Different Views of Information
Part II

***

Geometry in Cryptography and Communication

Andrei Romashchenko

UiT The Arctic University of Norway, October 2025

random string

which of these strings is random?

- 0000000000000000000000000000000000000000000000000
- 0101010101010101010101010101010101010101010101010
- 0011111001001101100111011000001110101011011110011
- 1010110111111000010101000101100010100010101110110
- 1100100100001111111011010101000100010000101101000

random string

which of these strings is random?

- 0000000000000000000000000000000000000000000000000
- 0101010101010101010101010101010101010101010101010
- 0011111001001101100111011000001110101011011110011
- $e \approx 10.1011011111100001010100010110001010001010111011 01$
- $\pi \approx 11.0010010000111111011010101000100010000101101000 11$

Explain your guess!

measure of information: Kolmogorov's approach

Informal Definition: Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

measure of information: Kolmogorov's approach

Formal Definition: Kolmogorov complexity (with a *decompressor* U)

$C_U(\mathbf{x}) = \min\{|p| \ : \ U(p) = \mathbf{x}\}$

measure of information: Kolmogorov's approach

Formal Definition: Kolmogorov complexity (with a *decompressor* U)

$C_U(\mathbf{x}) = \min\{|p| \ : \ U(p) = \mathbf{x}\}$

Theorem

There exists a (computable) U such that for every other V and all strings $\mathbf{x}$,

$$C_U(\mathbf{x}) \leq C_V(\mathbf{x}) + O(1).$$

measure of information: Kolmogorov's approach

Formal Definition: Kolmogorov complexity (with a *decompressor* U)

$C_U(\mathbf{x}) = \min\{|p| \ : \ U(p) = \mathbf{x}\}$

Theorem

There exists a (computable) U such that for every other V there is a constant λ such that for all strings x

$$C_U(\mathbf{x}) \leq C_V(\mathbf{x}) + \lambda.$$

Proof.

Idea: Let U be a universal machine that can simulate any other machine V... □

measure of information: Kolmogorov's approach

Formal Definition: Kolmogorov complexity (with a *decompressor* U)

$C_U(\mathbf{x}) = \min\{|p| \ : \ U(p) = \mathbf{x}\}$

Theorem

There exists a (computable) U such that for every other V there is a constant λ such that for all strings x

$$C_U(\mathbf{x}) \leq C_V(\mathbf{x}) + \lambda.$$

Proof.

Idea: Let U be a universal machine that can simulate any other machine V... □

In what follows we fix U and let $\mathrm{C}(\mathbf{x}) := C_U(\mathbf{x})$

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties:

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties:

- $\mathrm{C}(\mathbf{x}) \leq |\mathbf{x}| + O(1)$,

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties:

- $\mathrm{C}(\mathbf{x}) \leq |\mathbf{x}| + O(1)$,
- $\mathrm{C}(\mathbf{xx}) \leq |\mathbf{x}| + O(1)$,

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties:

- $\mathrm{C}(\mathbf{x}) \leq |\mathbf{x}| + O(1)$,
- $\mathrm{C}(\mathbf{xx}) \leq |\mathbf{x}| + O(1)$,
- $\mathrm{C}(F(\mathbf{x})) \leq \mathrm{C}(\mathbf{x}) + O(1)$ for any computable F,

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties:

- $\mathrm{C}(\mathbf{x}) \leq |\mathbf{x}| + O(1)$,
- $\mathrm{C}(\mathbf{xx}) \leq |\mathbf{x}| + O(1)$,
- $\mathrm{C}(F(\mathbf{x})) \leq \mathrm{C}(\mathbf{x}) + O(1)$ for any computable F,
- for every n there exists a string of length n with complexity at least n,

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties:

- $\mathrm{C}(\mathbf{x}) \leq |\mathbf{x}| + O(1)$,
- $\mathrm{C}(\mathbf{xx}) \leq |\mathbf{x}| + O(1)$,
- $\mathrm{C}(F(\mathbf{x})) \leq \mathrm{C}(\mathbf{x}) + O(1)$ for any computable F,
- for every n there exists a string of length n with complexity at least n,
- there exists a $\lambda \geq$ s.t. for every n, at least 99% of strings of length n satisfy $n - \lambda \ \leq \ \mathrm{C}(\mathbf{x}) \ \leq \ n + \lambda$.

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties:

- $\mathrm{C}(\mathbf{x}) \leq |\mathbf{x}| + O(1)$,
- $\mathrm{C}(\mathbf{xx}) \leq |\mathbf{x}| + O(1)$,
- $\mathrm{C}(F(\mathbf{x})) \leq \mathrm{C}(\mathbf{x}) + O(1)$ for any computable F,
- for every n there exists a string of length n with complexity at least n,
- there exists a $\lambda \geq$ s.t. for every n, at least 99% of strings of length n satisfy $n - \lambda \ \leq \ \mathrm{C}(\mathbf{x}) \ \leq \ n + \lambda$.
- if there is an algorithm that for every input n produces a list of strings S_n, [binary expansion of n] $\mapsto$ `alg` $\mapsto$ [list of elements of S_n]
  then
  - for every $\mathbf{x} \in S_n$ we have $\mathrm{C}(\mathbf{x}) \leq \log \mathrm{Card}(S_n) + O(\log n)$
  - for most $\mathbf{x} \in S_n$ we have $\mathrm{C}(\mathbf{x}) \geq \log \mathrm{Card}(S_n) - O(1)$

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

another simple property:

- if a bit string $\mathbf{x}$ contains $p_0 n$ zeros and $p_1 n$ ones, then

  $\mathrm{C}(\mathbf{x}) \leq \log \frac{n!}{(p_0 n)! \cdot (p_1 n)!} + O(\log n)$

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

another simple property:

- if a bit string $\mathbf{x}$ contains $p_0 n$ zeros and $p_1 n$ ones, then
  $\mathrm{C}(\mathbf{x}) \leq \log \frac{n!}{(p_0 n)! \cdot (p_1 n)!} + O(\log n) = \left(p_0 \log \frac{1}{p_0} + p_1 \log \frac{1}{p_1} \right) n + O(\log n)$

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

terminology: $\mathbf{x}$ is λ-**incompressible** if $\mathrm{C}(\mathbf{x}) \geq |\mathbf{x}| - \lambda$

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

terminology: $\mathbf{x}$ is λ-**incompressible** if $\mathrm{C}(\mathbf{x}) \geq |\mathbf{x}| - \lambda$

informal wording: $\mathbf{x}$ is **random** if $\mathrm{C}(\mathbf{x}) \approx |\mathbf{x}|$

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

terminology: $\mathbf{x}$ is λ-**incompressible** if $\mathrm{C}(\mathbf{x}) \geq |\mathbf{x}| - \lambda$

informal wording: $\mathbf{x}$ is **random** if $\mathrm{C}(\mathbf{x}) \approx |\mathbf{x}|$

intuition: $\mathbf{x}$ is **random** if there is no regularities in it

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties of conditional Kolmogorov complexity:

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties of conditional Kolmogorov complexity:

- $\mathrm{C}(\mathbf{x} \mid \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + O(1)$,

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties of conditional Kolmogorov complexity:

- $\mathrm{C}(\mathbf{x} \mid \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + O(1)$,
- $\mathrm{C}(\mathbf{x} \mid \mathbf{x}) \leq O(1)$,

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

simple properties of conditional Kolmogorov complexity:

- $\mathrm{C}(\mathbf{x} \mid \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + O(1)$,
- $\mathrm{C}(\mathbf{x} \mid \mathbf{x}) \leq O(1)$,
- $\mathrm{C}(F(\mathbf{x}) \mid \mathbf{x}) \leq O(1)$ for any computable F.

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

strange properties:

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

strange properties:

- Kolmogorov complexity $\mathrm{C}(\mathbf{x})$ is not a computable function

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

strange properties:

- Kolmogorov complexity $\mathrm{C}(\mathbf{x})$ is not a computable function
- no algorithm which, given n, produces a string $\mathbf{x}_n$ such that $\mathrm{C}(\mathbf{x}_n) > n$

measure of information: Kolmogorov's approach

Definition Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

---

strange properties:

- Kolmogorov complexity $\mathrm{C}(\mathbf{x})$ is not a computable function
- no algorithm which, given n, produces a string $\mathbf{x}_n$ such that $\mathrm{C}(\mathbf{x}_n) > n$
- almost all statements of the form "$\mathrm{C}(\mathbf{x}) > |\mathbf{x}|/2$" are unprovable
  (a sort of Gödel's *incompleteness* theorem)

secure secret key: Kolmogorov's approach

what is a secure secret key of size n?

secure secret key: Kolmogorov's approach

what is a secure secret key of size n?

possible answer: **x** is secure if any *simple* device brute-forcing the keys would try this **x** at step $\sim 2^n$.

secure secret key: Kolmogorov's approach

what is a secure secret key of size n?

possible answer: **x** is secure if any *simple* device brute-forcing the keys would try this **x** at step $\sim 2^n$.

this is essentially equivalent to the condition $\mathrm{C}(\mathbf{x}) \approx n$

secure secret key: Kolmogorov's approach

what is a secure secret key of size n?

possible answer: **x** is secure if any *simple* device brute-forcing the keys would try this **x** at step $\sim 2^n$.

this is essentially equivalent to the condition $\mathrm{C}(\mathbf{x}) \approx n$ (i.e., **x** is random)

measure of information: Kolmogorov's approach

Definition of Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

Information theory:

measure of information: Kolmogorov's approach

Definition of Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

Information theory:

- $\mathrm{C}(\mathbf{x}, \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$

measure of information: Kolmogorov's approach

Definition of Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

Information theory:

- $\mathrm{C}(\mathbf{x}, \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x}, \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$

measure of information: Kolmogorov's approach

Definition of Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

Information theory:

- $\mathrm{C}(\mathbf{x}, \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x}, \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x}, \mathbf{y}) = \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) \pm O(\log(|\mathbf{x}| + |\mathbf{y}|))$ [Kolmogorov–Levin]

measure of information: Kolmogorov's approach

Definition of Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

Information theory:

- $\mathrm{C}(\mathbf{x}, \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x}, \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x}, \mathbf{y}) = \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) \pm O(\log(|\mathbf{x}| + |\mathbf{y}|))$ [Kolmogorov–Levin]

Definition: mutual information

$\mathrm{I}(\mathbf{x} : \mathbf{y}) := \mathrm{C}(\mathbf{y}) - \mathrm{C}(\mathbf{y} \mid \mathbf{x})$

measure of information: Kolmogorov's approach

Definition of Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

Information theory:

- $\mathrm{C}(\mathbf{x},\mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x},\mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x},\mathbf{y}) = \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) \pm O(\log(|\mathbf{x}| + |\mathbf{y}|))$ [Kolmogorov–Levin]

Definition: mutual information

$\mathrm{I}(\mathbf{x} : \mathbf{y}) := \mathrm{C}(\mathbf{y}) - \mathrm{C}(\mathbf{y} \mid \mathbf{x})$ and $\mathrm{I}(\mathbf{x} : \mathbf{y} \mid \mathbf{z}) := \mathrm{C}(\mathbf{y} \mid \mathbf{z}) - \mathrm{C}(\mathbf{y} \mid \mathbf{x}, \mathbf{z})$

measure of information: Kolmogorov's approach

Definition of Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

Information theory:

- $\mathrm{C}(\mathbf{x},\mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x},\mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x},\mathbf{y}) = \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) \pm O(\log(|\mathbf{x}| + |\mathbf{y}|))$ [Kolmogorov–Levin]

Definition: mutual information

$\mathrm{I}(\mathbf{x} : \mathbf{y}) := \mathrm{C}(\mathbf{y}) - \mathrm{C}(\mathbf{y} \mid \mathbf{x})$ and $\mathrm{I}(\mathbf{x} : \mathbf{y} \mid \mathbf{z}) := \mathrm{C}(\mathbf{y} \mid \mathbf{z}) - \mathrm{C}(\mathbf{y} \mid \mathbf{x}, \mathbf{z})$

Symmetry of the mutual information:

measure of information: Kolmogorov's approach

Definition of Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

Information theory:

- $\mathrm{C}(\mathbf{x},\mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x},\mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x},\mathbf{y}) = \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) \pm O(\log(|\mathbf{x}| + |\mathbf{y}|))$ [Kolmogorov–Levin]

Definition: mutual information

$\mathrm{I}(\mathbf{x} : \mathbf{y}) := \mathrm{C}(\mathbf{y}) - \mathrm{C}(\mathbf{y} \mid \mathbf{x})$ and $\mathrm{I}(\mathbf{x} : \mathbf{y} \mid \mathbf{z}) := \mathrm{C}(\mathbf{y} \mid \mathbf{z}) - \mathrm{C}(\mathbf{y} \mid \mathbf{x},\mathbf{z})$

Symmetry of the mutual information:

- $\mathrm{I}(\mathbf{x} : \mathbf{y}) = \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) - \mathrm{C}(\mathbf{x},\mathbf{y}) \pm O(\log(|\mathbf{x}| + |\mathbf{y}|))$

measure of information: Kolmogorov's approach

Definition of Kolmogorov complexity:

$\mathrm{C}(\mathbf{x}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x}\}$

$\mathrm{C}(\mathbf{x}|\mathbf{y}) = \min\{|p| \ : \ \text{program } p \text{ produced } \mathbf{x} \text{ given } \mathbf{y}\}$

Information theory:

- $\mathrm{C}(\mathbf{x},\mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x},\mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$
- $\mathrm{C}(\mathbf{x},\mathbf{y}) = \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y} \mid \mathbf{x}) \pm O(\log(|\mathbf{x}| + |\mathbf{y}|))$ [Kolmogorov–Levin]

Definition: mutual information

$\mathrm{I}(\mathbf{x} : \mathbf{y}) := \mathrm{C}(\mathbf{y}) - \mathrm{C}(\mathbf{y} \mid \mathbf{x})$ and $\mathrm{I}(\mathbf{x} : \mathbf{y} \mid \mathbf{z}) := \mathrm{C}(\mathbf{y} \mid \mathbf{z}) - \mathrm{C}(\mathbf{y} \mid \mathbf{x},\mathbf{z})$

Symmetry of the mutual information:

- $\begin{aligned}\mathrm{I}(\mathbf{x} : \mathbf{y}) &= \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) - \mathrm{C}(\mathbf{x},\mathbf{y}) \pm O(\log(|\mathbf{x}| + |\mathbf{y}|)) \\ &= \mathrm{I}(\mathbf{y} : \mathbf{x}) \pm O(\log(|\mathbf{x}| + |\mathbf{y}|))\end{aligned}$

Kolmogorov complexity: information inequalities

similar to Shannon's case:

Kolmogorov complexity: information inequalities

similar to Shannon's case:

- monotonicity:
  $\mathrm{C}(\mathbf{x}) \leq \mathrm{C}(\mathbf{x}, \mathbf{y}) + O(1)$, cf. $\mathrm{C}(\mathbf{y} \mid \mathbf{x}) \geq 0$

Kolmogorov complexity: information inequalities

similar to Shannon's case:

- monotonicity:
  $\mathrm{C}(\mathbf{x}) \leq \mathrm{C}(\mathbf{x}, \mathbf{y}) + O(1)$, cf. $\mathrm{C}(\mathbf{y} \mid \mathbf{x}) \geq 0$
- subadditivity:
  $\mathrm{C}(\mathbf{x}, \mathbf{y}) \leq \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$, cf. $\mathrm{I}(\mathbf{x} : \mathbf{y}) \geq -O(\log(|\mathbf{x}| + |\mathbf{y}|))$

Kolmogorov complexity: information inequalities

similar to Shannon's case:

- monotonicity:

  $\mathrm{C}(\mathbf{x}) \le \mathrm{C}(\mathbf{x},\mathbf{y}) + O(1)$, cf. $\mathrm{C}(\mathbf{y} \mid \mathbf{x}) \ge 0$

- subadditivity:

  $\mathrm{C}(\mathbf{x},\mathbf{y}) \le \mathrm{C}(\mathbf{x}) + \mathrm{C}(\mathbf{y}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$, cf. $\mathrm{I}(\mathbf{x} : \mathbf{y}) \ge -O(\log(|\mathbf{x}| + |\mathbf{y}|))$

- submodularity:

  $\mathrm{C}(\mathbf{x},\mathbf{y},\mathbf{z}) + \mathrm{C}(\mathbf{z}) \le \mathrm{C}(\mathbf{x},\mathbf{z}) + \mathrm{C}(\mathbf{y},\mathbf{z}) + O(\log(|\mathbf{x}| + |\mathbf{y}|))$,
  cf. $\mathrm{I}(\mathbf{x} : \mathbf{y} \mid \mathbf{z}) \ge -O(\log(|\mathbf{x}| + |\mathbf{y}| + |\mathbf{z}|))$

Kolmogorov complexity: information inequalities

similar to Shannon's case:

- monotonicity:
  $\mathrm{C}(\mathbf{x}_{\mathcal{I}}) \leq \mathrm{C}(\mathbf{x}_{\mathcal{I}\cup\mathcal{J}}) + O(1)$
- subadditivity:
  $\mathrm{C}(\mathbf{x}_{\mathcal{I}\cup\mathcal{J}})) \leq \mathrm{C}(\mathbf{x}_{\mathcal{I}}) + \mathrm{C}(\mathbf{x}_{\mathcal{J}}) + O(\log \ldots)$
- submodularity:
  $\mathrm{C}(\mathbf{x}_{\mathcal{I}\cup\mathcal{J}\cup\mathcal{K}})) + \mathrm{C}(\mathbf{x}_{\mathcal{K}}) \leq \mathrm{C}(\mathbf{x}_{\mathcal{I}\cup\mathcal{K}}) + \mathrm{C}(\mathbf{x}_{\mathcal{J}\cup\mathcal{K}}) + O(\log \ldots)$

Kolmogorov complexity: information inequalities

similar to Shannon's case:

- monotonicity:
  $\mathrm{C}(\mathbf{x}_{\mathcal{I}}) \leq \mathrm{C}(\mathbf{x}_{\mathcal{I}\cup\mathcal{J}}) + O(1)$
- subadditivity:
  $\mathrm{C}(\mathbf{x}_{\mathcal{I}\cup\mathcal{J}})) \leq \mathrm{C}(\mathbf{x}_{\mathcal{I}}) + \mathrm{C}(\mathbf{x}_{\mathcal{J}}) + O(\log \ldots)$
- submodularity:
  $\mathrm{C}(\mathbf{x}_{\mathcal{I}\cup\mathcal{J}\cup\mathcal{K}})) + \mathrm{C}(\mathbf{x}_{\mathcal{K}}) \leq \mathrm{C}(\mathbf{x}_{\mathcal{I}\cup\mathcal{K}}) + \mathrm{C}(\mathbf{x}_{\mathcal{J}\cup\mathcal{K}}) + O(\log \ldots)$

Theorem

The same classes of linear inequalities are true for Shannon entropy and (up to a log*-term) for Kolmogorov complexity.*

mutual information and structural properties

How to construct $\mathbf{x} = x_1 \dots x_{2n}$ and $\mathbf{y} = y_1 \dots y_{2n}$ such that

mutual information and structural properties

How to construct $\mathbf{x} = x_1 \dots x_{2n}$ and $\mathbf{y} = y_1 \dots y_{2n}$ such that

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n\ ?$$

mutual information and structural properties

How to construct $\mathbf{x} = x_1 \dots x_{2n}$ and $\mathbf{y} = y_1 \dots y_{2n}$ such that

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n\ ?$$

Example 1:

$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

mutual information and structural properties

How to construct $\mathbf{x} = x_1 \dots x_{2n}$ and $\mathbf{y} = y_1 \dots y_{2n}$ such that

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n\ ?$$

Example 1:

$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

Example 2: $\mathbf{x}, \mathbf{y} \in \{0,1\}^{2n}$ and

$$\mathrm{Dist}_{\mathrm{Hamming}}(\mathbf{x}, \mathbf{y}) = 0.11 \dots \cdot (2n).$$

mutual information and structural properties

How to construct $\mathbf{x} = x_1 \dots x_{2n}$ and $\mathbf{y} = y_1 \dots y_{2n}$ such that

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n\ ?$$

Example 1:

$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

Example 2: $\mathbf{x}, \mathbf{y} \in \{0,1\}^{2n}$ and

$$\mathrm{Dist}_{\mathrm{Hamming}}(\mathbf{x}, \mathbf{y}) = 0.11 \dots \cdot (2n).$$

$$\mathrm{C}(\mathbf{x} \mid \mathbf{y}) \approx \log \binom{2n}{0.11 \cdot (2n)} \approx n$$

mutual information and structural properties

How to construct $\mathbf{x} = x_1 \dots x_{2n}$ and $\mathbf{y} = y_1 \dots y_{2n}$ such that

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n\ ?$$

Example 1:

$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

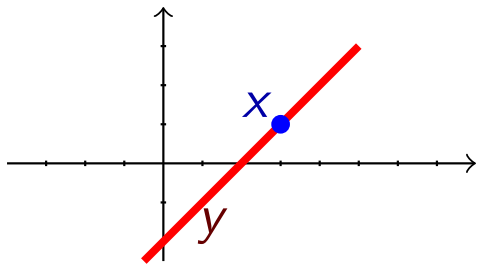
Example 2: $\mathbf{x}, \mathbf{y} \in \{0,1\}^{2n}$ and

$$\mathrm{Dist}_{\mathrm{Hamming}}(\mathbf{x}, \mathbf{y}) = 0.11 \dots \cdot (2n).$$

$$\mathrm{C}(\mathbf{x} \mid \mathbf{y}) \approx \log \binom{2n}{0.11 \cdot (2n)} \approx n$$

Example 3: finite field $\mathbb{F}$ with 2^n elements

$$\begin{aligned} \mathbf{x} &= \text{point on } \mathbb{F}^2 \\ \mathbf{y} &= \text{line on } \mathbb{F}^2 \end{aligned}$$



line and **point** are incident

mutual information and structural properties

We have examples of $\mathbf{x} = x_1 \dots x_{2n}$ and $\mathbf{y} = y_1 \dots y_{2n}$ such that

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n\ ?$$

Example 1:

$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

Example 2: $\mathbf{x}, \mathbf{y} \in \{0,1\}^{2n}$ and $\mathrm{Dist}_{\mathrm{Hamming}}(\mathbf{x}, \mathbf{y}) = 0.11 \dots \cdot (2n)$.

Example 3: finite field $\mathbb{F}$ with 2^n elements

$$\begin{aligned} \mathbf{x} &= \text{point on } \mathbb{F}^2 \\ \mathbf{y} &= \text{line on } \mathbb{F}^2 \end{aligned}$$

line and **point** are incident

mutual information and structural properties

We have examples of $\mathbf{x} = x_1 \dots x_{2n}$ and $\mathbf{y} = y_1 \dots y_{2n}$ such that

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n\ ?$$

Example 1:

$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

Example 2: $\mathbf{x}, \mathbf{y} \in \{0,1\}^{2n}$ and $\mathrm{Dist}_{\mathrm{Hamming}}(\mathbf{x}, \mathbf{y}) = 0.11 \dots \cdot (2n)$.

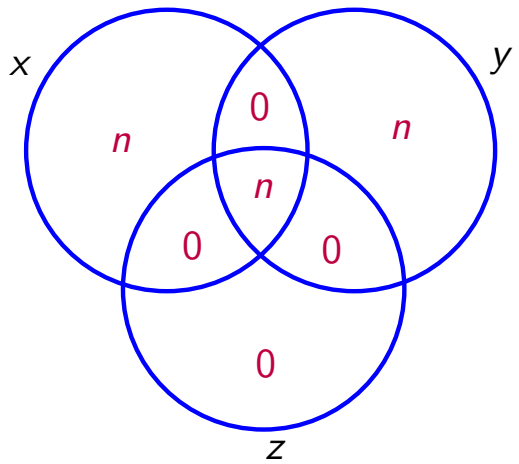
Example 3: finite field $\mathbb{F}$ with 2^n elements

$$\begin{aligned} \mathbf{x} &= \text{point on } \mathbb{F}^2 \\ \mathbf{y} &= \text{line on } \mathbb{F}^2 \end{aligned}$$

line and **point** are incident

does there exist a z as follows?

- $\mathrm{C}(\mathbf{z}) \approx n$
- $\mathrm{C}(\mathbf{z} \mid \mathbf{x}) \approx 0$
- $\mathrm{C}(\mathbf{z} \mid \mathbf{y}) \approx 0$



mutual information and structural properties

We have examples of $\mathbf{x} = x_1 \dots x_{2n}$ and $\mathbf{y} = y_1 \dots y_{2n}$ such that

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n\ ?$$

Example 1:

$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

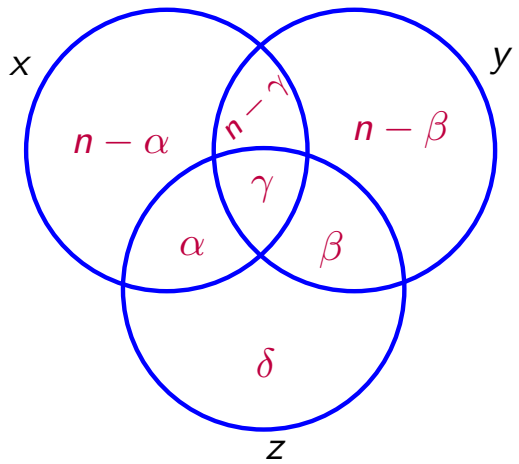
Example 2: $\mathbf{x}, \mathbf{y} \in \{0,1\}^{2n}$ and $\mathrm{Dist}_{\mathrm{Hamming}}(\mathbf{x}, \mathbf{y}) = 0.11 \dots \cdot (2n)$.

Example 3: finite field $\mathbb{F}$ with 2^n elements

$$\begin{aligned} \mathbf{x} &= \text{point on } \mathbb{F}^2 \\ \mathbf{y} &= \text{line on } \mathbb{F}^2 \end{aligned}$$

line and **point** are incident

In general, what **profiles** for $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ can we get for these $(\mathbf{x}, \mathbf{y})$ and various z?



secret key agreement

Alice holds **x**

Bob holds **y**

secret key agreement

Alice holds $\mathbf{x} = x_1 \dots x_{2n}$

Bob holds $\mathbf{y} = y_1 \dots y_{2n}$

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key $\mathbf{w}$

secret key agreement

Alice holds $\mathbf{x} = x_1 \dots x_{2n}$
Bob holds $\mathbf{y} = y_1 \dots y_{2n}$

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key $\mathbf{w}$

secrecy means $\mathrm{I}(\mathbf{w} : \texttt{communication\_transcript}) \approx 0$

secret key agreement

Alice holds $\mathbf{x} = x_1 \dots x_{2n}$
Bob holds $\mathbf{y} = y_1 \dots y_{2n}$

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key $\mathbf{w}$

secrecy means $\mathrm{I}(\mathbf{w} : \texttt{communication\_transcript}) \approx 0$

Example 1:

$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

secret key agreement

Alice holds $\mathbf{x} = x_1 \dots x_{2n}$
Bob holds $\mathbf{y} = y_1 \dots y_{2n}$

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key $\mathbf{w}$

secrecy means $\mathrm{I}(\mathbf{w} : \texttt{communication\_transcript}) \approx 0$

Example 1:

$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

Example 2: (x_i, y_i) is a sequence of $2n$ i.i.d. pairs,

$$\mathrm{prob}[x_i = 1] = 0.5,\ \mathrm{prob}[y_i = 1] = 0.5,\ \mathrm{prob}[x_i = y_i] \approx 0.11$$

secret key agreement

Alice holds $\mathbf{x} = x_1 \dots x_{2n}$
Bob holds $\mathbf{y} = y_1 \dots y_{2n}$

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key $\mathbf{w}$

secrecy means $\mathrm{I}(\mathbf{w} : \mathtt{communication\_transcript}) \approx 0$

Example 1:

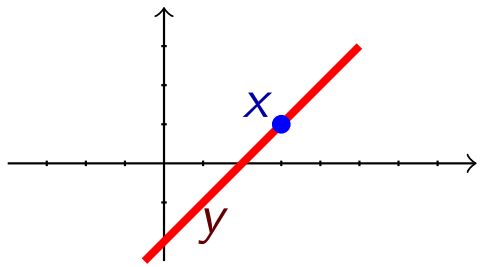
$$\begin{aligned} x_1 \dots x_{2n} &= u_1 \dots u_n w_1 \dots w_n \\ y_1 \dots y_{2n} &= v_1 \dots v_n w_1 \dots w_n \end{aligned}$$

Example 2: (x_i, y_i) is a sequence of $2n$ i.i.d. pairs,

$$\mathrm{prob}[x_i = 1] = 0.5,\ \mathrm{prob}[y_i = 1] = 0.5,\ \mathrm{prob}[x_i = y_i] \approx 0.11$$

Example 3: finite field $\mathbb{F}$ with 2^n elements

$\mathbf{x}$ = point on $\mathbb{F}^2$
$\mathbf{y}$ = line on $\mathbb{F}^2$



line and **point** are incident

secret key agreement

Alice holds **x** and **Bob** holds **y**,

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

secret key agreement

Alice holds **x** and **Bob** holds **y**,

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key **w**

secret key agreement

Alice holds **x** and **Bob** holds **y**,

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key **w**

secrecy means $\mathrm{I}(\mathbf{w} : \mathtt{communication\_transcript}) \approx 0$

Theorem

There exists a protocol that guarantees a secret key **w** *such that* $\mathrm{C}(\mathbf{w}) \approx n$.

secret key agreement

Alice holds **x** and **Bob** holds **y**,

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key **w**

secrecy means $\mathrm{I}(\mathbf{w} : \mathtt{communication\_transcript}) \approx 0$

Theorem

There exists a protocol that guarantees a secret key **w** *such that* $\mathrm{C}(\mathbf{w}) \approx n$.

Theorem

No protocol guarantees $\mathrm{C}(\mathbf{w}) \gg n$.

secret key agreement

Alice holds **x** and **Bob** holds **y**,

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key **w**

secrecy means $\mathrm{I}(\mathbf{w} : \texttt{communication\_transcript}) \approx 0$

Theorem

There exists a protocol that guarantees a secret key **w** *such that* $\mathrm{C}(\mathbf{w}) \approx n$.

Theorem

No protocol guarantees $\mathrm{C}(\mathbf{w}) \gg n$.

Theorem

- *There exists a protocol with* $\mathrm{C}(\mathbf{w}) \approx n$ *where*
  Alice sends $\mathrm{C}(\mathbf{x} \mid \mathbf{y}) \approx n$ *bits and Bob sends nothing.*
- *There exists a protocol with* $\mathrm{C}(\mathbf{w}) \approx n$ *where*
  Bob sends $\mathrm{C}(\mathbf{y} \mid \mathbf{x}) \approx n$ *bits and Alice sends nothing.*

secret key agreement

Alice holds **x** and **Bob** holds **y**,

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key **w**

secrecy means $\mathrm{I}(\mathbf{w} : \texttt{communication\_transcript}) \approx 0$

Theorem

- *There exists a protocol s.t. for all such* $\mathbf{x}, \mathbf{y}$ *we get* $\mathrm{C}(\mathbf{w}) \approx n$
  Alice sends $\mathrm{C}(\mathbf{x} \mid \mathbf{y}) \approx n$ *bits and Bob sends nothing.*
- *There exists a protocol s.t. for all such* $\mathbf{x}, \mathbf{y}$ *we get* $\mathrm{C}(\mathbf{w}) \approx n$
  Bob sends $\mathrm{C}(\mathbf{y} \mid \mathbf{x}) \approx n$ *bits and Alice sends nothing.*
-

secret key agreement

Alice holds **x** and **Bob** holds **y**,

$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key **w**

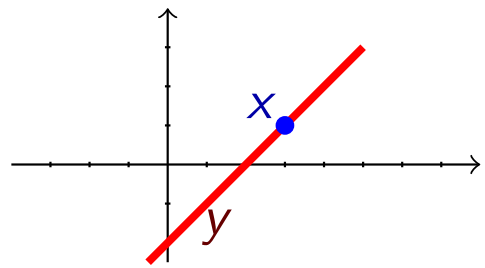
secrecy means $\mathrm{I}(\mathbf{w} : \texttt{communication\_transcript}) \approx 0$

Theorem

- *There exists a protocol s.t. for all such* $\mathbf{x}, \mathbf{y}$ *we get* $\mathrm{C}(\mathbf{w}) \approx n$
  Alice sends $\mathrm{C}(\mathbf{x} \mid \mathbf{y}) \approx n$ *bits and Bob sends nothing.*
- *There exists a protocol s.t. for all such* $\mathbf{x}, \mathbf{y}$ *we get* $\mathrm{C}(\mathbf{w}) \approx n$
  Bob sends $\mathrm{C}(\mathbf{y} \mid \mathbf{x}) \approx n$ *bits and Alice sends nothing.*
- *for some* $\mathbf{x}, \mathbf{y}$ *we cannot do anything substantially different.*

Simple Example: finite field $\mathbb{F}$ with 2^n elements

$$\begin{aligned} \mathbf{x} &= \text{point on } \mathbb{F}^2 \\ \mathbf{y} &= \text{line on } \mathbb{F}^2 \end{aligned}$$



line and **point** are incident

secret key agreement

Alice holds **x** and **Bob** holds **y**,

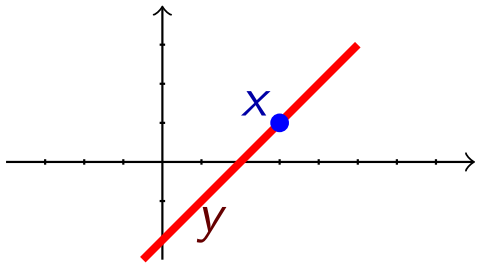
$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key **w**

secrecy means $\mathrm{I}(\mathbf{w} : \texttt{communication\_transcript}) \approx 0$

Interesting Example: finite field $\mathbb{F}$ with 2^n elements

$$\begin{array}{rcl} \mathbf{x} & = & \text{point on } \mathbb{F}^2 \\ \mathbf{y} & = & \text{line on } \mathbb{F}^2 \end{array}$$



line and **point** are incident

Theorem

If $\mathrm{C}(\mathbf{w}) \approx n$ *then Alice sends* $\approx n$ *bit or Bob sends* $\approx n$ *bits.*

secret key agreement

Alice holds **x** and **Bob** holds **y**,

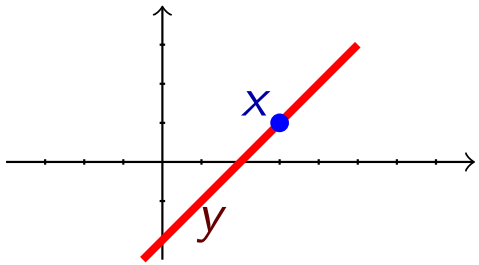
$$\mathrm{C}(\mathbf{x}) = 2n,\ \mathrm{C}(\mathbf{y}) = 2n,\ \mathrm{I}(\mathbf{x} : \mathbf{y}) = n.$$

Alice and Bob communication via a public channel and agree on a secret key **w**

secrecy means $\mathrm{I}(\mathbf{w} : \texttt{communication\_transcript}) \approx 0$

Interesting Example: finite field $\mathbb{F}$ with 2^n elements

$$\begin{array}{rcl} \mathbf{x} & = & \text{point on } \mathbb{F}^2 \\ \mathbf{y} & = & \text{line on } \mathbb{F}^2 \end{array}$$



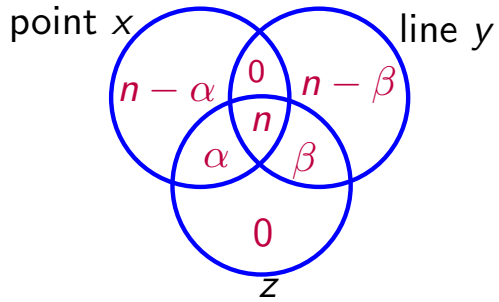
line and **point** are incident

Theorem

If $\mathrm{C}(\mathbf{w}) \approx n$ then Alice sends $\approx n$ bit or Bob sends $\approx n$ bits.

Lemma (An. Muchnik)

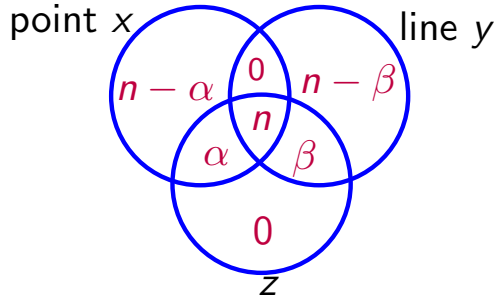
In such a **complexity profile** *either $\alpha = n$ or $\beta = n$*



combinatorics of the plane

Lemma (An. Muchnik)

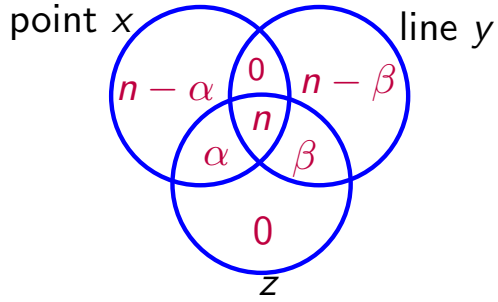
In such a **complexity profile** *either* $\alpha = n$ *or* $\beta = n$



combinatorics of the plane

Lemma (An. Muchnik)

In such a **complexity profile** *either* $\alpha = n$ *or* $\beta = n$

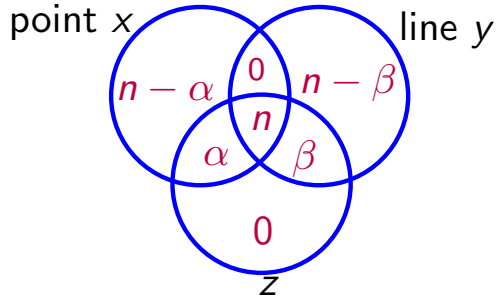


sketch of proof:

combinatorics of the plane

Lemma (An. Muchnik)

In such a **complexity profile**
either $\alpha = n$ *or* $\beta = n$



sketch of proof: w.l.o.g. $\alpha \geq \beta$

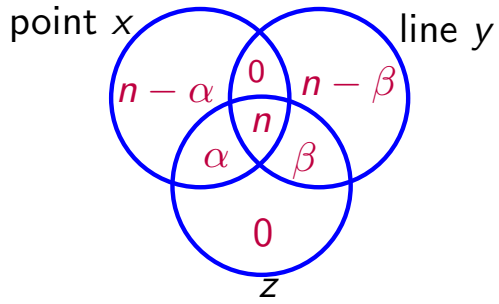
$$\mathrm{C}(x \mid z) = n - \alpha,\ \mathrm{C}(y \mid z) = n - \beta,\ \mathrm{C}(x, y \mid z) = 2n - \alpha - \beta$$

$$\begin{aligned} A &= \{x' \text{ is a point on } \mathbb{F}^2 \ :\ \mathrm{C}(x' \mid z) \leq n - \alpha\} \\ B &= \{y' \text{ is a line on } \mathbb{F}^2 \ :\ \mathrm{C}(y' \mid z) \leq n - \beta\} \end{aligned}$$

combinatorics of the plane

Lemma (An. Muchnik)

In such a **complexity profile**
either $\alpha = n$ *or* $\beta = n$



sketch of proof: w.l.o.g. $\alpha \geq \beta$

$$\mathrm{C}(x \mid z) = n - \alpha,\ \mathrm{C}(y \mid z) = n - \beta,\ \mathrm{C}(x, y \mid z) = 2n - \alpha - \beta$$

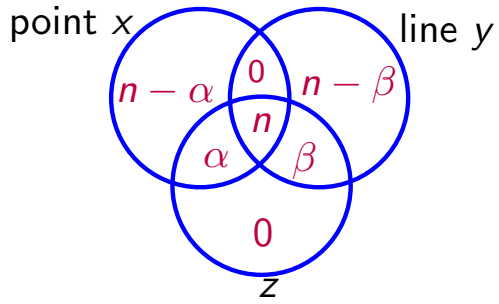
$$\begin{array}{rcl} A & = & \{x' \text{ is a point on } \mathbb{F}^2 \ : \ \mathrm{C}(x' \mid z) \leq n - \alpha\} \\ B & = & \{y' \text{ is a line on } \mathbb{F}^2 \ : \ \mathrm{C}(y' \mid z) \leq n - \beta\} \end{array}$$

Counting Claim: $\mathrm{Card}(A) = 2^{n-\alpha \pm O(\log n)}$ and $\mathrm{Card}(B) = 2^{n-\beta \pm O(\log n)}$

combinatorics of the plane

Lemma (An. Muchnik)

In such a **complexity profile**
either $\alpha = n$ *or* $\beta = n$



sketch of proof: w.l.o.g. $\alpha \geq \beta$

$$\mathrm{C}(x \mid z) = n - \alpha,\ \mathrm{C}(y \mid z) = n - \beta,\ \mathrm{C}(x, y \mid z) = 2n - \alpha - \beta$$

$$\begin{array}{rcl} A & = & \{x' \text{ is a point on } \mathbb{F}^2 \ : \ \mathrm{C}(x' \mid z) \leq n - \alpha\} \\ B & = & \{y' \text{ is a line on } \mathbb{F}^2 \ : \ \mathrm{C}(y' \mid z) \leq n - \beta\} \end{array}$$

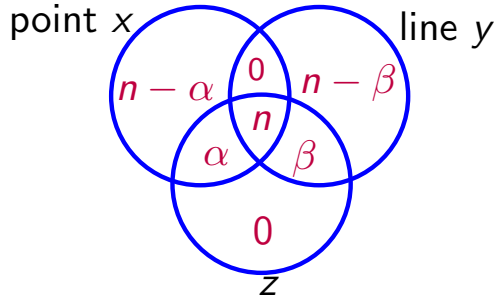
Counting Claim: $\mathrm{Card}(A) = 2^{n-\alpha \pm O(\log n)}$ and $\mathrm{Card}(B) = 2^{n-\beta \pm O(\log n)}$

Geometric fact: number of incidences in $A \times B$ is $\leq O\left(\sqrt{\mathrm{Card}(A)} \cdot \mathrm{Card}(B)\right)$

combinatorics of the plane

Lemma (An. Muchnik)

In such a **complexity profile**
either $\alpha = n$ *or* $\beta = n$



sketch of proof: w.l.o.g. $\alpha \geq \beta$

$$\mathrm{C}(x \mid z) = n - \alpha,\ \mathrm{C}(y \mid z) = n - \beta,\ \mathrm{C}(x, y \mid z) = 2n - \alpha - \beta$$

$$\begin{array}{rcl} A & = & \{x' \text{ is a point on } \mathbb{F}^2 \ : \ \mathrm{C}(x' \mid z) \leq n - \alpha\} \\ B & = & \{y' \text{ is a line on } \mathbb{F}^2 \ : \ \mathrm{C}(y' \mid z) \leq n - \beta\} \end{array}$$

Counting Claim: $\mathrm{Card}(A) = 2^{n-\alpha \pm O(\log n)}$ and $\mathrm{Card}(B) = 2^{n-\beta \pm O(\log n)}$

Geometric fact: number of incidences in $A \times B$ is $\leq O\left(\sqrt{\mathrm{Card}(A)} \cdot \mathrm{Card}(B)\right)$

therefore:

$$\begin{array}{rcl} n - \alpha + n - \beta & = & \\ \mathrm{C}(x, y \mid z) & \leq & \log[\text{ no. of incidences in } A \times B\ ] \\ & \leq & 0.5 \log \mathrm{Card}(A) + \log \mathrm{Card}(B) = 1.5n - 0.5\alpha - \beta \end{array}$$

from combinatorics of the plane to secret sharing

Reminder: a finite plane; $A =$ *some set of lines* and $B =$ *some set of points*

from combinatorics of the plane to secret sharing

Reminder: a finite plane; $A =$ *some set of lines* and $B =$ *some set of points*

Geometric fact: number of incidences in $A \times B$ is $\leq O\left(\sqrt{\mathrm{Card}(A)} \cdot \mathrm{Card}(B)\right)$

or $\leq O\left(\mathrm{Card}(A) \cdot \sqrt{\mathrm{Card}(B)}\right)$

from combinatorics of the plane to secret sharing

Reminder: a finite plane; $A =$ *some set of lines* and $B =$ *some set of points*

Geometric fact: number of incidences in $A \times B$ is $\leq O\left(\sqrt{\mathrm{Card}(A)} \cdot \mathrm{Card}(B)\right)$

or $\leq O\left(\mathrm{Card}(A) \cdot \sqrt{\mathrm{Card}(B)}\right)$

Conclusion: in a secret key agreement protocol, on *some* pairs of inputs, either Alice sends $\mathrm{C}(x \mid y)$ bits or Bob sends $\mathrm{C}(y \mid x)$ bits

from combinatorics of the plane to secret sharing

Reminder: a finite plane; $A =$ *some set of lines* and $B =$ *some set of points*

Geometric fact: number of incidences in $A \times B$ is $\leq O\left(\sqrt{\mathrm{Card}(A)} \cdot \mathrm{Card}(B)\right)$

or $\leq O\left(\mathrm{Card}(A) \cdot \sqrt{\mathrm{Card}(B)}\right)$

Conclusion: in a secret key agreement protocol, on *some* pairs of inputs, either Alice sends $\mathrm{C}(x \mid y)$ bits or Bob sends $\mathrm{C}(y \mid x)$ bits

Comment: some subtler properties of planes imply some subtler bounds for communication protocols

Proceed with the exercises!