On Essentially Conditional Information Inequalities

Tarik Kaced[1] and Andrei Romashchenko[2]

[1]LIF de Marseille, Univ. Aix-Marseille
[2]CNRS, LIF de Marseille & IITP of RAS (Moscow)

ISIT 2011, August 4

Linear information inequalities

Linear information inequalities

Basic inequalities:

$$H(a, b) \leq H(a) + H(b) \qquad [I(a : b) \geq 0]$$

Linear information inequalities

Basic inequalities:

$$H(a,b) \le H(a) + H(b) \qquad [I(a:b) \ge 0]$$
$$H(a,b,c) + H(c) \le H(a,c) + H(b,c) \qquad [I(a:b\,|\,c) \ge 0]$$

Linear information inequalities

Basic inequalities:

$$H(a,b) \le H(a) + H(b) \qquad [I(a:b) \ge 0]$$
$$H(a,b,c) + H(c) \le H(a,c) + H(b,c) \qquad [I(a:b\,|\,c) \ge 0]$$

Shannon type inequalities [combinations of basic ineq]:

example 1: $H(a) \le H(a\,|\,b) + H(a\,|\,c) + I(b:c)$

example 2: $2H(a,b,c) \le H(a,b) + H(a,c) + H(b,c)$

Linear information inequalities

General form: A linear information inequality is a combination of reals $\{\lambda_{i_1,\dots,i_k}\}$ such that

$$\sum \lambda_{i_1,\dots,i_k} H(a_{i_1},\dots,a_{i_k}) \geq 0$$

for all $(a_1,\dots,a_n)$.

Linear information inequalities

General form: A linear information inequality is a combination of reals $\{\lambda_{i_1,\dots,i_k}\}$ such that

$$\sum \lambda_{i_1,\dots,i_k} H(a_{i_1},\dots,a_{i_k}) \geq 0$$

for all $(a_1,\dots,a_n)$.

Applications:

- multi-source network coding
- secret sharing
- combinatorial interpretations
- group theoretical interpretation
- Kolmogorov complexity
- ...

Shannon type information inequalities:

- subadditivity $H(A \cup B) \leq H(A) + H(B)$,
- submodularity
  $H(A \cup B \cup C) + H(C) \leq H(A \cup C) + H(B \cup C)$,
- combinations of basic inequalities

Shannon type information inequalities:

- subadditivity $H(A \cup B) \leq H(A) + H(B)$,
- submodularity
$H(A \cup B \cup C) + H(C) \leq H(A \cup C) + H(B \cup C)$,
- combinations of basic inequalities

Th [Z. Zhang, R.W. Yeung 1998] There exists a non-Shannon type information inequality:

$$\begin{aligned} I(c:d) \ \leq \ & 2I(c:d\,|\,a) + I(c:d\,|\,b) + I(a:b) \\ & + I(a:c\,|\,d) + I(a:d\,|\,c) \end{aligned}$$

Theorem [Z. Zhang, R.W. Yeung 1997] There exists a conditional non Shannon type inequality:

$$I(a:b) = I(a:b\,|\,c) = 0$$

$$\Downarrow$$

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

Conditional information inequalities

(a) **Trivial, Shannon-type**:

if $I(a:b) = 0$ then $H(c) \le H(c \mid a) + H(c \mid b)$

Conditional information inequalities

(a) **Trivial, Shannon-type**:

if $I(a:b)=0$ then $H(c) \leq H(c \mid a) + H(c \mid b)$

this is true since $H(c) \leq H(c \mid a) + H(c \mid b) + I(a:b)$
[Shannon-type unconditional inequalitiy]

Conditional information inequalities

(b) **Trivial, non Shannon-type**:

if $I(c:d\,|\,e) = I(e:c\,|\,d) = I(e:d\,|\,c) = 0$ then

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

Conditional information inequalities

(b) **Trivial, non Shannon-type**:

if $I(c:d\,|\,e) = I(e:c\,|\,d) = I(e:d\,|\,c) = 0$ then

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

this is true since

$$\begin{aligned} I(c:d) \;\; \le \;\; & I(c:d\,|\,a) + I(c:d\,|\,b) + I(a:b) \\ & + I(c:d\,|\,e) + I(e:c\,|\,d) + I(e:d\,|\,c) \end{aligned}$$

[non Shannon-type unconditional inequalitiy]

Conditional information inequalities

(c) **Non trivial, non Shannon-type**:

- **Zhang,Yeung 97:** if $I(a : b) = I(a : b \mid c) = 0$ then
$$I(c : d) \leq I(c : d \mid a) + I(c : d \mid b) + I(a : b)$$

Conditional information inequalities

(c) **Non trivial, non Shannon-type**:

- **Zhang,Yeung 97:** if $I(a:b) = I(a:b\,|\,c) = 0$ then
$$I(c:d) \leq I(c:d\,|\,a) + I(c:d\,|\,b) + I(a:b)$$
- **F. Matúš 99:** if $I(a:b\,|\,c) = I(b:d\,|\,c) = 0$ then
$$I(c:d) \leq I(c:d\,|\,a) + I(c:d\,|\,b) + I(a:b)$$

Conditional information inequalities

(c) **Non trivial, non Shannon-type**:

- **Zhang,Yeung 97:** if $I(a:b) = I(a:b\,|\,c) = 0$ then
$$I(c:d) \le I(c:d\,|\,a) + I(c:d\,|\,b) + I(a:b)$$
- **F. Matúš 99:** if $I(a:b\,|\,c) = I(b:d\,|\,c) = 0$ then
$$I(c:d) \le I(c:d\,|\,a) + I(c:d\,|\,b) + I(a:b)$$
- **our result:** if $H(c\,|\,a,b) = I(a:b\,|\,c) = 0$ then
$$I(c:d) \le I(c:d\,|\,a) + I(c:d\,|\,b) + I(a:b)$$

$$\underbrace{I(a:b) = I(a:b|c) = 0}_{\text{[Zhang–Yeung 97]}} \qquad \underbrace{I(a:b|c) = I(b:d|c) = 0}_{\text{[Matúš 99]}} \qquad \underbrace{H(c|a,b) = I(a:b|c) = 0}_{\text{[this paper]}}$$

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

$$\underbrace{I(a:b) = I(a:b|c) = 0}_{\text{[Zhang–Yeung 97]}} \qquad \underbrace{I(a:b|c) = I(b:d|c) = 0}_{\text{[Matúš 99]}} \qquad \underbrace{H(c|a,b) = I(a:b|c) = 0}_{\text{[this paper]}}$$

$$\searrow \qquad\qquad \downarrow \qquad\qquad \swarrow$$

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

Main Theorem. These three statements are *essentially* conditional inequalities.

Main Theorem [the first case of three]

The inequality

$$I(a:b) = I(a:b|c) = 0 \Rightarrow I(c:d) \leq I(c:d|a) + I(c:d|b)$$

is *essentially* conditional.

Main Theorem [the first case of three]

The inequality

$$I(a:b) = I(a:b|c) = 0 \Rightarrow I(c:d) \leq I(c:d|a) + I(c:d|b)$$

is *essentially* conditional.

More precisely, for all C_1, C_2 the inequality

$$I(c:d) \leq I(c:d \mid a) + I(c:d \mid b) + C_1 I(a:b) + C_2 I(a:b \mid c)$$

does not hold!

Main Theorem [the first case of three]

The inequality

$$I(a:b) = I(a:b|c) = 0 \Rightarrow I(c:d) \leq I(c:d|a) + I(c:d|b)$$

is *essentially* conditional.

More precisely, for all C_1, C_2 there exist (a, b, c, d) such that

$$I(c:d) \not\leq I(c:d \mid a) + I(c:d \mid b) + C_1 I(a:b) + C_2 I(a:b \mid c)$$

Claim: For any C_1, C_2 there exist (a, b, c, d) such that

$$I(c:d) \not\leq I(c:d \mid a) + I(c:d \mid b) + C_1 I(a:b) + C_2 I(a:b \mid c)$$

Claim: For any C_1, C_2 there exist (a, b, c, d) such that

$$I(c:d) \not\leq I(c:d\,|\,a)+I(c:d\,|\,b)+C_1 I(a:b)+C_2 I(a:b\,|\,c)$$

Proof:

a	b	c	d	$\mathrm{Prob}[a, b, c, d]$
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

Claim: For any C_1, C_2 there exist (a, b, c, d) such that

$$I(c:d) \not\leq I(c:d\,|\,a) + I(c:d\,|\,b) + C_1 I(a:b) + C_2 I(a:b\,|\,c)$$

Proof:

a	b	c	d	$\mathrm{Prob}[a,b,c,d]$
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

$$\begin{array}{ccccccccc} I(c:d) & \not\leq & I(c:d\,|\,a) & + & I(c:d\,|\,b) & + & C_1 I(a:b) & + & C_2 I(a:b\,|\,c) \\ \| & & \| & & \| & & \| & & \| \\ \Theta(\varepsilon) & & 0 & + & 0 & + & O(\varepsilon^2) & + & 0 \end{array}$$

Remark on algorithmic entropy:

- Exactly the same classes of unconditional linear inequalities hold for Shannon's entropy and for Kolmogorov complexity.

Remark on algorithmic entropy:

- Exactly the same classes of unconditional linear inequalities hold for Shannon's entropy and for Kolmogorov complexity.
- Essentially conditional inequality [ZY97] is true for Shannon's entropy **but not** for Kolmogorov complexity (in some natural sense).

See Proceedings for details.

Question 1: Can we apply essentially conditional inequalities (converse coding theorems, secret sharing problems, etc.)?

Question 1: Can we apply essentially conditional inequalities (converse coding theorems, secret sharing problems, etc.)?

Question 2: *May* we apply essentially conditional inequalities in 'real world' problems? These inequalities are not robust; do they make any 'physical' sense?

Acknowledgments: We indebted to the anonymous referees for helpful comments; following their suggestions we changed the title, reworked the introduction, modified statements of theorems, the bibliography, ..., and even corrected several *really essential* things in our paper.

Thank you! Any questions?