Introduction to Quantum Information Processing

Roei Rosenzweig 313590937,
Roey Maor 205798440

April 30, 2017

1 Mutual Information - Solution

1. We expand the expression to get:

$$I(X;Y) = H(X) - H(X|Y) = -\sum_x p(x)\log_2 p(x) + \sum_{x,y} p(x,y)\log_2 p(x|y)$$

We know that a probability distribution of variable X can be computed from the mutual probability of X and Y by summing all the values in range for Y:

$$p(x) = \sum_y p(x,y)$$

Plugging this into the previous equation, we get:

$$I(X;Y) = \sum_{x,y} p(x,y)\log_2 p(x|y) - \sum_{x,y} p(x,y)\log_2 p(x) = \sum_{x,y} p(x,y)\log_2\left(\frac{p(x|y)}{p(x)}\right)$$

From logarithm rules and conditional probability definition:

$$\log_2\left(\frac{p(x|y)}{p(x)}\right) = -\log_2\left(\frac{p(x)p(y)}{p(x,y)}\right)$$

Plugging it, we get:

$$\boxed{I(X;Y) = -\sum_{x,y} p(x,y)\log_2\left(\frac{p(x)p(y)}{p(x,y)}\right)}$$

2. We can write $I(X;Y)$ using the logarithm-identity $\log_a x \cdot \log_b a = \log_b x$ as:

$$K \cdot I(X;Y) = -\sum_{x,y} p(x,y)\ln\left(\frac{p(x)p(y)}{p(x,y)}\right)$$

Where $K = \ln 2 > 0$. By using the identity $\ln t \leq t-1$ for $t > 0$ and knowing that $\frac{p(x)p(y)}{p(x,y)}$ is non-negative (because probability cannot be negative, obv.) we show:

$$-K \cdot I(X;Y) \leq \sum_{x,y} p(x,y)\left(\frac{p(x)p(y)}{p(x,y)} - 1\right) = \sum_{x,y}\left(p(x)p(y) - p(x,y)\right)$$

$\ln t \leq t-1$ is equality **iff** $t = 1$.

Corollary 1.0.1. *$-K \cdot I(X;Y) = \sum_{x,y}\left(p(x)p(y) - p(x,y)\right)$ iff X, Y are independent.* ***Proof:*** *If X, Y are independent $\iff$ $p(x)p(y) = p(x,y)$ for every pair of x, y $\iff$ $\forall x, y : \frac{p(x)p(y)}{p(x,y)} = 1$ $\iff$*

We expand the expression to get sums over probabilities (which we can reduce to 1):

$$
\begin{gathered}
-K \cdot I(X;Y) \leq \sum_x \left(p(x) \cdot \sum_y p(y) \right) - \sum_{x,y} p(x,y) \\
\Rightarrow I(X;Y) \geq K \cdot \sum_x p(x) - 1 = 0 \Rightarrow \boxed{I(X;Y) \geq 0}
\end{gathered}
$$

From 1.0.1 and the above expansion we can conclude that $I(X;Y) = 0 \iff X, Y$ are independent.

2 Entropy and Mutual Information

1.

$$
\begin{aligned}
Y &= \begin{cases} 1, & \text{the keys are in the pocket} \\ 0, & \textit{otherwise} \end{cases} \\
X &= \begin{cases} i \in [1,100], & \text{the keys are in the i-th location} \\ 0, & \text{otherwise} \end{cases}
\end{aligned}
$$

2.

	$Y=0$	$Y=1$	
$X=0$	$p(X=0,Y=0) = 0$ $p(X=0 \vert Y=0) = 0$ $p(Y=0 \vert X=0) = 0$	$p(X=0,Y=1) = 0.99$ $p(X=0 \vert Y=1) = 1$ $p(Y=1 \vert X=0) = 1$	$p(X=0) = 0.99$
$X=i>0$	$i>0$ $p(X=i,Y=1) = 0$ $p(X=i \vert Y=1) = 0$ $p(Y=1 \vert X=i) = 0$	$i>0$ $p(X=i,Y=0) = 0.0001$ $p(X=i \vert Y=0) = 0.01$ $p(Y=0 \vert X=i) = 1$	$p(X=i>0) = 0.0001$
	$p(Y=0) = 0.01$	$p(Y=1) = 0.99$	1

3.

$$
\begin{aligned}
H(X) &= -\sum_x p(X=x) \log_2 p(X=x) \\
&= -p(X=0) \log_2 p(X=0) - 100 \cdot (X=i) \log_2 p(X=i) \\
&= -0.99 \cdot \log_2 0.99 - 100 \cdot 0.0001 \log_2 0.0001 \\
&= 0.044
\end{aligned}
$$

$$
\begin{aligned}
H(Y) &= -\sum_y p(Y=y) \log_2 p(Y=y) \\
&= -p(Y=0) \log_2 p(Y=0) - \cdot (Y=1) \log_2 p(Y=1) \\
&= -0.01 \cdot \log_2 0.01 - 0.99 \log_2 0.99 \\
&= 0.024
\end{aligned}
$$

$$
\begin{aligned}
H(X|Y=0) &= -\sum_{x} p(X|Y=0)\log_2 p(X|Y=0) \\
&= -p(X=0|Y=0)\log_2 p(X=0|Y=0) - 100\cdot (X=i|Y=0)\log_2 p(X=i|Y=0) \\
&= -100\cdot 0.01\log_2 0.01 \\
&= 2
\end{aligned}
$$

$$
\begin{aligned}
H(X|Y=1) &= -\sum_{x} p(X|Y=1)\log_2 p(X|Y=1) \\
&= -p(X=0|Y=1)\log_2 p(X=0|Y=1) - 100\cdot (X=i|Y=1)\log_2 p(X=i|Y=1) \\
&= -1\cdot 0 \\
&= 0
\end{aligned}
$$

$$
\begin{aligned}
H(X|Y) &= -\sum_{x,y} p(X=x,Y=y)\log_2 p(X=x|Y=y) \\
&= -p(X=0,Y=0)\log_2 p(X=0|Y=0) - \sum_{i=1}^{100} p(X=i,Y=0)\log_2 p(X=i|Y=0) \\
&\quad - p(X=0,Y=1)\log_2 p(X=0|Y=1) - \sum_{i=1}^{100} p(X=i,Y=1)\log_2 p(X=i|Y=1) \\
&= 0 - 100\cdot 0.0001\log_2 0.01 - 0.99\log_2 1 - 100\cdot 0 \\
&= 0.02
\end{aligned}
$$

$$
\begin{aligned}
H(Y|X) &= -\sum_{x,y} p(X=x,Y=y)\log_2 p(Y=y|X=x) \\
&= -p(X=0,Y=0)\log_2 p(Y=0|X=0) - \sum_{i=1}^{100} p(X=i,Y=0)\log_2 p(Y=0|X=i) \\
&\quad - p(X=0,Y=1)\log_2 p(Y=1|X=0) - \sum_{i=1}^{100} p(Y=1,X=i)\log_2 p(Y=1|X=i) \\
&= 0 - 0 - 0 - 0 \\
&= 0
\end{aligned}
$$

4.