Tutorial 4

P2 Claim: $H(X,Y,f(X,Y)) = H(X,Y)$

$$H(X,Y,Z) = -\sum_{x,y,z} P(X=x, Y=y, Z=z) \log\left(P(X=x, Y=y, Z=z)\right)$$

$$P(X=x, Y=y, Z=z) = \begin{cases} P(X=x, Y=y) & \text{if } z = f(x,y) \\ 0 & \text{otherwise} \end{cases}$$

$$\Rightarrow H(X,Y,Z) = -\sum_{x,y} P(X=x, Y=y) \log\left(P(X=x, Y=y)\right) = H(X,Y)$$

Note: $0 \cdot \log(0) = 0$

P3 $M_+ = \{m \in \mathcal{M} \mid P(\hat{M} = m) > 0\}$

$C'_+ = \{c \in C' \mid P(\hat{C} = c) > 0\}$

Assumptions: i) $|\mathcal{M}| = |\mathcal{K}| = |C'|$

ii) $P(\hat{M} = m) > 0 \quad \forall m \in \mathcal{M}$

With Lemma 4.12 a)

$$|\mathcal{M}_+| \overset{\downarrow}{\leq} |C'_+| \overset{i)}{\leq} |C'| \overset{ii)}{\leq} |\mathcal{M}| = |\mathcal{M}_+|$$

$\Rightarrow |C'_+| = |C'| \Rightarrow C'_+ = C'$

Let $m \in \mathcal{M}$, $c \in C'$

$$0 < P(\hat{C} = c) \overset{\text{perfect secrecy}}{=} P(\hat{C} = c \mid \hat{M} = m) = P(e(\hat{M}, \hat{K}) = c \mid \hat{M} = m)$$

$$= P(e(m, \hat{K}) = c) = \sum_{k \in \mathcal{K} : e(m,k) = c} P(\hat{K} = k) \neq 0$$

$\Rightarrow \forall m \in \mathcal{M}, c \in C' \; \exists k : e(m,k) = c$

For uniqueness of k fix $M \in \mathcal{M}$

$$|C'_+| = |C'| = |\{e(M,k) \mid k \in \mathcal{K}_+ = \mathcal{K}\}| \leq |\mathcal{K}| = |C'|$$

$\Rightarrow$ k is unique with $k = k(M,c)$

Let $M \in \mathcal{M}$, $C \in C'$

$$\Rightarrow P(\hat{C} = C) = P(\hat{k} = k(M,c))$$

Fix $C_0 \in C'$

$$\Rightarrow \{k(M,C_0) \mid M \in \mathcal{M}\} = \mathcal{K}$$

$$\Rightarrow P(\hat{C} = C) = P(\hat{k} = k) \quad \forall C \in C', k \in \mathcal{K}$$

$$\Rightarrow P(\hat{k} = k) = \frac{1}{|\mathcal{K}|} \quad \forall k \in \mathcal{K}$$

P1] a) $0 \leq H(X)$ $\quad p_i := P(X = x_i)$

$$H(X) = -\sum_i p_i \log(p_i) \geq 0$$

as $p_i \geq 0$; $-\log(p_i) \geq 0$, because $0 < p_i \leq 1$ and $0 \cdot \log(0) = 0$

$$\Rightarrow -p_i \log(p_i) \geq 0 \Rightarrow H(X) \geq 0$$

Equality holds if all $-p_i \cdot \log(p_i) = 0 \Leftrightarrow p_i \in \{0, 1\}$ $\forall i = 1, \dots, n$

b) $H(X) \leq \log(n)$ with equality if and only if $p(X = x_i) = \frac{1}{n}$

$$H(X) - \log(n) = -\sum_i p_i \log(p_i) - \underbrace{\sum_i p_i}_{=1} \log(n)$$

$$= \sum_{i: p_i > 0} p_i \log\left(\frac{1}{p_i \cdot n}\right) \qquad \underline{\text{Hint}}: \ln(z) \leq z - 1 \quad \forall z > 0$$

$$\leq \log(e) \sum_{i: p_i > 0} p_i \left(\frac{1}{p_i \cdot n} - 1\right)$$

$$= \log(e) \left(\sum_{i: p_i > 0} \frac{1}{n} - 1 \right) = \log(e) \left(\frac{k}{n} - 1 \right) \leq 0$$

$$k = |\{ i \mid : p_i > 0 \}| \leq n$$

$\Rightarrow$ Equality holds true iff $p(X = x_i) = \frac{1}{n}$

c) also uses $\ln(z) \leq z - 1$

d) see solution as pdf

e) $H(X, Y) \leq H(X) + H(Y)$

$$H(X, Y) \overset{d)}{=} H(X) + H(Y|X) \overset{(c)}{\leq} H(X) + H(Y)$$

equality in c) holds true, iff X and Y are stoch. independent