$\dots$	ξ_n	Prob
u_1	v_1	$\dots$	z_1	p_1
u_2	v_1	$\dots$	z_1	p_2
u_1	v_2	$\dots$	z_1	p_3
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
u_j	v_k	$\dots$	z_ℓ	p_s

The probabilities sum to 1:
$\sum p_i = 1$.

How to define a distribution?

Simplest method: list the values and the probabilities.

ξ_1	ξ_2	$\dots$	ξ_n	Prob
u_1	v_1	$\dots$	z_1	p_1
u_2	v_1	$\dots$	z_1	p_2
u_1	v_2	$\dots$	z_1	p_3
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
u_j	v_k	$\dots$	z_ℓ	p_s

An example: the *ringing bells*

How to define a distribution?

Simplest method: list the values and the probabilities.

ξ_1	ξ_2	...	ξ_n	Prob
u_1	v_1	...	z_1	p_1
u_2	v_1	...	z_1	p_2
u_1	v_2	...	z_1	p_3
...	...	...	...	...
u_j	v_k	...	z_ℓ	p_s

The probabilities sum to 1: $\sum p_i = 1$.

An example: the *ringing bells*

We have two ropes, c and d. When **any of them** is pulled, a rings, when **both** are pulled, b rings. Pull each rope independently with $1/2$ probability.

a	b	c	d	Prob
0	0	0	0	1/4
1	0	0	1	1/4
1	0	1	0	1/4
1	1	1	1	1/4

Marginals

To get the marginal for a subset of variables: take their columns, merge identical rows, and sum the probabilities.

Original ($abcd$)

a	b	c	d	Prob
0	0	0	0	1/4
1	0	0	1	1/4
1	0	1	0	1/4
1	1	1	1	1/4

Marginal (bc)

b	c	Prob
0	0	1/2
0	1	1/4
1	1	1/4

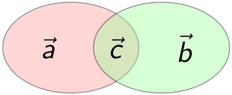
Marginal (ab)

a	b	Prob
0	0	1/4
1	0	1/2
1	1	1/4

The entropy is $\boldsymbol{H} = \sum_i -p_i \log_2(p_i)$. Since $-(1/4)\log_2(1/4) = 1/2, \quad -(1/2)\log_2(1/2) = 1/2$, thus we have

$$\boldsymbol{H}(abcd) = 2, \qquad \boldsymbol{H}(bc) = 3/2, \qquad \boldsymbol{H}(ab) = 3/2.$$

Redefining a distribution



Variables:	$\vec a, \vec c, \vec b$
Probabilities:	$P = (\vec a\vec c\vec b)$
Marginals:	$(\vec a\vec c) = \sum_{\vec b}(\vec a\vec c\vec b)$
	$(\vec c\vec b) = \sum_{\vec c}(\vec a\vec c\vec b)$
	$(\vec c) = \sum_{\vec a,\vec b}(\vec a\vec c\vec b)$
New probabilities:	$P^* = \dfrac{(\vec a\vec c)\,(\vec c\vec b)}{(\vec c)}$

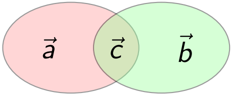
Marginals of P and P^* on $\vec a\vec c$ and $\vec c\vec b$ are the same.

The entropy change is

$$\boldsymbol{H}(P^*) - \boldsymbol{H}(P) = -\sum \frac{(\vec a\vec c)\,(\vec c\vec b)}{(\vec c)} \log \frac{(\vec a\vec c)\,(\vec c\vec b)}{(\vec c)} + \sum(\vec a\vec c\vec b)\log(\vec a\vec c\vec b)$$
$$= \boldsymbol{H}(\vec a,\vec b|\vec c) \geq 0.$$

Zero iff $\vec a$ and $\vec b$ are independent given $\vec c$, and then $P = P^*$

Merging two distributions



Variables: $\vec a\vec c$ and $\vec c\vec b$

Probabilities: $(\vec a\vec c)$ and $(\vec c\vec b)$

Marginals are the same on $(\vec c)$:

$$\textstyle\sum_{\vec a}(\vec a\vec c) = \sum_{\vec b}(\vec c\vec b)$$

Joint probabilities: $P^* = \dfrac{(\vec a\vec c)\,(\vec c\vec b)}{(\vec c)}$

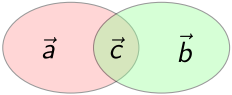
After merging, $\vec a$ and $\vec b$ become independent given $\vec c$, that is,

$$\boldsymbol{H}(\vec a,\vec b|\vec c) = 0.$$

A structural property of entropic polymatroids

Any two entropic polymatroids on XM and MY with the same distribution on M have an amalgam on XMY with $(X,Y|M)=0$.

Merging two distributions



Variables: $\vec a\vec c$ and $\vec c\vec b$

Probabilities: $(\vec a\vec c)$ and $(\vec c\vec b)$

Marginals are the same on $(\vec c)$:

$$\textstyle\sum_{\vec a}(\vec a\vec c) = \sum_{\vec b}(\vec c\vec b)$$

Joint probabilities: $P^* = \dfrac{(\vec a\vec c)\,(\vec c\vec b)}{(\vec c)}$

After merging, $\vec a$ and $\vec b$ become independent given $\vec c$, that is,

not the same entropies $\vec b|\vec c) = 0$.

A structural property of entropic polymatroids

Any two entropic polymatroids on XM and MY with the same distribution on M have an amalgam on XMY with $(X, Y|M) = 0$.

Outline

Operations

1. Polymatroids are vectors $\Rightarrow$ **linear combination**.
2. **Direct union** with rank $f(A \cap N_f) + g(A \cap N_g)$.
3. Discard the subset $T \subseteq N \Rightarrow$ **contract**
4. Factor over an equivalence on $N \Rightarrow$ **factoring**
5. Restrict to $N - T \Rightarrow$ **restriction**
6. **Tightening** (next slide)
7. **Principal extension**, and many more ...

Operations

1. Polymatroids are vectors $\Rightarrow$ **linear combination**.
2. **Direct union** with rank $f(A\cap N_f)+g(A\cap N_g)$.
3. Discard the subset $T\subseteq N$ $\Rightarrow$ **contract**
4. Factor over an equivalence on N $\Rightarrow$ **factoring**
5. Restrict to $N-T$ $\Rightarrow$ **restriction**
6. **Tightening** (next slide)
7. **Principal extension**, and many more ...

The general idea

Find operations which **preserve** entropic (or aent) polymatroids but **don't preserve** general polymatroids.

Tightening

$\lambda \boldsymbol{r}_A$ is **entropic polymatroid** for $A \subseteq N$ and $\lambda \geq 0$, where

$$\boldsymbol{r}_A : J \to \begin{cases} 0 & \text{if } A \cap J = \emptyset, \\ 1 & \text{if } A \cap J \neq \emptyset. \end{cases}$$

$f + \lambda \boldsymbol{r}_a \Rightarrow a \in N$ gets λ information
$f - \lambda \boldsymbol{r}_a \Rightarrow$ take away λ information from a

Definition (Tightening)

Take away as much private information as possible:

$$f{\downarrow}a = f - \lambda \boldsymbol{r}_a \text{ for maximal } \lambda \text{ such that } f - \lambda \boldsymbol{r}_a \geq 0.$$

To get $f{\downarrow}$, tighten at every $a \in N$.

Clearly, if f is polymatroid, then so is $f{\downarrow}$.

Theorem (Frantisek Matúš)

If f is almost entropic, then so is $f{\downarrow}$.

Operations

Operation	polymatroid	entropic	aent
Sum $f+g$	✓	✓	✓
Direct union $f\oplus g$	✓	✓	✓
Scaling λf	✓	✗	✓
Conic $\sum\lambda_i f_i$	✓	✗	✓
Factoring $f/\sim$	✓	✓	✓
Restriction $f\backslash T$	✓	✓	✓
Contraction f/T	✓	✗	✓
Tightening $f{\downarrow}$	✓	✗	✓
Principal extension	✓	✗	✓

None of them works! Fortunately

Operations

Operation	**polymatroid**	**entropic**	**aent**
Sum $f+g$	✓	✓	✓
Direct union $f \oplus g$	✓	✓	✓
Scaling λf	✓	✗	✓
Conic $\sum \lambda_i f_i$	✓	✗	✓
Factoring $f/\sim$	✓	✓	✓
Restriction $f \backslash T$	✓	✓	✓
Contraction f/T	✓	✗	✓
Tightening $f\downarrow$	✓	✗	✓
Principal extension	✓	✗	✓
M.E.P. embedding	✗	✓	✓
Copy lemma	✗	✓	✓
Ahlswede-Körner	✗	✗	✓

Outline

Maximum entropy principle

We have random variables with **unknown** joint probabilities, but

ξ_1	ξ_2	$\dots$	ξ_M	Prob
u_1	v_1	$\dots$	z_1	?
u_2	v_1	$\dots$	z_1	?
u_1	v_2	$\dots$	z_1	?
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
u_j	v_k	$\dots$	z_ℓ	?

known marginal distributions on $J_1, J_2, \dots \subset M$.

$\Rightarrow$ linear constraints on the unknown probabilities

$\Rightarrow \mathcal{Q} =$ all distributions satisfying these constraints.

Maximum entropy principle

We have random variables with **unknown** joint probabilities, but

ξ_1	ξ_2	...	ξ_M	Prob
u_1	v_1	...	z_1	?
u_2	v_1	...	z_1	?
u_1	v_2	...	z_1	?
...	...	...	...	...
u_j	v_k	...	z_ℓ	?

known marginal distributions on $J_1, J_2, \dots \subset M$.

$\Rightarrow$ linear constraints on the unknown probabilities

$\Rightarrow \mathcal{Q} =$ all distributions satisfying these constraints.

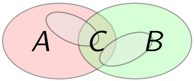
Choose $P \in \mathcal{Q}$ with maximum entropy

As the entropy is strictly convex, there is a unique solution.

M.E.P. (in physics, statistics, philosophy, etc.) If you face uncertainty, your best bet is to take the distribution with the largest entropy — the one with maximum uncertainty.

The M.E.P. heuristics

- $\langle \xi_i : i \in M \rangle$ is the M.E. extension using the marginal distributions on $J_1, J_2, \dots \subset M$.
- $f(A) = \boldsymbol{H}(\xi_A)$ for $A \subseteq M$.



Claim

Let $A \cup C \cup B = M$ be a partition of M such that for each J_i, either $J_i \subseteq A \cup C$ or $J_i \subseteq C \cup B$. Then $f(A, B \mid C) = 0$.

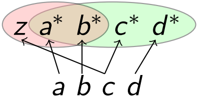
Proof.

If not, you can redefine the distribution with larger entropy and the same marginals on each J_i. $\square$

M.E.P. heuristics

Entropic polymatroids can be embedded into (entropic) polymatroids with this additional structural property.

The Zhang–Yeung inequality from M.E.P.



1. Take an entropic polymatroid on *abcd*. Embed it into $za^*b^*c^*d^*$ so that

- za^*b^* has the same distribution as *cab*
- $a^*b^*c^*d^*$ has the same distribution as *abcd*
- with these constraints $za^*b^*c^*d^*$ has maximum entropy.

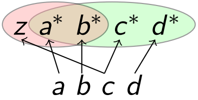
2. The partition $\overset{A}{z} \cup \overset{C}{a^*b^*} \cup \overset{B}{c^*d^*}$ satisfies the requirement that each fixed marginal is either in AC or in CB, thus $(z, c^*d^* \,|\, a^*b^*) = 0$.

3. The following inequality holds in every polymatroid[1]:

$$-(a^*, b^*) + (a^*, b^* \,|\, c^*) + (a^*, b^* \,|\, d^*) + (c^*, d^*) +$$
$$+ (a^*, b^* \,|\, z) + (a^*, z \,|\, b^*) + (b^*, z \,|\, a^*) \geq -3(z, c^*d^* \,|\, a^*b^*).$$

[1]See https://www.personal.ceu.edu/witip

The Zhang–Yeung inequality from M.E.P.



1. Take an entropic polymatroid on *abcd*. Embed it into $za^*b^*c^*d^*$ so that

- za^*b^* has the same distribution as *cab*
- $a^*b^*c^*d^*$ has the same distribution as *abcd*
- with these constraints $za^*b^*c^*d^*$ has maximum entropy.

2. The partition $\overset{A}{z} \cup \overset{C}{a^*b^*} \cup \overset{B}{c^*d^*}$ satisfies the requirement that each fixed marginal is either in AC or in CB, thus $(z, c^*d^*|a^*b^*) = 0$.

3. The following inequality holds in every polymatroid[1]:

$$-(a^*,b^*) + (a^*,b^*|c^*) + (a^*,b^*|d^*) + (c^*,d^*) +$$
$$+(a^*,b^*|z) + (a^*,z|b^*) + (b^*,z|a^*) \geq \cancel{-3(z,c^*d^*|a^*b^*)}.$$

4. Because corresponding marginals are equal, *abcd* satisfies

$$-(a,b)+(a,b|c)+(a,b|d)+(c,d)+(a,b|c)+(a,c|b)+(b,c|a) \geq 0.$$

[1] See https://www.personal.ceu.edu/witip

Witip

wITIP

This is **wITIP**, a web based Information Theoretic Inequality Prover.

Please specify your session ID to start working. The ID should start with a letter or hash tag; your name or your e-mail address is a good choice.

Your session ID

UTIA

CONTINUE

wITIP | **config** | **macros** | **constraints** | **check** | **session**

session ID: **UTIA ***

	true	`-(a,b)+(a,b|c)+(a,b|d)+(c,d)+(a,b|z)+(a,z|b)+(b,z|a)>=-3(z,cd|ab)`
	true	`z'<=(a,b|c)+(a,b|d)+(c,d)+2{az'+bz'-a-b}`

check `z'<=(a,b|c)+(a,b|d)+(c,d)+2{az'+bz'-a-b}`

A special case: the Copy Lemma

f is a polymatroid on N, and $N = X \cup M$ is a partition.

Lemma (Copy Lemma)

if f is entropic, then there is an entropic extension g to $X' \cup X \cup M$ such that

(i) $g{\restriction}(X' \cup M)$ *is isomorphic to* $f = g{\restriction}(X \cup M)$, *and*

(ii) $g(X', X \,|\, M) = 0$.

Proof Take the maximum entropy extension on $X'XM$ which satisfies (i). $\square$

Remark As g is also entropic, the Copy Lemma can be iterated

$$\Longleftrightarrow$$

g satisfies additional inequalities generated by the Copy Lemma

Outline

What is it?

An intermediate result in an Ahlswede–Körner paper was extracted and used by MMRV, and finally formulated by Kaced:

Lemma (Ahlswede–Körner lemma)

Suppose f is entropic on $MX \cup \{z\}$. There is an almost entropic extension to $MX \cup \{z, z'\}$ such that $f(z'M) = f(M)$, and $f(z'A) = f(zA) - f(zM) + f(M)$ for all $A \subseteq M$. $\square$

R. Ahlswede, J. Körner (1975) Source coding with side information and a converse for degraded broadcast channels. *IEEE trans. on Inf Theory* **21**(6) 629–637.

K. Makarychev, Yu. Makarychev, A. Romashchenko, N. Vereshchagin (2002) A new class of non-Shannon-type inequalities for entropies. *Comm. in Inf. and Systems* **2**(2) 147–166.

T. Kaced (2013) Equivalence of two proof techniques for non-Shannon-type inequalities. *Proceedings of the 2013 IEEE ISIT*, Istanbul, Turkey, July 7-12, 236–240.

Ahlswede–Körner lemma in action

Lemma (Repeated)

Suppose f is entropic on $MX \cup \{z\}$. There is an almost entropic extension to $MX \cup \{z, z'\}$ such that $f(z'M) = f(M)$, and $f(z'A) = f(zA) - f(zM) + f(M)$ for all $A \subseteq M$. □

Use $M = \{a, b\}$, $X = \{d\}$, and $z = c$. In the $z'abcd$ extension[1]

$$f(z') \le f(a, b|c) + f(a, b|d) + f(c, d) + \\ + 2\big(f(az') + f(z'b) - f(a) - f(b)\big).$$

Using that

$$f(z'J) = f(cJ) - f(abc) + f(ab) \quad \text{for} \quad J \subseteq \{a, b\},$$

this rewrites to the Zhang-Yeung inequality

$$-(a, b)+(a, b|c)+(a, b|d)+(c, d)+(a, b|c)+(a, c|b)+(b, c|a) \ge 0.$$

[1]See http://www.personal.ceu.edu/witip

Proof of the A–K lemma

Lemma (Repeated)

Suppose f is entropic on $MX \cup \{z\}$. There is an almost entropic extension to $MX \cup \{z, z'\}$ such that $f(z'M) = f(M)$, and $f(z'A) = f(zA) - f(zM) + f(M)$ for all $A \subseteq M$.

Proof

1. Extend f to $M \cup Xz \cup X'z'$ using the Copy Lemma. Then $g(Xz, X'z'|M) = 0 \quad \Rightarrow \quad g(Xz, z'|M) = 0$.
2. Restrict the extension to $M \cup Xz \cup z'$. Then $g(z'A) = f(zA)$ for $A \subseteq M$, and independence gives
$$g(MXzz') - g(MXz) = g(Mz') - g(M) = f(zM) - f(M).$$
3. Tighten g at z' by $\lambda =$. This $g{\downarrow_{z'}}$ extends f and
$$g{\downarrow_{z'}}(z'A) = g(z'A) - \lambda = f(zA) - \lambda,$$

thus $g{\downarrow_{z'}}$ is a good A–K extension. $\square$

Direct proof of the A–K lemma

1. Use typical sequences to make $M \times \{z\}$ to be quasi-uniform: each non-zero cell has the same probability; rows, columns have equal number of x-es
2. Make $|M|$ and $|z|$ large.
3. Choose rows randomly so that each column contains *exactly one* non-zero cell (except for $\varepsilon|M|$ columns).
4. z' is determined by M via the chosen rows.

M

	X		X		X
X				X	X
		X	X	X	
X	X	X			

z

Then

• $\boldsymbol{H}(z'M) = \boldsymbol{H}(M)$ as M determines z'.
• $\boldsymbol{H}(z'A) - \boldsymbol{H}(zA)$ is constant as each row contains the same number of non-empty cells even in columns corresponding to the subset A. $\square$

Outline

The methods

1. Maximum entropy method
   Given an entropic polymatroid on N, label elements of M by N, and choose $\mathcal{J} \subset 2^N$ with each $J \in \mathcal{J}$ has different labels. Require all $J \in \mathcal{J}$ to be isomorphic to its labels. Compute all conditional independences, and compute the consequences on N.
2. Copy Lemma
   A simple version of MaxEnt: choose a subset of N, and take a copy of the rest. Compute all consequences.
3. Ahlswede–Körner method
   Take the A–K extension of N and compute its consequences.

All methods can be iterated, which is the same as using established knowledge on the larger (almost) entropic polymatroid.

None of the methods distinguishes entropic and almost entropic polymatroids.

Ahlswede-Körner method

Theorem

(a) *All results provided by the A–K method are also given by a single application of the Copy Lemma.*

(b) *There is a single application of the Copy Lemma which is stronger than two iterations of the A–K method.*

Actually, we have an exact characterization of the strength of the A–K method: it is equivalent to a restricted application of the Copy Lemma, which, in turn, is weaker than the full strength Copy Lemma.

Maximum Entropy method

Clearly, the Copy Lemma is a special case of MaxEnt.
The iterated Copy Lemma uses local manipulation, while MaxEnt applies to a global arrangement.

Maximum Entropy method

Clearly, the Copy Lemma is a special case of MaxEnt.
The iterated Copy Lemma uses local manipulation, while MaxEnt applies to a global arrangement.

Theorem (L. Csirmaz, 2021)

The MaxEnt method is equivalent to the iterated usage of the Copy Lemma.

The easy direction is a simulation of the iterated Copy lemma using some complicated MaxEnt arrangement.
The hard direction uses induction on the number of conditional independences used in the MaxEnt method.

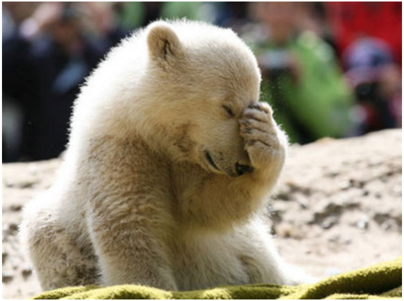
And the winner is . . .

No other methods are known which work for a wide range of polymatroids (and not for a sporadic set only). By these results, everything which can be proved using these methods, can be proved using the Copy Lemma only.

By exploiting the underlying symmetry provided by the Copy Lemma, several otherwise untractable problems can be solved numerically.

So our winner is the

Copy Lemma



Děkuji za pozornost