# New Properties of the Intrinsic Information and Their Relation to Bound Secrecy

Andrew Tung, Karthik Vedula

MIT PRIMES

October 15, 2022

# Overview

1. Entropy

2. Secret-key rate and bound secrecy

3. Our result

# Informal definition

Informally,

- Bit is 0 or 1
- Encoding a variable using bits = replacing outputs with binary strings (used to compress data)

# Informal definition

Informally,

- Bit is 0 or 1
- Encoding a variable using bits = replacing outputs with binary strings (used to compress data)

Data is generally a continuous stream of digits, so we can get confused about what a string represents

# Informal definition

Informally,

- Bit is 0 or 1
- Encoding a variable using bits = replacing outputs with binary strings (used to compress data)

Data is generally a continuous stream of digits, so we can get confused about what a string represents

Ex: Encoding from $a \to 0$, $b \to 01$. Bad because if first digit $= 0$, then we're confused

# Informal definition

Informally,

- Bit is 0 or 1
- Encoding a variable using bits = replacing outputs with binary strings (used to compress data)

Data is generally a continuous stream of digits, so we can get confused about what a string represents

Ex: Encoding from $a \to 0$, $b \to 01$. Bad because if first digit $= 0$, then we're confused

Goal: Try to use as few bits (on average) as possible to encode without confusion

# Informal definition

More precisely, for stream of digits, must have a **prefix code**:

# Informal definition

More precisely, for stream of digits, must have a **prefix code**:

**Definition**

A *prefix code* is encoding where no whole code word is a prefix of another code word.

# Informal definition

More precisely, for stream of digits, must have a **prefix code**:

**Definition**

A *prefix code* is encoding where no whole code word is a prefix of another code word.

Goal: try to find best prefix code

**Key Point**

Entropy is minimum number of bits (on average) needed to prefix encode a variable

# Motivating example

Consider a random variable defined as[1]

$$X = \begin{cases} a & \text{probability } \frac{1}{2} \\ b & \text{probability } \frac{1}{4} \\ c & \text{probability } \frac{1}{8} \\ d & \text{probability } \frac{1}{8} \end{cases}$$

How many bits do you need to encode this information?

[1] Example from Nielsen and Chuang, "Quantum Computation and Quantum information."

# Motivating example

One idea: There are 4 outputs, so use $\log_2(4) = 2$ bits (to get 4 outputs)

# Motivating example

One idea: There are 4 outputs, so use $\log_2(4) = 2$ bits (to get 4 outputs)

Encode $a \to 00$, $b \to 01$, $c \to 10$, $d \to 11$. Prefix code because all code words are distinct, fixed length

# Motivating example

One idea: There are 4 outputs, so use $\log_2(4) = 2$ bits (to get 4 outputs)

Encode $a \to 00$, $b \to 01$, $c \to 10$, $d \to 11$. Prefix code because all code words are distinct, fixed length

**Key Point**

Entropy of variable with $n$ outputs $\leq \log_2(n)$.

# Motivating example

No matter the value of $X$, 2 bits needed to encode

# Motivating example

No matter the value of $X$, 2 bits needed to encode

Can we do better/use less bits?

# Motivating example

No matter the value of $X$, 2 bits needed to encode

Can we do better/use less bits?

Yes!

# Motivating example

Idea: $a$ much more common than $b$, $c$, $d$ $\implies$ save a bit on it

# Motivating example

Idea: $a$ much more common than $b$, $c$, $d$ $\implies$ save a bit on it

Encode using this prefix code:

$$a \to 0$$
$$b \to 10$$
$$c \to 110$$
$$d \to 111$$

# Motivating example

Idea: $a$ much more common than $b$, $c$, $d$ $\implies$ save a bit on it

Encode using this prefix code:

$$a \to 0$$
$$b \to 10$$
$$c \to 110$$
$$d \to 111$$

Even though $c$, $d$ use more bits in this code, less prevalent $\implies$ overall save.

# Motivating example

Idea: $a$ much more common than $b$, $c$, $d$ $\implies$ save a bit on it

Encode using this prefix code:

$$\begin{aligned} a &\to 0 \\ b &\to 10 \\ c &\to 110 \\ d &\to 111 \end{aligned}$$

Even though $c$, $d$ use more bits in this code, less prevalent $\implies$ overall save.

Average number of bits required:

$$\frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{8} \cdot 3 + \frac{1}{8} \cdot 3 = \frac{7}{4} < 2$$

# Formal definition

This prefix code gives rise to the Shannon entropy:

# Formal definition

This prefix code gives rise to the Shannon entropy:

**Definition**

Suppose a discrete random variable $X$ has probability distribution $\{p_i\} = p_1, p_2, \ldots, p_n$. The *Shannon entropy* of $X$ is

$$H(X) := \sum_i -p_i \log p_i$$

(where log is taken base 2).

# Formal definition

This prefix code gives rise to the Shannon entropy:

**Definition**

Suppose a discrete random variable $X$ has probability distribution $\{p_i\} = p_1, p_2, \dots, p_n$. The *Shannon entropy* of $X$ is

$$H(X) := \sum_i -p_i \log p_i$$

(where log is taken base 2).

Check: $H(X) = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} = \frac{7}{4}$.

# Operational motivation

**Theorem (Shannon's noiseless coding theorem)**

Given a random variable $X$, any encoding using less than $H(X)$ bits on average is not reliable, while there is always an reliable encoding using $H(X) + \epsilon$ bits on average for all $\epsilon > 0$.

# Operational motivation

**Theorem (Shannon's noiseless coding theorem)**

Given a random variable $X$, any encoding using less than $H(X)$ bits on average is not reliable, while there is always an reliable encoding using $H(X) + \epsilon$ bits on average for all $\epsilon > 0$.

**Key Point**

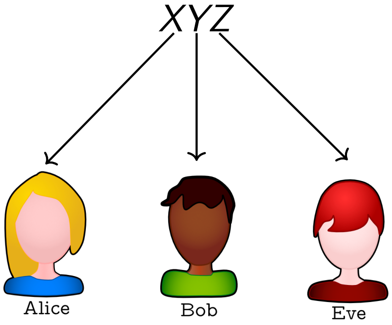
Shannon entropy = our notion of entropy

# Secret-key rate

Consider a joint probability distribution $XYZ$. We sample from the distribution and give Alice $X$, Bob $Y$, and Eve $Z$.

# Secret-key rate

Consider a joint probability distribution $XYZ$. We sample from the distribution and give Alice $X$, Bob $Y$, and Eve $Z$.

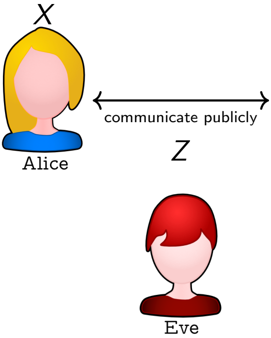


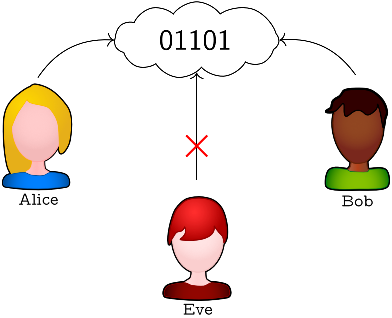
# Secret-key rate

After a sequence of communications which Eve can hear, Alice and Bob attempt to agree on a secret key.

# Secret-key rate

After a sequence of communications which Eve can hear, Alice and Bob attempt to agree on a secret key.



# Secret-key rate vs. sharing secrecy

- Secret-key rate = rate of distilling secret bits both Alice and Bob have that Eve does not

# Secret-key rate vs. sharing secrecy

- Secret-key rate = rate of distilling secret bits both Alice and Bob have that Eve does not
- Sharing secrecy = Alice and Bob have correlation in their random variables that Eve does not have access to

# Secret-key rate vs. sharing secrecy

- Secret-key rate = rate of distilling secret bits both Alice and Bob have that Eve does not
- Sharing secrecy = Alice and Bob have correlation in their random variables that Eve does not have access to

Both seem equivalent, but it is not obvious why. One direction has been proven:

# Secret-key rate vs. sharing secrecy

- Secret-key rate = rate of distilling secret bits both Alice and Bob have that Eve does not
- Sharing secrecy = Alice and Bob have correlation in their random variables that Eve does not have access to

Both seem equivalent, but it is not obvious why. One direction has been proven:

**Theorem (Maurer & Wolf, 1999)**

If Alice and Bob do not share secrecy, they cannot distill a secret key.

# Examples

| $X$ \ $Y$ | 0 | 1 |
|---|---|---|
| 0 | 1/4 | 1/4 |
| 1 | 1/4 | 1/4 |

| $Z$ | prob. |
|---|---|
| 0 | 1/2 |
| 1 | 1/2 |

| Share secrecy | Can gen. key |
|---|---|
| ✗ | ✗ |

# Examples

| Y \ X | 0 | 1 |
|---|---|---|
| 0 | 1/4 | 1/4 |
| 1 | 1/4 | 1/4 |

| $Z$ | prob. |
|---|---|
| 0 | 1/2 |
| 1 | 1/2 |

| Share secrecy | Can gen. key |
|---|---|
| ✗ | ✗ |

| Y \ X | 0 | 1 |
|---|---|---|
| 0 | 1/2 | 0 |
| 1 | 0 | 1/2 |

| $Z$ | prob. |
|---|---|
| 0 | 1/2 |
| 1 | 1/2 |

| Share secrecy | Can gen. key |
|---|---|
| ✓ | ✓ |

# Examples

| | Share secrecy | Can gen. key |
|---|---|---|
| Example 1 | ✗ | ✗ |
| Example 2 | ✓ | ✓ |
| Example 3 | ✗ | ✗ |

**Example 1**

| $X$ \ $Y$ | 0 | 1 |
|---|---|---|
| 0 | 1/4 | 1/4 |
| 1 | 1/4 | 1/4 |

| $Z$ | prob. |
|---|---|
| 0 | 1/2 |
| 1 | 1/2 |

Share secrecy: ✗ Can gen. key: ✗

**Example 2**

| $X$ \ $Y$ | 0 | 1 |
|---|---|---|
| 0 | 1/2 | 0 |
| 1 | 0 | 1/2 |

| $Z$ | prob. |
|---|---|
| 0 | 1/2 |
| 1 | 1/2 |

Share secrecy: ✓ Can gen. key: ✓

**Example 3**

| $X$ \ $Y$ | 0 | 1 |
|---|---|---|
| 0 | 1/2 | 0 |
| 1 | 0 | 1/2 |

Eve receives what Alice gets.

Share secrecy: ✗ Can gen. key: ✗

# Bound secrecy

The conjecture of bound secrecy states that there are distributions $XYZ$ such that Alice and Bob share secrecy but they cannot agree on a secret key.

| Share secrecy | Can generate a secret key |
|---|---|
| ✓ | ✗ |

# Bound secrecy

The conjecture of bound secrecy states that there are distributions $XYZ$ such that Alice and Bob share secrecy but they cannot agree on a secret key.

| Share secrecy | Can generate a secret key |
|---|---|
| ✓ | ✗ |

This seems impossible!

# Another non-example

| $X$ / $Y$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | $1/8$ | $1/8$ | 0 | 0 |
| 1 | $1/8$ | $1/8$ | 0 | 0 |
| 2 | 0 | 0 | $1/4$ | 0 |
| 3 | 0 | 0 | 0 | $1/4$ |

$$Z \equiv X + Y \text{ mod } 2 \text{ if } X, Y \in \{0, 1\},$$
$$Z \equiv X \text{ mod } 2 \text{ if } X, Y \in \{2, 3\}$$

# Another non-example

| $X$ / $Y$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 1/8 | 1/8 | 0 | 0 |
| 1 | 1/8 | 1/8 | 0 | 0 |
| 2 | 0 | 0 | 1/4 | 0 |
| 3 | 0 | 0 | 0 | 1/4 |

$$Z \equiv X + Y \bmod 2 \text{ if } X, Y \in \{0, 1\},$$
$$Z \equiv X \bmod 2 \text{ if } X, Y \in \{2, 3\}$$

Share secrecy ✓

Can generate a secret key ✓

How do Alice and Bob extract the secret key?

# Another non-example

| $X$ / $Y$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | $1/8$ | $1/8$ | 0 | 0 |
| 1 | $1/8$ | $1/8$ | 0 | 0 |
| 2 | 0 | 0 | $1/4$ | 0 |
| 3 | 0 | 0 | 0 | $1/4$ |

Let $U = \lfloor X/2 \rfloor$. This is a secret bit shared between Alice and Bob.

# Another non-example

| $X$ / $Y$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | $1/8$ | $1/8$ | 0 | 0 |
| 1 | $1/8$ | $1/8$ | 0 | 0 |
| 2 | 0 | 0 | $1/4$ | 0 |
| 3 | 0 | 0 | 0 | $1/4$ |

Let $U = \lfloor X/2 \rfloor$. This is a secret bit shared between Alice and Bob.

If Eve knew $U$, Alice and Bob would have no secrecy.

# Our results

Formalizing the previous example:

**Definition**

The *reduced intrinsic information* is informally the smallest amount of information we need to tell Eve in order for Alice and Bob to share no secrecy.

# Our results

Formalizing the previous example:

**Definition**

The *reduced intrinsic information* is informally the smallest amount of information we need to tell Eve in order for Alice and Bob to share no secrecy.

**Our results**

Assuming the conjecture of bound secrecy, we have shown that the reduced intrinsic information does NOT measure whether Alice and Bob can agree on a secret key.

# Acknowledgements


- Our mentor (Andrey Khesin)
- MIT PRIMES-USA, Prof. Pavel Etingof, Dr. Slava Gerovitch
- Dr. Tanya Khovanova


*Thanks for listening!*