UiT the Arctic University, October 2025.
Fall school on Geometry in Cryptography and Communication.

Mini-course *Different Views of Information.* Exercises Part I.

Exercise 1. There are n identical-looking coins, one of which is counterfeit and differs in weight (either lighter or heavier) from the others. Using a balance scale without additional weights, determine the minimum number of weighings needed to identify the counterfeit coin.
(a) $n = 15$; (b) $n = 14$; (c) $n = 12$

Exercise 2. Prove that for any probability distribution $(p_1, \ldots, p_k)$ (with $p_i \geq 0$ for each i, and $\sum p_i = 1$) we have

$$0 \leq \sum p_i \log \frac{1}{p_i} \leq \log k.$$

Explain when this expression (Shannon's entropy) is equal to 0 and when it attains the value $\log k$.

Exercise 3. Find a probability distribution $(p_1, \ldots, p_{100})$ such that $p_i > 0$ for each $i = 1, \ldots, 100$, and

$$\sum p_i \log \frac{1}{p_i} \leq 2.$$

Exercise 4. Let X_ϵ be a random variable such that

$$\begin{array}{rcl} \text{Prob}[X_\epsilon = 1] & = & \epsilon \\ \text{Prob}[X_\epsilon = 0] & = & 1 - \epsilon. \end{array}$$

Prove that $\mathrm{H}(X_\epsilon) \to 0$ as $\epsilon \to 0$.

Exercise 5. Let $\mathbb{F}_q$ be a finite field with q elements, and let $\mathbb{P}^2(\mathbb{F}_q)$ be the projective plane over this field. Let (X, Y) be a randomly chosen *incidence* in this plane : X is a uniformly random *point*, and Y is a uniformly random *line* passing through X. Compute $\mathrm{H}(X)$, $\mathrm{H}(Y)$, and $\mathrm{H}(X, Y)$.

Exercise 6. For jointly distributed (X, Y)
(a) $\mathrm{H}(X, Y) \leq \mathrm{H}(X) + \mathrm{H}(Y)$;
(b) moreover, $\mathrm{H}(X, Y) = \mathrm{H}(X) + \mathrm{H}(Y)$, if and only if X and Y are independent

Exercise 7. For jointly distributed (X, Y)
(a) $\mathrm{H}(X, Y) = \mathrm{H}(X \mid Y) + \mathrm{H}(Y)$,
(b) $\mathrm{H}(X \mid Y) \geq 0$, with $\mathrm{H}(X \mid Y) = 0$ if and only if $X = \text{Function}(Y)$.

Exercise 8. For jointly distributed (X, Y)
(a) $\mathrm{I}(X : Y) = \mathrm{I}(Y : X) = \mathrm{H}(X) + \mathrm{H}(Y) - \mathrm{H}(X, Y)$,
(b) $\mathrm{I}(X : Y) \leq \mathrm{H}(X)$, and $\mathrm{I}(X : Y) \leq \mathrm{H}(Y)$,
(c) $\mathrm{I}(X : Y) \geq 0$, with $\mathrm{I}(X : Y) = 0$ if and only if X and Y are independent,
(d) $\mathrm{I}(X : Y) = \mathrm{H}(X)$ if and only if $X = \text{Function}(Y)$,
(e) $\mathrm{I}(X : X) = \mathrm{H}(X)$.

Exercise 9. Let X and Y be two random variables distributed both on $\{1, \ldots k\}$ (for some $k > 1$), and $\text{Prob}[X \neq Y] < \epsilon$. Prove that $\mathrm{H}(X \mid Y) < 1 + \epsilon \log(k - 1)$.

Exercise 10. Prove that the following three definitions of $\mathrm{I}(X : Y \mid Z)$ are equivalent :

1st definition. $\mathrm{I}(X : Y \mid Z) := \sum_c \mathrm{I}(X : Y \mid Z = c) \Pr[Z = c]$.

2nd definition. $\mathrm{I}(X : Y \mid Z) := \mathrm{H}(Y \mid Z) - \mathrm{H}(Y \mid X, Z)$.

3rd definition. $\mathrm{I}(X : Y \mid Z) := \mathrm{H}(X \mid Z) + \mathrm{H}(Y \mid Z) - \mathrm{H}(X, Y \mid Z)$.

Exercise 11. Prove that the following three definitions of $\mathrm{I}(X : Y : Z)$ are equivalent :

$$\begin{array}{rcl} \text{(a) } \mathrm{I}(X : Y : Z) & := & \mathrm{I}(X : Y) - \mathrm{H}(X : Y \mid Z) \\ \text{(b) } \mathrm{I}(X : Y : Z) & := & \mathrm{I}(XY : Z) - \mathrm{I}(X : Z \mid Y) - \mathrm{I}(Y : Z \mid X) \\ \text{(c) } \mathrm{I}(X : Y : Z) & := & \mathrm{H}(X) + \mathrm{H}(Y) + \mathrm{H}(Z) - \mathrm{H}(X, Y) - \mathrm{H}(X, Z) - \mathrm{H}(Y, Z) \\ & & + \mathrm{H}(X, Y, Z) \end{array}$$

Exercise 12. (a) Construct a joint distribution (X, Y, Z) such that $\mathrm{I}(X : Y \mid Z) = 0$ but $\mathrm{I}(X : Y) > 0$.
(b) Construct a joint distribution (X, Y, Z) such that $\mathrm{I}(X : Y) = 0$ but $\mathrm{I}(X : Y \mid Z) > 0$.

Exercise 13. Construct a joint distribution (X, Y, Z) such that

$$\mathrm{I}(X : Y) = \mathrm{I}(X : Z) = \mathrm{I}(Y : Z) = 0$$

and

$$\mathrm{I}(X : Y \mid Z) = \mathrm{I}(X : Z \mid Y) = \mathrm{I}(Y : Z \mid X) = 1.$$

Exercise 14. Prove that for all jointly distributed (X, Y, Z)

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

Exercise 15. Prove that for all jointly distributed (X, Y, Z) such that $\mathrm{H}(Z \mid X) = 0$ and $\mathrm{H}(Z \mid Y) = 0$ we have

$$\mathrm{H}(Z) \leq \mathrm{I}(X : Y).$$

Exercise 16. Prove that for all Markov chains $X \to Y \to Z$ we have

$$\mathrm{I}(X : Z) \leq \mathrm{I}(X : Y) \text{ and } \mathrm{I}(X : Z) \leq \mathrm{I}(Y : Z).$$

Exercise 17. Prove that for all Markov chains $W \to X \to Y \to Z$ we have

$$\mathrm{I}(W : Z) \leq \mathrm{I}(X : Y).$$

Exercise 18. For the entropy values of (X_1, X_2, X_3) we have the following $3 \times 3 = 9$ linear constraints :

$$\mathrm{H}(X_1 \mid X_2, X_3) \geq 0, \ldots, \ \mathrm{I}(X_1 : X_2) \geq 0, \ldots, \ \mathrm{I}(X_1 : X_2 \mid X_3) \geq 0, \ldots$$

Prove that there is no other linear inequalities for entropies of three random variables besides these ones (and their linear combinations) that are true for all distributions (X_1, X_2, X_3).
Hint : try to determine the extreme rays of the cone $\overline{\mathbf{P}}_3$.

Exercise 19. Let $\mathbf{P}_n$ be the set of entropic profiles for all $(X_1, \ldots, X_n)$.
(a) If two vectors v and w belong to $\mathbf{P}_n$ then the sum $v + w$ also belongs to $\mathbf{P}_n$.
(b) If a vector v belongs to $\mathbf{P}_n$ then for every natural n the vector $n \cdot v$ also belongs to $\mathbf{P}_n$.
(c) If a vector v belongs to $\mathbf{P}_n$ then for every real $\lambda > 0$ the vector $\lambda \cdot v$ also belongs to $\overline{\mathbf{P}}_n$
N.B. : We do *not* claim that $\lambda \cdot v$ belongs to $\mathbf{P}_n$.
(d) Prove that $\overline{\mathbf{P}}_n$ (topological closure of $\mathbf{P}_n$) is a *convex cone* (show that $\overline{\mathbf{P}}_n$ is convex and that it is a cone).

Exercise 20. Prove *correctness* and *security* of the Shamir secret sharing scheme.

Exercise 21. (a) Assume that $\mathrm{I}(S_0 : S_1) = 0$ and $\mathrm{H}(S_0 \mid S_1, S_2) = 0$. Prove that $\mathrm{H}(S_2) \geq \mathrm{H}(S_0)$.
(b) Let $1 < t \leq n$. Assume in some secret sharing scheme with n participants every t participants can find the secret S_0 while every $t - 1$ participants get no information on S_0. Prove that fro every $i = 1, \ldots, n$ we have $\mathrm{H}(S_i) \geq \mathrm{H}(S_0)$.

Exercise 22. We consider secret sharing schemes with a random secret key S_0 and and shares S_A, S_B, S_C, S_D such that

- (*correctness*) the pairs $\{S_A, S_B\}$, $\{S_B, S_C\}$, $\{S_C, S_D\}$ allow to get the secret i.e., $\mathrm{H}(S_0 \mid S_A, S_B) = 0$, $\mathrm{H}(S_0 \mid S_B, S_C) = 0$, $\mathrm{H}(S_0 \mid S_C, S_D) = 0$
- (*security*) other pairs of shares give no information on the secret, i.e., $\mathrm{H}(S_0 \mid S_A, S_C) = \mathrm{H}(S_0)$, $\mathrm{H}(S_0 \mid S_A, S_D) = \mathrm{H}(S_0)$, $\mathrm{H}(S_0 \mid S_B, S_D) = \mathrm{H}(S_0)$.

(a) Construct a correct and secure scheme of secret sharing such that

$$\max\{\mathrm{H}(S_A), \mathrm{H}(S_B), \mathrm{H}(S_C), \mathrm{H}(S_D)\} \leq \frac{3}{2}\mathrm{H}(S_0)$$

(b) Prove that in *every* correct and secure scheme of secret sharing

$$\max\{\mathrm{H}(S_A), \mathrm{H}(S_B), \mathrm{H}(S_C), \mathrm{H}(S_D)\} \geq \frac{3}{2}\mathrm{H}(S_0)$$