

Homework #1

Jonathan McFadden

TCSS - 580 : Winter 2018

Information Theory

Problem 2.3): Let \mathbb{P}^n be the set of all n -dimensional probability vectors, with elements $\vec{p} \in \mathbb{P}^n$ defined as $\vec{p} = (p_1, p_2, \dots, p_i, \dots, p_n)$ for $i \in \mathbb{Z}^+ \ni i \leq n$. By the definition of a probability space, we must have

$$\vec{p} \cdot \vec{1} = \sum_{i=1}^n \{p_i\} = 1 \quad , \quad \forall \vec{p} \in \mathbb{P}^n, \quad (2.3-1)$$

where vector $\vec{1}$ is defined as $\vec{1} = (q_1, q_2, \dots, q_k, \dots, q_n) \in \mathbb{Z}^n$ with $q_k = 1, \forall k \in [1, n]$ (where the interval $[1, n]$ is defined such that $[1, n] \subseteq \mathbb{Z}^+$). Furthermore, the definition of a probability space also requires that, for any $\vec{p} \in \mathbb{P}^n$, the elements of \vec{p} (the $p_i \in \vec{p}$ such that $i \in \mathbb{Z}^+ \ni i \leq n$) satisfy the condition

$$p_i \geq 0 \quad (2.3-2)$$

for all $i \in \mathbb{Z}^+ \ni i \leq n$.

The expression in 2.3-1 guarantees that the p_i of any $\vec{p} \in \mathbb{P}^n$ satisfy the bound $0 \leq p_i \leq 1$ where $i \in \mathbb{Z}^+ \ni i \leq n$. Therefore, the relation

$$p_i \log_2 [p_i] \geq 0 \quad (2.3-3)$$

holds for all p_i of any $\vec{p} \in \mathbb{P}^n$. Moreover, for the cases where $p_i = 0$ or $p_i = 1$, it is clear that the expression in 2.3-3 reduces to equality. Specifically, the relation $p_i \log_2 [p_i]$ becomes

$$p_i \log_2 [p_i] = 0 \quad (2.3-4)$$

for the case where $p_i = 0$ or $p_i = 1$. Moreover, the relation in 2.3-4 also represents the **smallest** possible value/result for the expression $p_i \log_2 [p_i]$. That is to say, that when $p_i = 0$ or $p_i = 1$, then $p_i \log_2 [p_i]$ is at a minimum.

The result in 2.3-1, makes it clear that *only* **ONE** p_i in each $\vec{p} \in \mathbb{P}^n$ may have the value $p_i = 1$; therefore the probability vectors $\vec{p} \in \mathbb{P}^n$ which result in a minimum value for $p_i \log_2 [p_i]$ all have exactly one non-zero element with the non-zero element having a value of one. This implies that there are only n such probability vectors, \vec{p}^* within any \mathbb{P}^n . Furthermore, the value of $H(X) = \sum_{i=1}^n \{p_i \log_2 [p_i]\}$ for any such \vec{p}^* is also zero.

Problem 2.4 a): Recall the chain-rule for conditional entropies of X given Y ,

$$H(X | Y) = H(X, Y) - H(Y) \quad (2.4-1)$$

We apply the expression in 2.4-1 to the case of $g(X)$ given X to obtain

$$H(g(X) | X) = H(g(X), X) - H(X) \quad (0.0.1)$$

by rearranging the expression in the previous result as follows,

$$H(g(X), X) = H(X) + H(g(X) | X) \quad (2.4-2)$$

we obtain the desired result.

Problem 2.4 b): For any given value of X , we automatically know $g(X)$. Therefore, the expression for $H(g(X), X)$ in 2.4-2 becomes

$$H(g(X), X) = H(X)$$

which is the desired result.

Problem 2.4 c): Recalling the expression for the conditional entropy chain rule in 2.4-1 and using it for the case where $X = X$ and $Y = g(X)$ yields the result

$$H(X | g(X)) = H(X, g(X)) - H(g(X))$$

rearranging the above expression yields

$$H(X, g(X)) = H(g(X)) + H(X | g(X)) \quad (2.4-3)$$

we obtain the desired result.

Problem 2.4 c): Recalling the expression for the conditional entropy chain rule in 2.4-1 and using it for

the case where $X = X$ and $Y = g(X)$ yields the result

$$H(X | g(X)) = H(X, g(X)) - H(g(X))$$

rearranging the above expression yields

$$H(X, g(X)) = H(g(X)) + H(X | g(X)) \quad (2.4-3)$$

we obtain the desired result.

Problem 2.4 d): For any arbitrary function, $g(X)$, of a random variable X , the entropy $H(X | g(X))$ satisfies the condition

$$H(X | g(X)) \geq 0 \quad (2.4-4)$$

for the case where $g(X)$ is one-to-one, the relation in 2.4-4 simplifies to

$$H(X | g(X)) = 0$$

Applying the relation in 2.4-4 to the expression in 2.4-3 yields

$$\begin{aligned} H(X, g(X)) &= H(g(X)) + H(X | g(X)) \\ &\geq H(g(X)) + H(X | g(X)) - H(X | g(X)) \\ &\geq H(g(X)) \end{aligned}$$

Problem 2.9 a): Let $\rho(X, Y)$ be a function which is defined according to

$$\rho(X, Y) = H(X | Y) + H(Y | X) \quad (2.9-1)$$

for all x and y . Since conditional probabilities are always non-zero (*for arbitrary X and Y we have $H(X | Y) \geq 0$*), we can say that $H(X | Y)$ has the property

$$H(X | Y) \geq 0$$

and that $H(Y | X)$ has the property

$$H(Y | X) \geq 0$$

Applying these properties of $H(X | Y) \geq 0$ and $H(Y | X) \geq 0$ to the expression in 2.9-1 yields

$$\rho(X, Y) = H(X | Y) + H(Y | X) \geq 0 \quad (2.9-2)$$

which indicates that $\rho(X, Y)$ satisfies the first property of a metric over all x and y . By its definition in 2.9-1, we can say that $\rho(X, Y)$ is symmetric; therefore, we can additionally say that $\rho(X, Y)$ satisfies the second condition of a metric over all x and y .

Now, consider three random variables, X, Y , and Z . Then write

$$\rho(X, Y) = H(X | Y) + H(Y | X) \quad (2.9-3)$$

and

$$\rho(Y, Z) = H(Y | Z) + H(Y | Z) \quad (2.9-4)$$

and

$$\rho(X, Z) = H(X | Z) + H(Z | X) \quad (2.9-5)$$

We now add the expression in 2.9-3 and 2.9-4 to obtain

$$\begin{aligned} & H(X | Y) + H(Y | X) + H(Y | Z) + H(Z | Y) \\ & \left[H(X | Y) + H(Y | Z) \right] + \left[H(Z | Y) + H(Y | X) \right] \end{aligned} \quad (2.9-6)$$

By the chain rule for conditional entropies, we have $H(X | Y) + H(Y | Z) = H(X, Y | Z)$ and $H(Z | Y) + H(Y | X) = H(Z, Y | X)$ so the expression in 2.9-6 becomes

$$H(X, Y | Z) + H(Z, Y | X)$$

Again applying the chain rule for conditional entropies to the previous result, we have

$$\left[H(X | Z) + H(Y | X, Z) \right] + \left[H(Z | X) + H(Y | Z, X) \right]$$

Since conditional entropies are always greater or equal to zero, the $H(Y | X, Z)$ and $H(Y | Z, X)$ terms in the previous result satisfy $H(Y | X, Z) \geq 0$ and $H(Y | Z, X) \geq 0$. This allows us to rewrite the previous result as

$$\begin{aligned}
 \rho(X, Y) + \rho(Y, Z) &= H(Y | Z) + H(Y | Z) + H(X | Y) + H(Y | X) \\
 &= \left[H(X | Z) + H(Y | X, Z) \right] + \left[H(Z | X) + H(Y | Z, X) \right] \\
 &\geq H(X | Z) + H(Z | X)
 \end{aligned}$$

Using the definition from 2.9-5, the previous result becomes

$$\begin{aligned}
 \rho(X, Y) + \rho(Y, Z) &= \left[H(X | Z) + H(Y | X, Z) \right] + \left[H(Z | X) + H(Y | Z, X) \right] \\
 &\geq H(X | Z) + H(Z | X) \\
 &\geq \rho(X, Z)
 \end{aligned}$$

thereby indicating that $\rho(X, Y) + \rho(Y, Z) \geq \rho(X, Z)$ holds and, by extension, that the definition in 2.9-1 satisfies the fourth condition of a metric over all x and y .

Finally, we consider the case where $X = Y$ via a one-to-one mapping. Since $H(X, Y) = 0$ iff X is a function of Y and $H(Y, X) = 0$ iff Y is a function of X , $\rho(X, Y)$ can only equal zero if and only if $X = Y$. This satisfies the third and only remaining condition of a metric over all x and y ; therefore, for cases where X and Y are related by a one-to-one mapping, $\rho(X, Y)$ is a metric over all x and y .

Problem 2.9 b): Starting with the expression $I(X; Y) = H(X) - H(X | Y)$ we rearrange to obtain

$$H(X | Y) = H(X) - I(X; Y) \tag{2.9-7}$$

We also obtain

$$H(Y | X) = H(Y) - I(Y; X) \quad (2.9-8)$$

similarly. We now apply the expressions in 2.9-7 and 2.9-8 to the definition of $\rho(X, Y)$ in 2.9-1 to obtain the result

$$\begin{aligned} \rho(X, Y) &= H(X | Y) + H(Y | X) \\ &= H(X) - I(X; Y) + H(Y) - I(Y; X) \end{aligned}$$

Noting that $I(X; Y) = I(Y; X)$ the previous result can be simplified to the expression

$$\begin{aligned} \rho(X, Y) &= H(X) - I(X; Y) + H(Y) - I(Y; X) \\ &= H(X) - I(X; Y) + H(Y) - I(X; Y) \\ &= H(X) + H(Y) - 2I(X; Y) \end{aligned} \quad (2.9-9)$$

which proves the first line of the problem. Next, we note that $I(X; Y) = H(X) + H(Y) - H(X, Y)$ and apply this relation to the expression in 2.9-9 so that we obtain

$$\begin{aligned} \rho(X, Y) &= H(X) + H(Y) - 2I(X; Y) \\ &= H(X) + H(Y) - I(X; Y) - I(X; Y) \\ &= H(X) + H(Y) - I(X; Y) - [H(X) + H(Y) - H(X, Y)] \\ &= H(X, Y) - I(X; Y) \end{aligned} \quad (2.9-10)$$

as our result and proving the second line of the problem. Finally, we again note

$I(X; Y) = H(X) + H(Y) - H(X, Y)$ and then apply it to the expression in 2.9-10 to yield the result

$$\begin{aligned}\rho(X, Y) &= H(X, Y) - I(X; Y) \\ &= H(X, Y) - [H(X) + H(Y) - H(X, Y)] \\ &= 2H(X, Y) - H(X) - H(Y)\end{aligned}$$

which proves the third and final line of the problem.