HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023

09/10/2023. Lecture 5.

1 Inequalities for Shannon's entropy

In the previous lectures we proved several basic properties of Shannon's entropy, e.g.,

- $H(A, B) = H(A) + H(B \mid A)$
- $H(A, B) \leq H(A) + H(B)$
- $H(A \mid B) \leq H(A)$

We used this properties to prove several more involved inequalities for entropy.

Example 1. For any triple of jointly distributed random variables (X, Y, Z) we have

$$H(X, Y \mid Z) \leq H(X \mid Z) + H(Y \mid Z).$$

Indeed, the inequality $H(A, B) \leq H(A) + H(B)$ is true for any distribution of two random variables. In particular, this inequality applies to each conditional distribution of (X, Y) given the assumption that $Z = c_\ell$ (for each value c_ℓ of Z with a positive probability). In the usual notation, this means that

$$H(X, Y \mid Z = c_\ell) \leq H(X \mid Z = c_\ell) + H(Y \mid Z = c_\ell).$$

Therefore

$$\sum_\ell \mathrm{Prob}[Z = c_\ell] \cdot H(X, Y \mid Z = c_\ell) \leq \sum_\ell \mathrm{Prob}[Z = c_\ell] \cdot H(X \mid Z = c_\ell) + \sum_\ell \mathrm{Prob}[Z = c_\ell] \cdot H(Y \mid Z = c_\ell),$$

which gives $H(X, Y \mid Z) \leq H(X \mid Z) + H(Y \mid Z)$.

Example 2. For any triple of jointly distributed random variables (X, Y, Z) we have

$$H(X, Y, Z) + H(Z) \leq H(X, Z) + H(Y, Z).$$

Let us observe that this inequality is equivalent to

$$H(X, Y \mid Z) + 2H(Z) \leq H(X \mid Z) + H(Y \mid Z) + 2H(Z),$$

and we get again the inequality from Example 1.

Example 3. For any triple of jointly distributed random variables (X, Y, Z) we have

$$H(X \mid Y, Z) \leq H(X \mid Z)$$

Indeed, this inequality rewrites to $H(X, Y, Z) - H(Y, Z) \leq H(X, Y) - H(Z)$, which is equivalent to Example 2 above.

Example 4. For any triple of jointly distributed random variables (X, Y, Z) we have

$$I(X : Y) \leq I(X : \langle Y, Z \rangle).$$

(proven in the class).

In the class we discussed DM

$$2H(X,Y,Z) \leq H(X,Y) + H(X,Z) + H(Y,Z).$$

We also discussed the relation between

$$I(X:Z) + I(Y:Z) \text{ and } I(\langle X,Y\rangle : Z).$$

It turns out that for some distributions (X,Y,Z) we have $I(X:Z) + I(Y:Z) < I(\langle X,Y\rangle : Z)$ while for others $I(X:Z) + I(Y:Z) > I(\langle X,Y\rangle : Z)$.

Exercise 1. Show that for any triple of jointly distributed random variables (X,Y,Z)

$$H(Z) \leq H(Z \mid X) + H(Z \mid Y) + I(X:Y).$$

Exercise 2. Show that for any triple of jointly distributed random variables (X,Y,Z)

$$I(X : \langle Y,Z\rangle) \leq I(X:Y) + H(Z \mid Y).$$

2 Compression of clear texts and of a secret key

We briefly discussed theoretical limits of compression for an open text (the optimal compression Shannon entropy can be define din terms of Shannon's entropy) and for a secret key for any secure encryption scheme (cannot be made shorter than Shannon's entropy of the clear text).

3 Attack with a chosen pair of clear messages

Let $\Pi = \langle \mathrm{Gen}(), \mathrm{Enc}(), \mathrm{Dec}()\rangle$ be an encryption scheme, where $\mathcal{M}, \mathcal{E}, \mathcal{K}$ are the spaces of *clear messages*, *encrypted messages*, and *secret key* respectively. Let us consider the following game between an adversary and Alice.

- Adversary uses an algorithm $Adv_1()$ that chooses two clear messages $m_a, m_b \in \mathcal{M}$;
- Alice chooses at random $i \in \{a,b\}$ (with equal probabilities), samples a secret key $k \leftarrow \mathrm{Gen}()$, and computes the encrypted message $e = \mathrm{Enc}(m_i, k)$;
- Adversary computes $j \in \{a,b\}$ using another algorithm $j \leftarrow Adv_2(m_a, m_b, e)$.

The success of the adversary is defined as follows:

$$\mathbf{success} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$$

In words: the adversary prepared a pair of messages m_a, m_b; Alice decides which message to encrypt; then the adversary tries to understand which of the messages was encrypted.

Theorem 1. *If* $\Pi = \langle \mathrm{Gen}(), \mathrm{Enc}(), \mathrm{Dec}()\rangle$ *is a secure encryption scheme, then*

$$\mathrm{Prob}[\mathbf{success} = 1] = 1/2.$$

In words: the adversary has no better strategy than simply toss a coin and suggest an answer at random

(We proved this theorem in the class.)

4 Practical algorithms and admissibly small errors

We say that an algorithm is computationally efficient (feasible) if it stops in time at most $\mathrm{poly}(n)$ for all inputs of size n (for some polynomial $\mathrm{poly}(n)$). This definition applies to deterministic and to randomized algorithms. This definition defines the same class of algorithm for many popular models of computation, such as Turing machines with one or many tapes, random-access machine, and many other models.

We say that a function $f : \mathbb{N} \to \mathbb{R}_+$ is *negligible*, if for any polynomial $\mathrm{poly}(n)$ there is a natural number n_0 such that for all $n > n_0$ we have $|f(n)| < 1/|\mathrm{poly}(n)|$. In words: a negligible function goes to 0 faster than any inverted polynomial.

Exercise 3.
(a) If $f(n)$ and $g(n)$ are negligible functions, then $f(n) + g(n)$ and $f(n) \cdot g(n)$ are also negligible.
(b) If $f(n)$ is negligible function and C is a real number, then $C \cdot f(n)$ is also a negligible number.
(c) The functions e^{-n}, $e^{-n/10}$, $e^{\sqrt{n}}$, $n^{-\log n}$ are negligible.
(d) The functions $1/\log n$, $1/\sqrt{n}$, $1/(n+5)^2$, $1/n^{10}$ are not negligible.

5 Computational security: basic definiions

Definition 1. An encryption scheme $\Pi = \langle \mathrm{Gen}(), \mathrm{Enc}(), \mathrm{Dec}() \rangle$ is *poly-time computable* if

- $\mathrm{Gen}(\underbrace{11\ldots1}_{n})$ samples a key $k \in \mathcal{K}_n$ (a secret key used for messages of length n)
- $\mathrm{Enc}(m, k)$ applied to a clear message $m \in \mathcal{M}_n$ of length n and a secret key $k \in \mathcal{K}_n$ returns an encrypted message $e \in \mathcal{E}_n$
- $\mathrm{Dec}(m, k)$ applied to an encrypted message $e \in \mathcal{E}_n$ and a secret key $k \in \mathcal{K}_n$ returns either $m \in \mathcal{M}_n$ such that $\mathrm{Enc}(m, k) = e$ or the symbol $\perp$
- each of the algorithms $\langle \mathrm{Gen}(), \mathrm{Enc}(), \mathrm{Dec}() \rangle$ terminates in polynomial time
- for every $m \in \mathcal{M}_n$, for a randomly chosen $k \leftarrow Gen(\underbrace{11\ldots1}_{n})$, the probability

$$\mathrm{Prob}[\mathrm{Dec}(\mathrm{Enc}(m, k), k) = \perp]$$

  is a negligible function.

Definition 2. An encryption scheme $\Pi = \langle \mathrm{Gen}(), \mathrm{Enc}(), \mathrm{Dec}() \rangle$ is *computationally secure* (*sûr au sens calculatoire*), if for every game between Adversary and Alice (following the protocol explained in Section 3) such that the adversary's algorithms Adv_1 and Adv_2 are computable in polynomial time, the gap

$$\left| \mathrm{Prob}[\mathrm{succes}] - \frac{1}{2} \right|$$

is a negligible function.

In the next lecture we will discuss properties of poly-time computable and computationally secure encryption schemes and their potential advantages compared to absolutely secure schemes.

References

[1] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001.

[2] J. Katz, Y. Lindell. Introduction to modern cryptography, CRC Press, 2021

[3] B. Martin. Codage, cryptologie et applications. PPUR presses polytechniques, 2004