HOMEWORK 1 (2023) — SOLUTIONS

JAIST — SCHOOL OF INFORMATION SCIENCE — I232 INFORMATION THEORY

1. You have 9 gold ingots, but one of them is a counterfeit. The counterfeit is lighter than the others; you cannot otherwise distinguish the counterfeit. A balance with two cups is to be used; the balance will show "left cup is heavier," "right cup is heavier," or "equal."

   (a) What is the minimum number of uses of the balance that is guaranteed to always determine the counterfeit? Describe a method to determine the counterfeit.

   (b) Assume you have n ingots. Find a lower bound on t, the number of uses of the balance to determine the counterfeit. Use an information theory perspective.

Solution:

(a) Form three stacks of three ingots, and place two stacks ingots on the balance. If either stack is lighter, then it contains the counterfeit. If the two stacks are equal, then the third stack contains the counterfeit.

Having identified the stack of three containing the counterfeit, place two ingots from this stack on the balance. If either ingot is lighter, it will be identified as the counterfeit. If the two are equal, then the third ingot is identified as the counterfeit.

(b) The system has n states, corresponding to one of n coins being counterfeit, so the uncertainty (or entropy) is $\log n$ bits. Each weighing reduces the uncertainty by $\log 3$ bits. We want to reduce the uncertainty to 0 bits, so:

$$\begin{aligned}(\log n) - t(\log 3) &\leq 0\\ (\log n) &\leq t(\log 3)\\ \frac{\log n}{\log 3} &\leq t\\ t \geq \frac{\log n}{\log 3} &= \log_3 n\end{aligned}$$

The number of uses of the balance is the integer $\lceil \log_3 n \rceil$.

2. Let X and Z be independent random variables where X is a $(0,1)$ binary random variable distributed as $[\frac{1}{2}, \frac{1}{2}]$, and Z be distributed as:

$$p_{\mathsf{Z}}(z) = \begin{cases} 1-p & z = 0 \\ p & z = 1 \end{cases}.$$

Now, let $\mathsf{Y} = \mathsf{X} \oplus \mathsf{Z}$, where $\oplus$ is the exclusive-or operation $0 \oplus 0 = 1 \oplus 1 = 0$ and $1 \oplus 0 = 0 \oplus 1 = 1$. Recall the binary entropy function is $h(p)$, with $H(\mathsf{Z}) = h(p)$ and $H(\mathsf{X}) = h(\frac{1}{2})$.

(a) Find $p_{\mathsf{Y}}(y)$

Solution: Use the theorem of total probability: $p_{\mathsf{Y}}(y) = \sum_{z \in \mathcal{Z}} p_{\mathsf{Y}|\mathsf{Z}}(y|z) p_{\mathsf{Z}}(z)$

$$\begin{aligned}p_{\mathsf{Y}}(0) &= p_{\mathsf{Y}|\mathsf{Z}}(0|0)p_{\mathsf{Z}}(0) + p_{\mathsf{Y}|\mathsf{Z}}(0|1)p_{\mathsf{Z}}(1)\\ p_{\mathsf{Y}}(1) &= p_{\mathsf{Y}|\mathsf{Z}}(1|0)p_{\mathsf{Z}}(0) + p_{\mathsf{Y}|\mathsf{Z}}(1|1)p_{\mathsf{Z}}(1)\end{aligned}$$

Note that $p_{\mathsf{Y}|\mathsf{Z}}(0|0)$ is equal to $1/2$, because if $\mathsf{Z} = 0$, then $\mathsf{Y} = \mathsf{X}$ and $\Pr(\mathsf{Y} = 0|\mathsf{Z} = 0) = \Pr(\mathsf{X} = 0|\mathsf{Z} = 0) = \Pr(\mathsf{X} = 0)$.

$$\begin{aligned}p_{\mathsf{Y}}(0) &= \frac{1}{2} \cdot (1-p) + \frac{1}{2} \cdot p = \frac{1}{2}\\ p_{\mathsf{Y}}(1) &= \frac{1}{2} \cdot (1-p) + \frac{1}{2} \cdot p = \frac{1}{2}\end{aligned}$$

(b) Find $p_{\mathsf{Y}|\mathsf{X}}(y|x)$

Solution: Again use the theorem of total probability: $p_{\mathsf{Y}|\mathsf{X}}(y|x) = \sum_{z\in\mathcal{Z}} p_{\mathsf{Y}|\mathsf{XZ}}(y|x,z)p_{\mathsf{Z}|\mathsf{X}}(z|x)$. This time, $p_{\mathsf{Y}|\mathsf{XZ}}(y|x,z)$ will be 1 if $y = z \oplus x$, and otherwise 0, and $p_{\mathsf{Z}|\mathsf{X}}(z|x) = p_{\mathsf{Z}}(z)$ because X and Z are independent:

$$\begin{aligned}
p_{\mathsf{Y}|\mathsf{X}}(0|0) &= p_{\mathsf{Y}|\mathsf{XZ}}(0|0,0)p_{\mathsf{Z}}(0) + p_{\mathsf{Y}|\mathsf{XZ}}(0|0,1)p_{\mathsf{Z}}(1) = 1\cdot(1-p) + 0\cdot p = 1-p\\
p_{\mathsf{Y}|\mathsf{X}}(1|0) &= p_{\mathsf{Y}|\mathsf{XZ}}(1|0,0)p_{\mathsf{Z}}(0) + p_{\mathsf{Y}|\mathsf{XZ}}(1|0,1)p_{\mathsf{Z}}(1) = 0\cdot(1-p) + 1\cdot p = p\\
p_{\mathsf{Y}|\mathsf{X}}(0|1) &= p_{\mathsf{Y}|\mathsf{XZ}}(0|1,0)p_{\mathsf{Z}}(0) + p_{\mathsf{Y}|\mathsf{XZ}}(0|1,1)p_{\mathsf{Z}}(1) = 0\cdot(1-p) + 1\cdot p = p\\
p_{\mathsf{Y}|\mathsf{X}}(1|1) &= p_{\mathsf{Y}|\mathsf{XZ}}(1|1,0)p_{\mathsf{Z}}(0) + p_{\mathsf{Y}|\mathsf{XZ}}(1|1,1)p_{\mathsf{Z}}(1) = 1\cdot(1-p) + 0\cdot p = 1-p
\end{aligned}$$

(c) Find $H(\mathsf{Y}|\mathsf{X})$

Solution: First compute $H(\mathsf{Y}|\mathsf{X}=x)$:

$$\begin{aligned}
H(\mathsf{Y}|\mathsf{X}=0) &= p_{\mathsf{Y}|\mathsf{X}}(0|0)\log p_{\mathsf{Y}|\mathsf{X}}(0|0) + p_{\mathsf{Y}|\mathsf{X}}(1|0)\log p_{\mathsf{Y}|\mathsf{X}}(1|0)\\
&= -(1-p)\log(1-p) - p\log p = h(p)\\
H(\mathsf{Y}|\mathsf{X}=1) &= p_{\mathsf{Y}|\mathsf{X}}(0|1)\log p_{\mathsf{Y}|\mathsf{X}}(0|1) + p_{\mathsf{Y}|\mathsf{X}}(1|1)\log p_{\mathsf{Y}|\mathsf{X}}(1|1)\\
&= -p\log p - (1-p)\log(1-p) = h(p)
\end{aligned}$$

and then find $H(\mathsf{Y}|\mathsf{X})$:

$$\begin{aligned}
H(\mathsf{Y}|\mathsf{X}) = H(\mathsf{Y}|\mathsf{X}=0)p_{\mathsf{X}}(0) + H(\mathsf{Y}|\mathsf{X}=1)p_{\mathsf{X}}(1) = \frac{1}{2}h(p) + \frac{1}{2}h(p)\\
= h(p)
\end{aligned}$$

(d) Find $H(\mathsf{Y}\oplus\mathsf{X}|\mathsf{X})$

Solution: Note that $\mathsf{Y}\oplus\mathsf{X} = \mathsf{Z}$. So $H(\mathsf{Y}\oplus\mathsf{X}|\mathsf{X}) = H(\mathsf{Z}|\mathsf{X}) = H(\mathsf{Z})$, by the independence of X and Z. So $H(\mathsf{Z}) = h(p)$.
You just showed that $H(\mathsf{Y}\oplus\mathsf{X}|\mathsf{X}) = H(\mathsf{Y}|\mathsf{X})$.

3. Find the derivative $h'(p)$ of the binary entropy function $h(p)$.

Solution:

$$\begin{aligned}
h(p) &= -p\log p - (1-p)\log(1-p)\\
h'(p) &= -(\log p + p\cdot\frac{1}{p\ln 2}) - (-\log(1-p) + (1-p)\cdot\frac{1}{(1-p)\ln 2}\cdot(-1))\\
&= \log(1-p) - \log p\\
&= \log\frac{1-p}{p}
\end{aligned}$$