Exercise 1.

Consider a deterministic channel, and a partition $S_1, S_2, \dots, S_K$ of the secrets' space S, corresponding to the observables $o_1, o_2, \dots o_K$ i.e., such that:

$$\forall s \in S \quad p(o_i | s) = \begin{cases} 1 & \text{if } s \in S_i \\ 0 & \text{otherwise} \end{cases}$$

Define the prior that gives the Shannon capacity (i.e., the prior that maximizes the Shannon mutual information) in terms of the sizes of the S_i's.

Solution. By definition, $C = \sup_{p(\cdot)_S} I(S;O)$

where $I(S;O) = H(S) - H(S|O)$

$= H(O) - H(O|S)$

but in a deterministic channel, $H(O|S) = 0$

hence $I(S;O) = H(O)$.

The prior ~~entro~~ that maximizes $I(S;O)$ is therefore the prior that maximizes $H(O)$.

We know that the entropy of a random variable is max when the distribution is uniform, hence the maximizing prior ~~should~~ must be the one which gives as marginal $p(o_i) = \frac{1}{K}$ $\forall i = 1, \dots, K$

~~then~~ one possible such prior is:

$$p_S(s) = \frac{1}{K|S_i|} \quad \text{where } S_i \text{ is the set of the partition which contains } s.$$

The above is the "canonical" solution, but there are others

In practice every distribution $p_S(\cdot)$ on S such that

$$\forall i = 1, \dots, K \quad \sum_{s \in S_i} p_S(s) = \frac{1}{K}$$

is a prior that maximizes ~~I(S;O)~~ $I(S;O)$.

Exercise 2

Consider $S = \{s_1, s_2\}$ and $O = \{o_1, o_2, o_3\}$ with channel matrix

	o_1	o_2	o_3
s_1	$1/2$	$1/2$	0
s_2	0	$1/2$	$1/2$

Let $x = p(s_1)$.

~~Define~~ Express $I_\infty(S;O)$ as a function of x.

Solution $I_\infty(S;O) = H_\infty(S) - H_\infty(S|O)$ by definition

where $H_\infty(S) = -\log \max_s p(s) = \begin{cases} -\log(1-x) & 0 \le x \le 1/2 \\ -\log x & 1/2 \le x \le 1 \end{cases}$

and

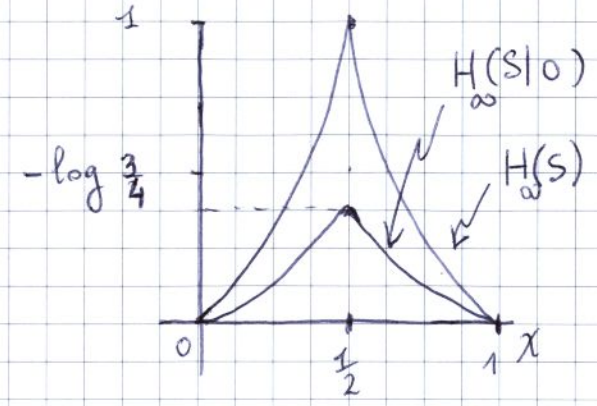
$$H_\infty(S|O) = -\log \sum_o \max_s \left(p(o|s) \cdot p(s)\right)$$

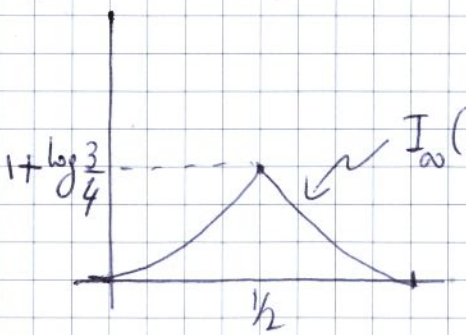
$$= -\log\Big(\max(0, \tfrac{1}{2}x) + \max(\tfrac{1}{2}x, \tfrac{1}{2}(1-x)) + \max(0, \tfrac{1}{2}(1-x))\Big)$$

$$= -\log\left(\tfrac{1}{2}x + \max\left(\tfrac{1}{2}x, \tfrac{1}{2}(1-x)\right) + \tfrac{1}{2}(1-x)\right)$$

$$= -\log\left(\tfrac{1}{2} + \max\left(\tfrac{1}{2}x, \tfrac{1}{2}(1-x)\right)\right)$$

$$= \begin{cases} -\log\left(\frac{1}{2} + \frac{1}{2}(1-x)\right) & 0 \le x \le 1/2 \\ -\log\left(\frac{1}{2} + \frac{1}{2}x\right) & 1/2 \le x \le 1 \end{cases}$$





Exercise 3

Prove that $\mathcal{L}_g(\pi, c) \geq 0$, i.e., $\log \frac{V_g(\pi, c)}{V_g(\pi)} \geq 0$ for every g s.t. $V_g(\pi) \neq 0$

Solution

$$\frac{V_g(\pi, c)}{V_g(\pi)} = \frac{\sum_y p(y) \cdot \max_w \left(\sum_x p(x|y) \cdot g(w,x) \right)}{\max_w \sum_x p(x) \cdot g(w,x)}$$

since $p(y)$ does not depend on w →

$$= \frac{\sum_y \max_w \left(p(y) \cdot \sum_x p(x|y)\, g(w,x) \right)}{\max_w \sum_x p(x) \cdot g(w,x)}$$

since $p(y)$ does not depend on x →

$$= \frac{\sum_y \max_w \sum_x p(y) \cdot p(x|y) \cdot g(w,x)}{\max_w \sum_x p(x) \cdot g(w,x)}$$

property of max →

$$\geq \frac{\max_w \sum_y \sum_x p(y)\, p(x|y)\, g(w,x)}{\max_w \sum_x p(x) \cdot g(w,x)}$$

since $g(w,x)$ does not depend on y →

$$= \frac{\max_w \sum_x g(w,x) \sum_y p(y) p(x|y)}{\max_w \sum_x p(x)\, g(w,x)}$$

since $\sum_y p(y) \cdot p(x|y) = \sum_y p(x,y) = p(x)$ →

$$= \frac{\max_w \sum_x g(w,x) \cdot p(x)}{\max_w \sum_x g(w,x) \cdot p(x)} = 1$$