Different Views of Information
Part I — supplementary materials

***

Geometry in Cryptography and Communication

Andrei Romashchenko

UiT The Arctic University of Norway, October 2025

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

Claim: $0 \leq \mathrm{H}(X) \leq \log k$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

Claim: $0 \leq \mathrm{H}(X) \leq \log k$

Proof:

$\sum p_i \log \frac{1}{p_i} \overset{?}{\leq} \log k$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

Claim: $0 \leq \mathrm{H}(X) \leq \log k$

Proof:

$\sum p_i \log \frac{1}{p_i} \overset{?}{\leq} \log k = \sum p_i \log k$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

Claim: $0 \leq \mathrm{H}(X) \leq \log k$

Proof:

$\sum p_i \log \frac{1}{p_i} \overset{?}{\leq} \log k = \sum p_i \log k$

$\sum p_i \log \frac{1}{kp_i} \overset{?}{\leq} 0$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

Claim: $0 \leq \mathrm{H}(X) \leq \log k$

Proof:

$\sum p_i \log \frac{1}{p_i} \overset{?}{\leq} \log k = \sum p_i \log k$

$\sum p_i \log \frac{1}{kp_i} \overset{?}{\leq} 0$

Jensen's inequality: if $\sum p_i = 1$ then $\sum p_i \log x_i \leq \log \left(\sum p_i x_i\right)$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

Claim: $0 \leq \mathrm{H}(X) \leq \log k$

Proof:

$\sum p_i \log \frac{1}{p_i} \overset{?}{\leq} \log k = \sum p_i \log k$

$\sum p_i \log \frac{1}{kp_i} \overset{?}{\leq} 0$

Jensen's inequality: if $\sum p_i = 1$ then $\sum p_i \log x_i \leq \log \left(\sum p_i x_i\right)$

Conclusion: $\sum_{i=1}^{k} p_i \log \frac{1}{kp_i} \leq \log \sum_{i=1}^{k} \left(p_i \frac{1}{kp_i}\right)$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

Claim: $0 \le \mathrm{H}(X) \le \log k$

Proof:

$\sum p_i \log \frac{1}{p_i} \overset{?}{\le} \log k = \sum p_i \log k$

$\sum p_i \log \frac{1}{kp_i} \overset{?}{\le} 0$

Jensen's inequality: if $\sum p_i = 1$ then $\sum p_i \log x_i \le \log \left(\sum p_i x_i \right)$

Conclusion: $\sum_{i=1}^{k} p_i \log \frac{1}{kp_i} \le \log \sum_{i=1}^{k} \left(p_i \frac{1}{kp_i} \right) = \log \sum_{i=1}^{k} \left(\frac{1}{k} \right)$

definitions (1)

entropy of random variable X with a distribution $(p_1, \dots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

Claim: $0 \leq \mathrm{H}(X) \leq \log k$

Proof:

$\sum p_i \log \frac{1}{p_i} \overset{?}{\leq} \log k = \sum p_i \log k$

$\sum p_i \log \frac{1}{kp_i} \overset{?}{\leq} 0$

Jensen's inequality: if $\sum p_i = 1$ then $\sum p_i \log x_i \leq \log \left(\sum p_i x_i\right)$

Conclusion: $\sum_{i=1}^{k} p_i \log \frac{1}{kp_i} \leq \log \sum_{i=1}^{k} \left(p_i \frac{1}{kp_i}\right) = \log \sum_{i=1}^{k} \left(\frac{1}{k}\right) = \log 1$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$ such that $\sum p_i = 1$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

Claim: $0 \leq \mathrm{H}(X) \leq \log k$

Proof:

$\sum p_i \log \frac{1}{p_i} \overset{?}{\leq} \log k = \sum p_i \log k$

$\sum p_i \log \frac{1}{kp_i} \overset{?}{\leq} 0$

Jensen's inequality: if $\sum p_i = 1$ then $\sum p_i \log x_i \leq \log \left(\sum p_i x_i\right)$

Conclusion: $\sum_{i=1}^{k} p_i \log \frac{1}{kp_i} \leq \log \sum_{i=1}^{k} \left(p_i \frac{1}{kp_i}\right) = \log \sum_{i=1}^{k} \left(\frac{1}{k}\right) = \log 1 = 0$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

We know: $0 \leq \mathrm{H}(X) \leq \log k$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

We know: $0 \leq \mathrm{H}(X) \leq \log k$

Claim: $\mathrm{H}(X)$ can be any real number between 0 and $\log k$

definitions (1)

entropy of random variable X with a distribution $(p_1, \ldots, p_k)$

$$\mathrm{H}(X) := \sum p_i \log \frac{1}{p_i}$$

We know: $0 \leq \mathrm{H}(X) \leq \log k$

Claim: $\mathrm{H}(X)$ can be any real number between 0 and $\log k$

i.e., **entropy of a random variable can be any non-negative real number**

definitions (2)

entropic profile (entropic vector) of a **pair** of random variables (X, Y) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(X, Y) \rangle$$

definitions (2)

entropic profile (entropic vector) of a **pair** of random variables (X, Y) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(X, Y) \rangle$$

Constraints: $0 \leq \mathrm{H}(X), \mathrm{H}(Y) \leq \mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

basic inequalities

Proposition. $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

basic inequalities

Proposition. $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

Proof:
$p_{ij} := \mathrm{prob}[X = a_i \text{ and } Y = b_j]$, $p_{i*} := \mathrm{prob}[X = a_i]$, $p_{*j} := \mathrm{prob}[Y = b_j]$

$$\sum_{ij} p_{ij} \log \frac{1}{p_{ij}} \overset{?}{\leq} \sum_i p_{i*} \log \frac{1}{p_{i*}} + \sum_j p_{*j} \log \frac{1}{p_{*j}}$$

basic inequalities

Proposition. $\mathrm{H}(X,Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

Proof:

$p_{ij} := \mathrm{prob}[X = a_i \text{ and } Y = b_j]$, $p_{i*} := \mathrm{prob}[X = a_i]$, $p_{*j} := \mathrm{prob}[Y = b_j]$

$$\sum_{ij} p_{ij} \log \frac{1}{p_{ij}} \overset{?}{\leq} \sum_{i} p_{i*} \log \frac{1}{p_{i*}} + \sum_{j} p_{*j} \log \frac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \frac{1}{p_{ij}} \overset{?}{\leq} \sum_{ij} p_{ij} \log \frac{1}{p_{i*}} + \sum_{ij} p_{ij} \log \frac{1}{p_{*j}}$$

basic inequalities

Proposition. $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

Proof:

$p_{ij} := \mathrm{prob}[X = a_i \text{ and } Y = b_j]$, $p_{i*} := \mathrm{prob}[X = a_i]$, $p_{*j} := \mathrm{prob}[Y = b_j]$

$$\sum_{ij} p_{ij} \log \frac{1}{p_{ij}} \stackrel{?}{\leq} \sum_{i} p_{i*} \log \frac{1}{p_{i*}} + \sum_{j} p_{*j} \log \frac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \frac{1}{p_{ij}} \stackrel{?}{\leq} \sum_{ij} p_{ij} \log \frac{1}{p_{i*}} + \sum_{ij} p_{ij} \log \frac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \frac{p_{i*} \cdot p_{*j}}{p_{ij}} \stackrel{?}{\leq} 0$$

basic inequalities

Proposition. $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

Proof:

$p_{ij} := \mathrm{prob}[X = a_i \text{ and } Y = b_j]$, $p_{i*} := \mathrm{prob}[X = a_i]$, $p_{*j} := \mathrm{prob}[Y = b_j]$

$$\sum_{ij} p_{ij} \log \tfrac{1}{p_{ij}} \stackrel{?}{\leq} \sum_{i} p_{i*} \log \tfrac{1}{p_{i*}} + \sum_{j} p_{*j} \log \tfrac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \tfrac{1}{p_{ij}} \stackrel{?}{\leq} \sum_{ij} p_{ij} \log \tfrac{1}{p_{i*}} + \sum_{ij} p_{ij} \log \tfrac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \tfrac{p_{i*} \cdot p_{*j}}{p_{ij}} \stackrel{?}{\leq} 0$$

$$\sum_{ij} p_{ij} \log \tfrac{p_{i*} \cdot p_{*j}}{p_{ij}} \stackrel{\mathit{Jensen}}{\leq} \log \left(\sum_{ij} p_{ij} \cdot \tfrac{p_{i*} \cdot p_{*j}}{p_{ij}} \right)$$

basic inequalities

Proposition. $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

Proof:

$p_{ij} := \mathrm{prob}[X = a_i \text{ and } Y = b_j]$, $p_{i*} := \mathrm{prob}[X = a_i]$, $p_{*j} := \mathrm{prob}[Y = b_j]$

$$\sum_{ij} p_{ij} \log \tfrac{1}{p_{ij}} \stackrel{?}{\leq} \sum_{i} p_{i*} \log \tfrac{1}{p_{i*}} + \sum_{j} p_{*j} \log \tfrac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \tfrac{1}{p_{ij}} \stackrel{?}{\leq} \sum_{ij} p_{ij} \log \tfrac{1}{p_{i*}} + \sum_{ij} p_{ij} \log \tfrac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \tfrac{p_{i*} \cdot p_{*j}}{p_{ij}} \stackrel{?}{\leq} 0$$

$$\sum_{ij} p_{ij} \log \tfrac{p_{i*} \cdot p_{*j}}{p_{ij}} \stackrel{\textit{Jensen}}{\leq} \log \left(\sum_{ij} p_{ij} \cdot \tfrac{p_{i*} \cdot p_{*j}}{p_{ij}} \right) = \log \left(\sum_{ij} p_{i*} \cdot p_{*j} \right)$$

basic inequalities

Proposition. $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

Proof:

$p_{ij} := \mathrm{prob}[X = a_i \text{ and } Y = b_j]$, $p_{i*} := \mathrm{prob}[X = a_i]$, $p_{*j} := \mathrm{prob}[Y = b_j]$

$$\sum_{ij} p_{ij} \log \frac{1}{p_{ij}} \stackrel{?}{\leq} \sum_i p_{i*} \log \frac{1}{p_{i*}} + \sum_j p_{*j} \log \frac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \frac{1}{p_{ij}} \stackrel{?}{\leq} \sum_{ij} p_{ij} \log \frac{1}{p_{i*}} + \sum_{ij} p_{ij} \log \frac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \frac{p_{i*} \cdot p_{*j}}{p_{ij}} \stackrel{?}{\leq} 0$$

$$\sum_{ij} p_{ij} \log \frac{p_{i*} \cdot p_{*j}}{p_{ij}} \stackrel{\text{Jensen}}{\leq} \log \left(\sum_{ij} p_{ij} \cdot \frac{p_{i*} \cdot p_{*j}}{p_{ij}} \right) = \log \left(\sum_{ij} p_{i*} \cdot p_{*j} \right)$$

$$= \log \left(\sum_i p_{i*} \cdot \sum_j p_{*j} \right)$$

basic inequalities

Proposition. $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

Proof:

$p_{ij} := \mathrm{prob}[X = a_i \text{ and } Y = b_j]$, $p_{i*} := \mathrm{prob}[X = a_i]$, $p_{*j} := \mathrm{prob}[Y = b_j]$

$$\sum_{ij} p_{ij} \log \tfrac{1}{p_{ij}} \overset{?}{\leq} \sum_{i} p_{i*} \log \tfrac{1}{p_{i*}} + \sum_{j} p_{*j} \log \tfrac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \tfrac{1}{p_{ij}} \overset{?}{\leq} \sum_{ij} p_{ij} \log \tfrac{1}{p_{i*}} + \sum_{ij} p_{ij} \log \tfrac{1}{p_{*j}}$$

$$\sum_{ij} p_{ij} \log \tfrac{p_{i*} \cdot p_{*j}}{p_{ij}} \overset{?}{\leq} 0$$

$$\sum_{ij} p_{ij} \log \tfrac{p_{i*} \cdot p_{*j}}{p_{ij}} \overset{Jensen}{\leq} \log \left(\sum_{ij} p_{ij} \cdot \tfrac{p_{i*} \cdot p_{*j}}{p_{ij}} \right) = \log \left(\sum_{ij} p_{i*} \cdot p_{*j} \right)$$

$$= \log \left(\sum_{i} p_{i*} \cdot \sum_{j} p_{*j} \right) = \log 1 = 0$$

definitions (2)

entropic profile (entropic vector) of a **pair** of random variables (X, Y) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(X, Y) \rangle$$

definitions (2)

entropic profile (entropic vector) of a **pair** of random variables (X, Y) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(X, Y) \rangle$$

$$0 \leq \mathrm{H}(X), \mathrm{H}(Y) \leq \mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$$

definitions (2)

entropic profile (entropic vector) of a **pair** of random variables (X, Y) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(X, Y) \rangle$$

$$0 \le \mathrm{H}(X), \mathrm{H}(Y) \le \mathrm{H}(X, Y) \le \mathrm{H}(X) + \mathrm{H}(Y)$$

each entropic vector (h_X, h_Y, h_{XY}) satisfies these inequalities

definitions (2)

entropic profile (entropic vector) of a **pair** of random variables (X, Y) is

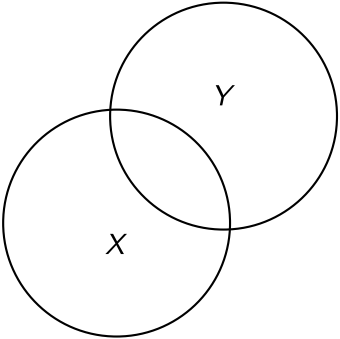
$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(X, Y) \rangle$$

$$0 \le \mathrm{H}(X), \mathrm{H}(Y) \le \mathrm{H}(X, Y) \le \mathrm{H}(X) + \mathrm{H}(Y)$$

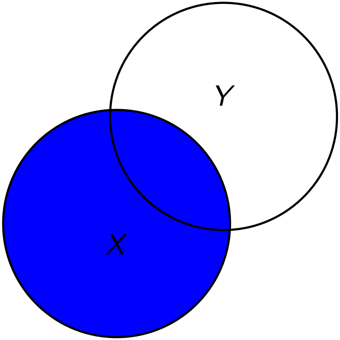
each entropic vector (h_X, h_Y, h_{XY}) satisfies these inequalities

three coordinates, $2 + 2 + 1$ inequalities

Inequalities in a diagram

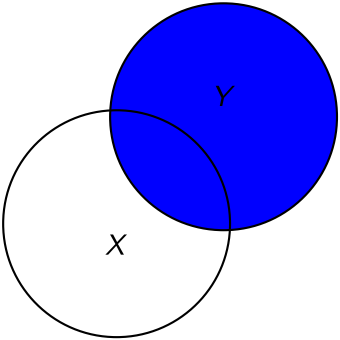


Inequalities in a diagram



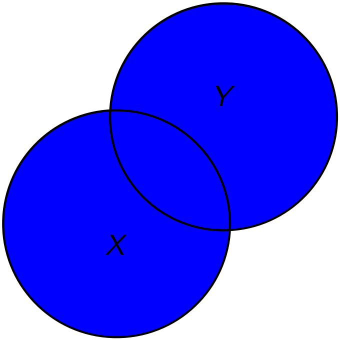
$\mathrm{H}(X)$

Inequalities in a diagram



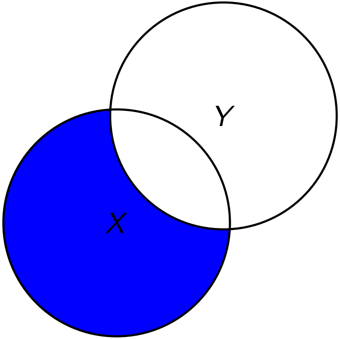
$\mathrm{H}(Y)$

Inequalities in a diagram



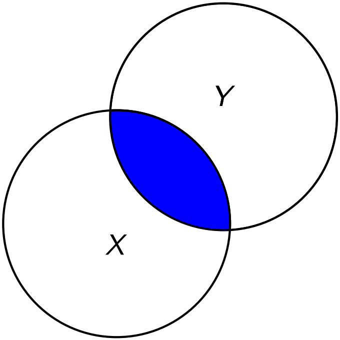
$\mathrm{H}(X, Y)$

Inequalities in a diagram



$\mathrm{H}(X \mid Y) = \mathrm{H}(X, Y) - \mathrm{H}(Y)$

Inequalities in a diagram



$\mathrm{I}(X : Y) = \mathrm{H}(X) + \mathrm{H}(Y) - \mathrm{H}(X, Y)$

The definitions (2) again

entropic profile (entropic vector) of a **pair** of random variables (X, Y) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(X, Y) \rangle$$

$$0 \leq \mathrm{H}(X), \mathrm{H}(Y) \leq \mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$$

each entropic vector (h_A, h_B, h_{AB}) satisfies these inequalities

three coordinates, $2 + 2 + 1$ inequalities

~~**Theorem**~~ **Simple observation:** no other inequalities for entropy vector of **pairs**

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z)\rangle$$

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z)\rangle$$

Inequalities:

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X,Y), \mathrm{H}(X,Z), \mathrm{H}(Y,Z), \mathrm{H}(X,Y,Z) \rangle$$

Inequalities:

- monotonicity, e.g., $\mathrm{H}(X,Y) \leq \mathrm{H}(X,Y,Z)$

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z)\rangle$$

Inequalities:

- monotonicity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X, Y, Z)$
  (a.k.a. $\mathrm{H}(Z \mid X, Y) \geq 0$)

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z)\rangle$$

Inequalities:

- monotonicity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X, Y, Z)$
  (a.k.a. $\mathrm{H}(Z \mid X, Y) \geq 0$)
- subadditivity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z) \rangle$$

Inequalities:

- monotonicity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X, Y, Z)$
  (a.k.a. $\mathrm{H}(Z \mid X, Y) \geq 0$)
- subadditivity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$
  (a.k.a. $\mathrm{I}(X : Y) \geq 0$)

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z)\rangle$$

Inequalities:

- monotonicity, e.g., $\mathrm{H}(X, Y) \le \mathrm{H}(X, Y, Z)$
  (a.k.a. $\mathrm{H}(Z \mid X, Y) \ge 0$)
- subadditivity, e.g., $\mathrm{H}(X, Y) \le \mathrm{H}(X) + \mathrm{H}(Y)$
  (a.k.a. $\mathrm{I}(X : Y) \ge 0$)
- submodularity, $\mathrm{H}(X, Y, Z) + \mathrm{H}(X) \le \mathrm{H}(X, Y) + \mathrm{H}(X, Z)$

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X,Y), \mathrm{H}(X,Z), \mathrm{H}(Y,Z), \mathrm{H}(X,Y,Z) \rangle$$

Inequalities:

- monotonicity, e.g., $\mathrm{H}(X,Y) \le \mathrm{H}(X,Y,Z)$
  (a.k.a. $\mathrm{H}(Z \,|\, X,Y) \ge 0$)
- subadditivity, e.g., $\mathrm{H}(X,Y) \le \mathrm{H}(X) + \mathrm{H}(Y)$
  (a.k.a. $\mathrm{I}(X : Y) \ge 0$)
- submodularity, $\mathrm{H}(X,Y,Z) + \mathrm{H}(X) \le \mathrm{H}(X,Y) + \mathrm{H}(X,Z)$
  (a.k.a. $\mathrm{I}(Y : Z \,|\, X) \ge 0$)

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z)\rangle$$

Inequalities:

- monotonicity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X, Y, Z)$
  (a.k.a. $\mathrm{H}(Z \,|\, X, Y) \geq 0$)
- subadditivity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$
  (a.k.a. $\mathrm{I}(X : Y) \geq 0$)
- submodularity, $\mathrm{H}(X, Y, Z) + \mathrm{H}(X) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z)$
  (a.k.a. $\mathrm{I}(Y : Z \,|\, X) \geq 0$)

each entropic vector (7-tuple of real numbers) satisfies these inequalities

The definitions (3)

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z) \rangle$$

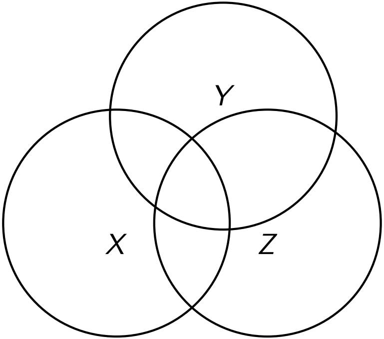
Inequalities:

- monotonicity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X, Y, Z)$
  (a.k.a. $\mathrm{H}(Z \,|\, X, Y) \geq 0$)
- subadditivity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$
  (a.k.a. $\mathrm{I}(X : Y) \geq 0$)
- submodularity, $\mathrm{H}(X, Y, Z) + \mathrm{H}(X) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z)$
  (a.k.a. $\mathrm{I}(Y : Z \,|\, X) \geq 0$)

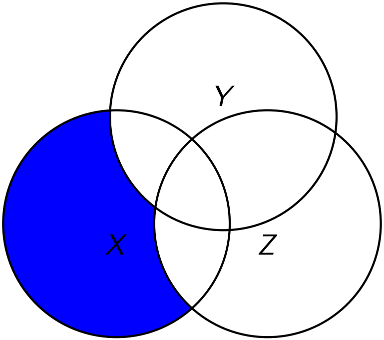
each entropic vector (7-tuple of real numbers) satisfies these inequalities

seven coordinates and *at least* $3 + 3 + 3$ inequalities

Entropy inequalities in diagrams

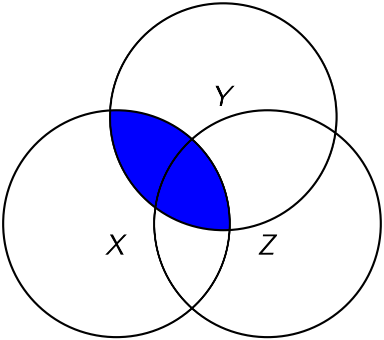


Entropy inequalities in diagrams



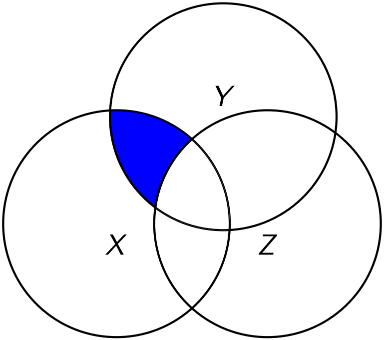
$\mathrm{H}(X \mid Y, Z) = \mathrm{H}(X, Y, Z) - \mathrm{H}(Y, Z)$

Entropy inequalities in diagrams



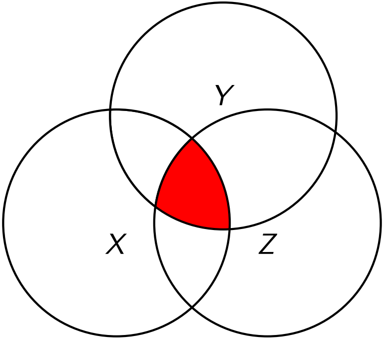
$\mathrm{I}(X : Y) = \mathrm{H}(X) + \mathrm{H}(Y) - \mathrm{H}(X, Y)$

Entropy inequalities in diagrams



$\mathrm{I}(X : Y \mid Z) = \mathrm{H}(X, Z) + \mathrm{H}(Y, Z) - \mathrm{H}(X, Y, Z) - \mathrm{H}(Z)$

Entropy inequalities in diagrams



$\mathrm{I}(X : Y : Z) =$
$\mathrm{H}(X) + \mathrm{H}(Y) + \mathrm{H}(Z) - \mathrm{H}(X, Y) - \mathrm{H}(X, Z) - \mathrm{H}(Y, Z) + \mathrm{H}(X, Y, Z)$

(may be negative!)

The definitions (3) again

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle\ \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z)\ \rangle$$

or equivalently

$$\begin{array}{lll} \langle\ \mathrm{H}(X \,|\, Y, Z), & \mathrm{H}(Y \,|\, X, Z), \quad \mathrm{H}(Z \,|\, X, Y), & \\ & \mathrm{I}(X : Y \,|\, Z), \quad \mathrm{I}(X : Z \,|\, Y), \quad \mathrm{I}(Y : Z \,|\, X), & \mathrm{I}(X : Y : Z)\ \rangle \end{array}$$

Inequalities:

The definitions (3) again

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \, \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z) \, \rangle$$

or equivalently

$$\begin{aligned} \langle \, \mathrm{H}(X \mid Y, Z),\ & \mathrm{H}(Y \mid X, Z), \quad \mathrm{H}(Z \mid X, Y), \\ & \mathrm{I}(X : Y \mid Z), \quad \mathrm{I}(X : Z \mid Y), \quad \mathrm{I}(Y : Z \mid X),\ \mathrm{I}(X : Y : Z) \, \rangle \end{aligned}$$

Inequalities:

- monotonicity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X, Y, Z)$ (a.k.a. $\mathrm{H}(Z \mid X, Y) \geq 0$)
- subadditivity, e.g., $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$ (a.k.a. $\mathrm{I}(X : Y) \geq 0$)
- submodularity, $\mathrm{H}(X, Y, Z) + \mathrm{H}(X) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z)$ (a.k.a. $\mathrm{I}(Y : Z \mid X) \geq 0$)

each entropic vector (7-tuple of real numbers) satisfies these inequalities

The definitions (3) one more time

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle\ \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X,Y), \mathrm{H}(X,Z), \mathrm{H}(Y,Z), \mathrm{H}(X,Y,Z)\ \rangle$$

or equivalently

$$\begin{aligned}\langle\ \mathrm{H}(X \mid Y,Z),\ & \mathrm{H}(Y \mid X,Z), \quad \mathrm{H}(Z \mid X,Y),\\ & \mathrm{I}(X:Y \mid Z), \quad \mathrm{I}(X:Z \mid Y), \quad \mathrm{I}(Y:Z \mid X),\ \mathrm{I}(X:Y:Z)\ \rangle\end{aligned}$$

Observation 1: (vector of entropies) $\leftrightarrow$ (vector of atomic I-measures)
is a non-degenerate linear transformation

The definitions (3) one more time

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle\ \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X,Y), \mathrm{H}(X,Z), \mathrm{H}(Y,Z), \mathrm{H}(X,Y,Z)\ \rangle$$

or equivalently

$$\begin{aligned}\langle\ \mathrm{H}(X\,|\,Y,Z),\ & \mathrm{H}(Y\,|\,X,Z), \quad \mathrm{H}(Z\,|\,X,Y), \\ & \mathrm{I}(X:Y\,|\,Z), \quad \mathrm{I}(X:Z\,|\,Y), \quad \mathrm{I}(Y:Z\,|\,X),\ \mathrm{I}(X:Y:Z)\ \rangle\end{aligned}$$

Observation 1: (vector of entropies) $\leftrightarrow$ (vector of atomic I-measures)
is a non-degenerate linear transformation

Observation 2: every 7-vector with non-negative atomic I-measures is entropic.

The definitions (3) one more time

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle \ \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X, Y), \mathrm{H}(X, Z), \mathrm{H}(Y, Z), \mathrm{H}(X, Y, Z) \ \rangle$$

or equivalently

$$\begin{array}{llll} \langle \ \mathrm{H}(X \mid Y, Z), & \mathrm{H}(Y \mid X, Z), & \mathrm{H}(Z \mid X, Y), & \\ & \mathrm{I}(X : Y \mid Z), & \mathrm{I}(X : Z \mid Y), & \mathrm{I}(Y : Z \mid X), \ \mathrm{I}(X : Y : Z) \ \rangle \end{array}$$

Observation 1: (vector of entropies) $\leftrightarrow$ (vector of atomic I-measures) is a non-degenerate linear transformation

Observation 2: every 7-vector with non-negative atomic I-measures is entropic. This is a full dimension cone of entropic vectors!

The definitions (3) one more time

entropic profile (entropic vector) of a **triple** of random variables (X, Y, Z) is

$$\langle\ \mathrm{H}(X), \mathrm{H}(Y), \mathrm{H}(Y), \mathrm{H}(X,Y), \mathrm{H}(X,Z), \mathrm{H}(Y,Z), \mathrm{H}(X,Y,Z)\ \rangle$$

or equivalently

$$\begin{array}{l} \langle\ \mathrm{H}(X \mid Y, Z),\ \mathrm{H}(Y \mid X, Z),\quad \mathrm{H}(Z \mid X, Y), \\ \qquad\qquad\qquad \mathrm{I}(X : Y \mid Z),\quad \mathrm{I}(X : Z \mid Y),\quad \mathrm{I}(Y : Z \mid X),\ \mathrm{I}(X : Y : Z)\ \rangle \end{array}$$

Observation 1: (vector of entropies) $\leftrightarrow$ (vector of atomic I-measures) is a non-degenerate linear transformation

Observation 2: every 7-vector with non-negative atomic I-measures is entropic. This is a full dimension cone of entropic vectors!

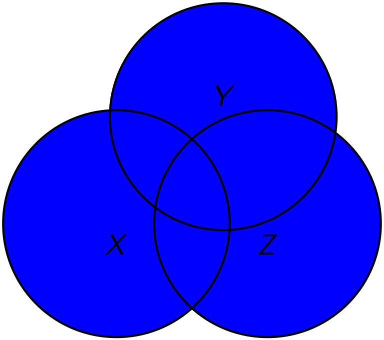
But there are also entropic vectors with a negative value of $\mathrm{I}(X : Y : Z)$.

Fun with diagrams (1)

How to prove $2\mathrm{H}(X, Y, Z) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?

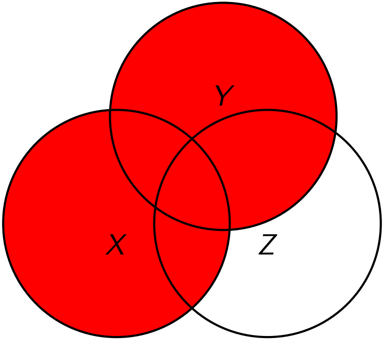
Fun with diagrams (1)

How to prove $2\mathrm{H}(X, Y, Z) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?



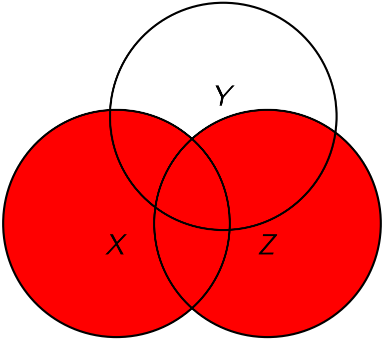
Fun with diagrams (1)

How to prove $2\mathrm{H}(X, Y, Z) \le \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?



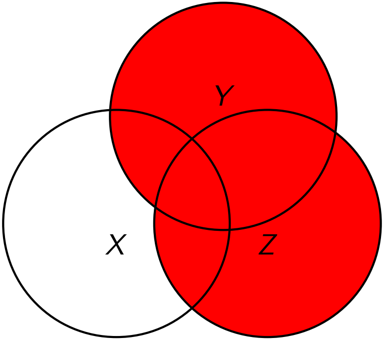
Fun with diagrams (1)

How to prove $2\mathrm{H}(X, Y, Z) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?



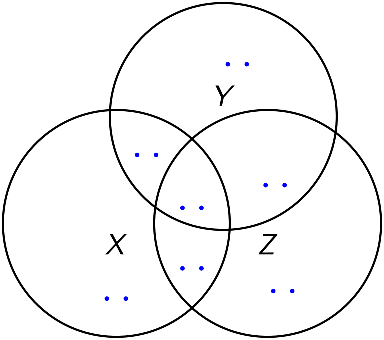
Fun with diagrams (1)

How to prove $2\mathrm{H}(X, Y, Z) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?



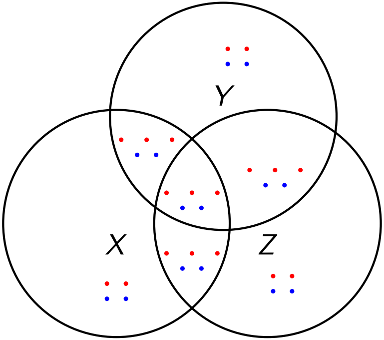
Fun with diagrams (1)

How to prove $\color{blue}{2\mathrm{H}(X, Y, Z)} \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?



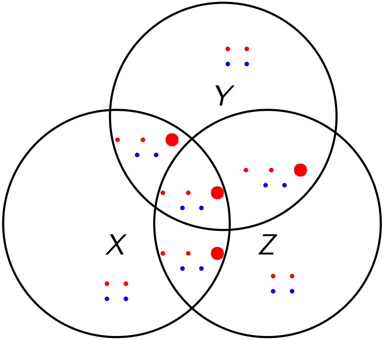
Fun with diagrams (1)

How to prove $2\mathrm{H}(X, Y, Z) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?



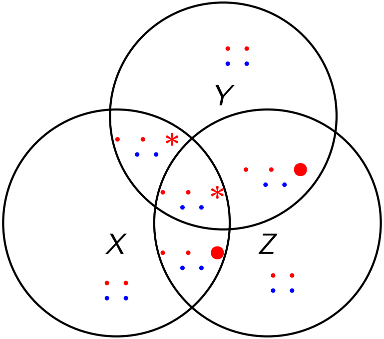
Fun with diagrams (1)

How to prove $2\mathrm{H}(X, Y, Z) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?



Fun with diagrams (1)

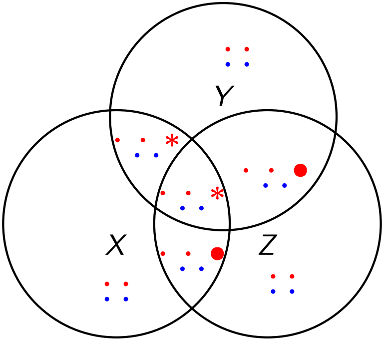
How to prove $2\mathrm{H}(X, Y, Z) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?



$[\text{RHS}] - [\text{LHS}] = \mathrm{I}(X : Y) + \mathrm{I}(X : Z \mid Y) + \mathrm{I}(Y : Z \mid X)$

Fun with diagrams (1)

How to prove $2\mathrm{H}(X, Y, Z) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$?



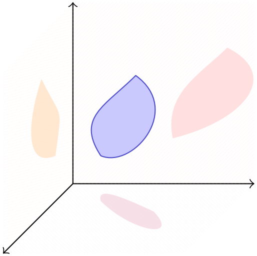
$[\text{RHS}] - [\text{LHS}] = \mathrm{I}(X : Y) + \mathrm{I}(X : Z \mid Y) + \mathrm{I}(Y : Z \mid X) \geq 0$

Fun with diagrams (1)

$2\mathrm{H}(X, Y, Z) \leq \mathrm{H}(X, Y) + \mathrm{H}(X, Z) + \mathrm{H}(Y, Z)$
implies that for every body in $\mathbb{R}^3$

$$\mathsf{Vol}^2 \leq \mathsf{area}(\mathsf{Proj}_{12}) \cdot \mathsf{area}(\mathsf{Proj}_{13}) \cdot \mathsf{area}(\mathsf{Proj}_{23})$$

(the Loomis–Whitney inequality)



Fun with diagrams (2)

If

- $\mathrm{H}(\text{ciphertext} \mid \text{message}, \text{key}) = 0$
- $\mathrm{H}(\text{message} \mid \text{ciphertext}, \text{key}) = 0$
- $\mathrm{I}(\text{message} : \text{ciphertext}) = 0$,

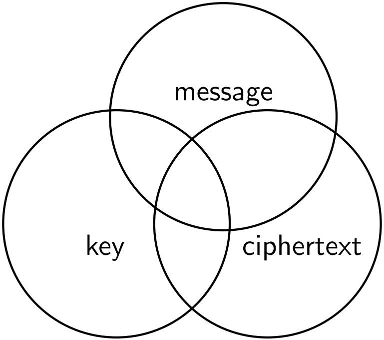
then $\mathrm{H}(\text{key}) \geq \mathrm{H}(\text{message})$

Fun with diagrams (2)

If

- $\mathrm{H}(\text{ciphertext} \mid \text{message}, \text{key}) = 0$
- $\mathrm{H}(\text{message} \mid \text{ciphertext}, \text{key}) = 0$
- $\mathrm{I}(\text{message} : \text{ciphertext}) = 0$,

then $\mathrm{H}(\text{key}) \geq \mathrm{H}(\text{message})$

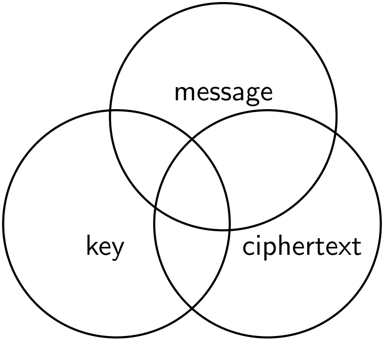


Fun with diagrams (2)

If

- $\mathrm{H}(\text{ciphertext} \mid \text{message}, \text{key}) = 0$
- $\mathrm{H}(\text{message} \mid \text{ciphertext}, \text{key}) = 0$
- $\mathrm{I}(\text{message} : \text{ciphertext}) = 0$,

then $\mathrm{H}(\text{key}) \geq \mathrm{H}(\text{message})$



Prove this claim using the diagram!